



ESTUDIO
DE MERCADO

2024



El mercado de la ciberseguridad en Suiza

Oficina Económica y Comercial
de la Embajada de España en Berna

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.

icex



ESTUDIO
DE MERCADO

9 de abril de 2024
Berna

Este estudio ha sido realizado por
Borja Tórtola Medina

Bajo la supervisión de la Oficina Económica y Comercial
de la Embajada de España en Berna

<https://suiza.oficinascomerciales.es>

© ICEX España Exportación e Inversiones, E.P.E.

NIPO: 224240080

Índice

1. Introducción	5
2. Definición del sector	6
2.1. Definición	6
2.2. Delimitación del sector	6
2.3. Tipos de soluciones de ciberseguridad	8
2.4. El sector de la ciberseguridad en el mundo	9
2.5. Clasificación arancelaria	10
3. Oferta – Análisis de competidores	11
3.1. El sector de la ciberseguridad en Suiza	11
3.1.1. Legislación	11
3.1.2. Instituciones	12
3.1.3. Principales ataques contra la ciberseguridad en Suiza	14
3.1.4. Tamaño del mercado	14
3.1.5. Comercio exterior	15
3.2. Empresas de ciberseguridad en Suiza	19
3.2.1. Empresas internacionales	20
3.2.2. Empresas nacionales	21
3.2.3. Empresas suizas inversoras en el sector TIC en España	23
3.2.4. Asociaciones nacionales de ciberseguridad	25
4. Demanda	27
4.1. Factores de la demanda	27
4.1.1. Empresas e infraestructuras críticas suizas: demanda de productos y servicios	29
4.2. Comercio exterior	31
5. Precios	32
6. Percepción del producto español	34
7. Canales de distribución	36
7.1. Acceso a potenciales socios	37
7.2. Ferias del sector	38
7.3. Publicaciones del sector	38
8. Acceso al mercado – Barreras	39
8.1. Aspectos a tener en cuenta	39
8.2. Criterios de inversión en Suiza	40
8.3. Concursos públicos y licitaciones	42
8.4. Certificación	43



9. Perspectivas del sector	44
9.1. Tendencias en el mercado de la ciberseguridad a nivel global	44
9.2. Tendencias en el mercado de la ciberseguridad en Suiza	45
10. Oportunidades	47
11. Información práctica	50
11.1. Perfil del dirigente suizo	51

icex

1. Introducción

La ciberseguridad, enmarcado dentro de las Tecnologías de la Información y Comunicación (TIC), centra en la protección de sistemas de información e infraestructuras críticas, abordando aspectos como la prevención de pérdida de información, fraude y ataques a redes y sistemas. Existen diversas soluciones en ciberseguridad, que se pueden clasificar en tres tipos principales: prevención, control y mitigación.

El Centro Nacional de Ciberseguridad de Suiza (National Cybersecurity Centre, NCSC), establecido en 2024, asume un papel crucial en la asesoría, evaluación de incidentes y coordinación del intercambio de datos de ciberseguridad. La centralización reciente de la legislación suiza en este ámbito refleja el compromiso del país con la colaboración internacional en este campo. A pesar del pequeño volumen de empresas en el sector, Suiza destaca como un centro de innovación mundial, ofreciendo oportunidades para establecer conexiones con empresas líderes y acceder a incentivos fiscales para actividades de I+D.

En el ámbito internacional, Suiza comercializa sus productos y servicios de ciberseguridad principalmente en Estados Unidos, Alemania y Reino Unido, aunque presenta un déficit comercial persistente en la partida TIC. En cuanto al comercio bilateral, la partida de comercio de servicios en tecnologías de la información y las comunicaciones (TIC) ha sido la más dinámica en los intercambios entre España y Suiza en los últimos años, habiéndose casi cuadruplicado las exportaciones españolas a Suiza en dicha partida entre 2014 y 2021, pasando de 216 a 824 millones de francos y de un saldo negativo para España de 61 millones de francos a uno positivo de 564 millones de francos.

La demanda de productos y servicios relacionados con la ciberseguridad en Suiza está influenciada por la necesidad de proteger tanto a las empresas como a las instituciones gubernamentales de los crecientes riesgos cibernéticos. Se estima que el mercado de ciberseguridad generó unos ingresos en 2023 de aproximadamente 808 millones de dólares.

A pesar de ser una potencia mundial en ciberseguridad, la mayoría de las empresas de ciberseguridad españolas no tienen presencia en Suiza, lo que contribuye a una percepción escasa de sus productos.

A medida que Suiza avanza hacia la modernización y la introducción de tecnologías como *Fintech*, *cloud computing* e IoT, la demanda de protección cibernética se incrementa. Sin embargo, se enfrenta a desafíos como la falta de personal especializado y la necesidad de mejorar las herramientas de ciberseguridad.

2. Definición del sector

2.1. Definición

La ciberseguridad se clasifica como un subsector dentro del sector de las Tecnologías de la Información y Comunicación (TIC).

La legislación española (Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información) define la ciberseguridad como la capacidad de las redes y sistemas de comunicación de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos.

El sector y el mercado de los productos y servicios relacionados con la ciberseguridad son muy amplios. Debido a la continua evolución de los sistemas informáticos y todo lo relativo a ellos, los ataques se han sofisticado, dando lugar a que la oferta de productos y servicios se encuentre en una constante evolución y crecimiento a nivel mundial.

2.2. Delimitación del sector

Dada la gran dimensión del mercado, es preciso mencionar que en este estudio se ahondará en el sector de la ciberseguridad relacionado con los productos y servicios relacionados con la protección de los sistemas de información y las infraestructuras críticas, según la clasificación de INCIBE (Instituto Nacional de Ciberseguridad de España). Es decir, se expondrá información sobre la defensa y reacción frente a pérdidas o robos de información, espionaje, fraude, interrupción de sistemas, ataques contra redes o sistemas, e infecciones de sistemas. También se tratarán los sistemas de computación en la nube y a las tecnologías móviles.

A continuación, se muestra la taxonomía de soluciones de ciberseguridad realizada por INCIBE¹ en la que se muestran productos relativos a este campo y su ámbito de aplicación. Cada una de estas soluciones tiene un público objetivo distinto. Pueden estar dirigidos a la seguridad de la información de particulares, de empresas y de infraestructuras (incluidas las críticas).

¹ INCIBE: Taxonomía de soluciones de ciberseguridad (2015)

TABLA 1. TAXONOMÍA DE SOLUCIONES DE CIBERSEGURIDAD

CATEGORÍA DEL PRODUCTO	Gestión de acceso e identidad	Seguridad en el puesto de trabajo	Seguridad en aplicaciones y datos	Seguridad en los sistemas	Seguridad en las redes
Antifraude: <i>Anti-Phishing, Anti-spam, Herramientas de filtrado de navegación, UTM, Appliance.</i>		✓	✓	✓	✓
Anti-malware: <i>Anti-virus, Anti-Adware, Anti-spyware, UTM, Appliance.</i>		✓	✓	✓	✓
Auditoría técnica: Análisis de <i>logs</i> y puertos, vulnerabilidades, Auditoría de contraseñas, Auditoría de sistemas y ficheros.	✓		✓		✓
Certificación normativa: SGSI, Análisis de riesgos, Planes y políticas de seguridad, Normativas de seguridad.		✓	✓	✓	✓
Contingencia y continuidad: H. de gestión de planes de contingencia y continuidad, Copias de seguridad, Infraestructura de respaldo, Virtualización, <i>Cloud</i> .		✓	✓	✓	✓
Control de acceso y autenticación: Control de acceso a red, NAC, Gestión de identidad y autenticación, <i>Single Sign-On</i> , Certificados digitales, Firma electrónica.	✓				
Cumplimiento legal: Herramientas de cumplimiento legal (LOPD, LSSI.), Borrado seguro, Destrucción documental.	✓	✓	✓		
Prevención de fuga de información: Control de contenidos confidenciales, Gestión del ciclo de vida de la información, Herramientas de cifrado.		✓	✓		✓
Protección de las comunicaciones: Cortafuegos (<i>firewall</i>), VPN, IDS, IPS, UTM, <i>Appliance</i> , Filtro de contenidos, P2P, Gestión y control de ancho de banda.		✓	✓		✓
Inteligencia de seguridad: Gestión de eventos de seguridad, SIM/SIEM, <i>Big Data</i> , Herramientas de monitorización y <i>reporting</i>			✓	✓	✓
Seguridad en dispositivos móviles: Seguridad para dispositivos móviles, Seguridad para redes inalámbricas, <i>BYOD</i> ² .		✓			

Fuente: Elaboración propia a partir de datos de INCIBE. Taxonomía de soluciones de ciberseguridad (2015).

² BYOD: Bring Your Own Device

2.3. Tipos de soluciones de ciberseguridad

Las soluciones para los destinatarios finales pueden clasificarse en tres grandes tipos:

1. **Soluciones de prevención**, con el fin de prevenir los incidentes.
2. **Soluciones de control**, para gestionar diferentes opciones de seguridad y cumplir con la normativa.
3. **Soluciones de mitigación**, orientación tras la recuperación y continuidad en caso de incidente.

Dentro de las soluciones de prevención encontramos:

- **Soluciones antimalware**: herramientas que protegen sistemas informáticos y cuya función es detectar y eliminar todo tipo de software malicioso. Ejemplos: antivirus, *anti-adware*, *antispyware*.
- **Soluciones antifraude**: protege a los usuarios de las actividades fraudulentas en Internet, como el robo de datos bancarios, robo de información personal, suplantación de identidad, etc.
- **Soluciones de prevención de fuga de información**: identifican, detectan y previenen fugas de información, a través de políticas de uso de la información, para garantizar la confidencialidad y la integridad. Ejemplos: control de contenidos confidenciales, herramientas de cifrado, etc.
- **Soluciones para la protección de las comunicaciones**: protegen los sistemas y dispositivos conectados a una red, por medio de la monitorización del tráfico generado y recibido. Ejemplos: cortafuegos, redes privadas virtuales (*Virtual Private Network*, VPN), *routers* seguros, etc.
- **Soluciones de seguridad en dispositivos móviles**: protegen las redes inalámbricas y dispositivos móviles, de forma que se minimicen o reduzcan los incidentes de seguridad.

Dentro de las soluciones de control, se incluyen las siguientes:

- **Soluciones de auditoría técnica**: realización de auditorías de sistemas, aplicaciones y datos, determinando posibles fallos de seguridad. Ejemplos: análisis de puertos, auditoría de contraseñas, herramientas de recuperación de datos, etc.
- **Soluciones de certificación normativa**: facilitar el cumplimiento normativo aplicable en materia de seguridad y la obtención de certificados según dichas normativas. Ejemplos: soluciones de gestión de riesgos, los Sistemas de Gestión de Seguridad de la Información (SGSI), los planes y las políticas de seguridad.

- **Soluciones de cumplimiento legal:** facilitar el cumplimiento legal en materia de seguridad de la información. Ejemplos: herramientas de cumplimiento legal, borrado seguro, destrucción documental, etc.
- **Soluciones de control de acceso y autenticación:** gestión de usuarios y datos de identificación en entidades y organismos, políticas de seguridad y control de acceso a los recursos. Ejemplos: control de acceso a la red (NAC), gestión de identidad y autenticación, certificados digitales, firma electrónica, etc.

Por último, dentro del bloque de soluciones de mitigación, encontramos:

- **Soluciones de contingencia y continuidad:** planes de actuación y contingencia, destinados a mitigar el impacto provocado por incidentes de seguridad y puesta en marcha de mecanismos de recuperación. Ejemplos: copias de seguridad, gestión de planes de contingencia, etc.
- **Soluciones de inteligencia de seguridad:** gestión de incidentes de ciberseguridad en cualquiera de sus fases y ayuda en la detección de amenazas de forma rápida, identificar vulnerabilidades, priorizar riesgos y automatizar actividades de cumplimiento normativo. Ejemplos: gestión de eventos de seguridad (SEM), soluciones Big Data, herramientas de monitorización, etc.

2.4. El sector de la ciberseguridad en el mundo

Los informes 2022 Global Threat Intelligence Report del grupo NTT, 2023 Data Breach Investigations Report de Verizon, el Internet Security Threat Report 2023 de Symantec y el CrowdStrike Global Threat Report 2024 identifican las tendencias del sector a nivel mundial en los últimos años y muestran una imagen general de la ciberseguridad en el mundo:

- Según el informe realizado por MarketsAndMarkets en 2023, el mercado global de ciberseguridad se estimaba en torno a los 190.400 millones de dólares. Se proyecta una tasa de crecimiento anual compuesta del 9,4 % hasta 2028, hasta alcanzar ese año un valor de 298.500 millones.
- Las amenazas al sector de comunicaciones se duplicaron debido a la mayor dependencia digital y teletrabajo después del COVID-19.
- Asimismo, las tensiones geopolíticas y disrupciones en las cadenas de suministro han provocado el mismo aumento en los ataques al sector logístico.
- Los ciberataques a la industria tecnológica abarcaron el 21 % del total de amenazas en 2021, seguido por el sector financiero (17 %), manufacturero (14 %) y de la educación (11 %).

- En 2022, los ciberataques a la industria tecnológica abarcan el 25,9 % del total de amenazas, seguido por el sector manufacturero (19 %), educación (11,37 %), sector público (9,1 %) y transporte y distribución (8,12 %).
- En 2022 el porcentaje de ataques a aplicaciones web (42 %) y a aplicaciones específicas (30 %) había aumentado un 5 % respecto a 2020.
- Se registraron 21.957 estados de vulnerabilidad en 2021. En promedio, se detectó una vulnerabilidad nueva cada 24 minutos.
- El total de ataques dirigidos a las 5 principales industrias ha disminuido de un 78 % a un 72 % del total, lo que significa que los autores de amenazas están diversificando sus objetivos y reenfocando ataques hostiles hacia otras industrias y organizaciones.
- Durante 2021 se registró un aumento del 50 % en el *malware* con respecto a 2020 liderado por troyanos y *botnets*. Asimismo, Los troyanos representaron el 65 % del *malware* en 2021, frente al 35 % del año anterior, seguido de las *botnets* (11 %).
- El 24 % de todos los compromisos de respuesta a incidentes en 2021 estaban relacionados con el *ransomware*, un crecimiento del 240 %, frente al 7 % que representaban en 2019.
- El 74 % de los ataques incluyen el elemento humano, con personas implicadas por error, abuso de privilegios, uso de credenciales robadas o ingeniería social.
- La motivación principal de los ataques sigue siendo abrumadoramente financiera, hasta en un 95 % de los casos.

2.5. Clasificación arancelaria

Al tratarse de un servicio, la ciberseguridad encaja en el grupo J62 del código de Clasificación Nacional de Actividades Económicas (CNAE): Programación, consultoría y otras actividades relacionadas con la informática. Dentro de este grupo existen diferentes subgrupos:

- **J620: Programación, consultoría y otras actividades relacionadas con la informática**
 - 6201: Actividades de programación informática
 - 6202: Actividades de consultoría informática
 - 6203: Gestión de recursos informáticos
 - 6209: Otros servicios relacionados con las tecnologías de la información y la informática.

3. Oferta – Análisis de competidores

3.1. El sector de la ciberseguridad en Suiza

Suiza es un estado federal y se caracteriza por tener un gobierno muy descentralizado. La rama ejecutiva se divide en tres: el Consejo Federal, cantones y municipios. El país cuenta con 26 cantones y 2.240 municipios, lo que hace que el reparto de competencias sea complicado. Dada esta división, las competencias concernientes a la ciberseguridad están repartidas entre diferentes instituciones y organismos que deben actuar de forma conjunta.

3.1.1. Legislación

El Consejo Federal suizo publica estrategias y directrices que se aprueban en cuanto surge una necesidad concreta para proteger a la administración federal de los riesgos cibernéticos.

La Ordenanza sobre Transformación Digital e Informática (Verordnung über die digitale Transformation und die Informatik, VDTI), aprobada en noviembre de 2020 y entrado en vigor el 1 de enero de 2021, crea la base jurídica para la organización interdepartamental de la administración federal en materia de transformación digital y gestión de las TIC.

La Ley de Seguridad de la Información (Informationssicherheitsgesetz, ISG), aprobada en diciembre de 2020, y las normas de implementación asociadas entraron en vigor el 1 de enero de 2024. El nuevo Reglamento sobre seguridad de la información (Informationssicherheitsverordnung, ISV) ha sustituido a los dos reglamentos anteriores, el Reglamento sobre riesgos cibernéticos (Cyberrisikenverordnung, CyRV) y el Reglamento sobre protección de la información (Informationsschutzverordnung, ISchV).

La nueva Estrategia Nacional Suiza para la Protección de Ciber riesgos (Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken – NCS) fue aprobada por el Consejo Federal durante su reunión del 5 de abril de 2023 y por los cantones el 13 de abril de 2023. Esta estrategia establece los objetivos y medidas con los que el Gobierno federal y los cantones, junto con la comunidad empresarial y las universidades, pretenden contrarrestar las ciber amenazas. No es una regulación como tal, pero guía a los organismos competentes en sus actuaciones relacionadas con este sector, describe el panorama actual de la ciberseguridad en Suiza, así como los riesgos existentes y dibuja un esquema de cómo defenderse de los mismos. Además, esta estrategia insta a los actores e instituciones competentes a identificar lagunas para proponer los ajustes normativos pertinentes. La NCS define 16 medidas para minimizar los ciber riesgos y potenciar la ciberseguridad englobadas en cuatro campos: prevención, respuesta, continuidad y gestión de crisis, y procesos de soporte (educación, investigación, coordinación internacional y propuestas de ley).

Aparte de la NCS, el sector de la ciberseguridad cuenta con las siguientes leyes y estrategias:

- **Estrategia Digital Switzerland:** presenta un análisis de efectos de la estrategia de ciberseguridad en la que se incluye un examen de la cooperación internacional, sobre todo en relación con la red y la seguridad de la información relacionada con la UE.
- **Ley Federal de Protección de Datos** ([*Bundesgesetz über den Datenschutz – DSG*³](#)).
- **Ley Federal de Telecomunicaciones** ([*Fernmeldegesetzes - FMG*](#)).
- **Código Penal de Suiza** (*Schweizerisches Strafgesetzbuch*).
- **Reglamento General de Protección de Datos** de la UE (*General Data Protection Regulation - GDPR*): Suiza y las empresas suizas tendrán que adoptar esta legislación a partir de mayo de 2018 si tratan y o están en contacto con datos de particulares y empresas europeos que están protegidos por la GDPR.

3.1.2. Instituciones

A continuación, se muestra un esquema de las organizaciones oficiales a tener en cuenta en este sector:

- **Centro de Análisis y Reporte para la Protección de Datos** (Melde- und Analysestelle Informationssicherung – **MELANI**): Era hasta 2024 el principal centro de información y análisis del sistema de ciberseguridad del gobierno suizo. El centro es ahora parte del Centro Nacional de Ciberseguridad de Suiza (NCSC).
- **Centro Nacional de Ciberseguridad de Suiza (NCSC)**: Creado el 1 de enero de 2024 como una nueva oficina federal dependiente del Ministerio de Defensa, Protección Civil y Deportes, su presupuesto asciende a 14,5 millones (16,2 millones de dólares) y entre sus principales funciones se encuentran:
 - Aconsejar y ayudar a más de 140 operadores de infraestructuras críticas en relación con ciber incidentes y amenazas;
 - Evaluar incidentes y remitir información relacionada con ciberataques;
 - Coordinar el intercambio de datos de ciberseguridad entre empresas públicas y privadas, operadores de infraestructuras críticas y proveedores de servicios y sistemas.

La Ciber Estrategia Nacional (NCS) se basa en las actividades anteriores y especifica cómo deben ampliarse, desarrollarse y complementarse para alcanzar los objetivos estratégicos. También se describen las prioridades a la hora de aplicar las medidas y los agentes implicados.

³ Todas las disposiciones legales aparecen al menos en tres idiomas: alemán, francés e italiano

Las medidas que se describen a continuación se aplican para alcanzar los cinco objetivos estratégicos establecidos por la NCSC:

Objetivos estratégicos	Medidas
Empoderamiento	M1: Educación, investigación e innovación en ciberseguridad M2: Sensibilización M3: Actuación ante amenazas M4: Análisis de tendencias, riesgos y dependencias
Servicios e infraestructuras digitales seguros	M5: Detección y prevención de vulnerabilidades M6: Resiliencia, normalización y regulación M7: Ampliación de la cooperación entre las autoridades
Detección, prevención, gestión y defensa eficaces contra los ciberataques	M8: Gestión de incidentes M9: Atribución M10: Gestión de crisis M11: Ciberdefensa
Lucha y persecuciones eficaces de la ciberdelincuencia	M12: Ampliación de la cooperación entre fiscalías M13: Resumen de casos M14: Formación de los fiscales
Papel protagonista en la cooperación internacional	M15: Fortalecimiento de la Ginebra digital internacional M16: Normas internacionales en el ciberespacio M17: Cooperación bilateral con socios estratégicos y centros de competencia internacionales

- **Oficina Federal de Protección Civil** (Bundesamt für Bevölkerungsschutz – **BABS**): Se encarga de coordinar la implementación de la NCS por el Gobierno Federal, los cantones y los municipios.

Organización de Apoyo de las Fuerzas Armadas (Führungsunterstützungsbasis – **FUB**): FUB está a cargo de la ciberseguridad en las Fuerzas Armadas suizas. Esta organización dispone del MilCERT, que colabora con GovCERT.

- **Organizaciones sectoriales**: cada sector tiene una asociación u organización de la cual depende la implementación de legislación o medidas aprobadas o aconsejadas por el Gobierno Federal. Por ejemplo, una de las encargadas es la Autoridad Supervisora del Mercado Financiero Suizo (Eidgenössische Finanzmarktaufsicht – **FINMA**) responsable de los sistemas que controlan los mercados financieros nacionales. El sector financiero es uno de los más controlados, pues es un pilar fundamental de la economía del país. No obstante, algunos sectores minoritarios no gozan de las suficientes medidas de ciberseguridad.

3.1.3. Principales ataques contra la ciberseguridad en Suiza

En 2022, los ciberataques a la industria tecnológica abarcaron el 25,9 % del total de amenazas, seguido por el sector manufacturero (19 %) educación (11,4 %), sector público (9,1 %) y transporte y distribución (8,1 %). En cuanto a ataques, los más comunes son de ciber espionaje, *ransomware* y de robo de identidad.

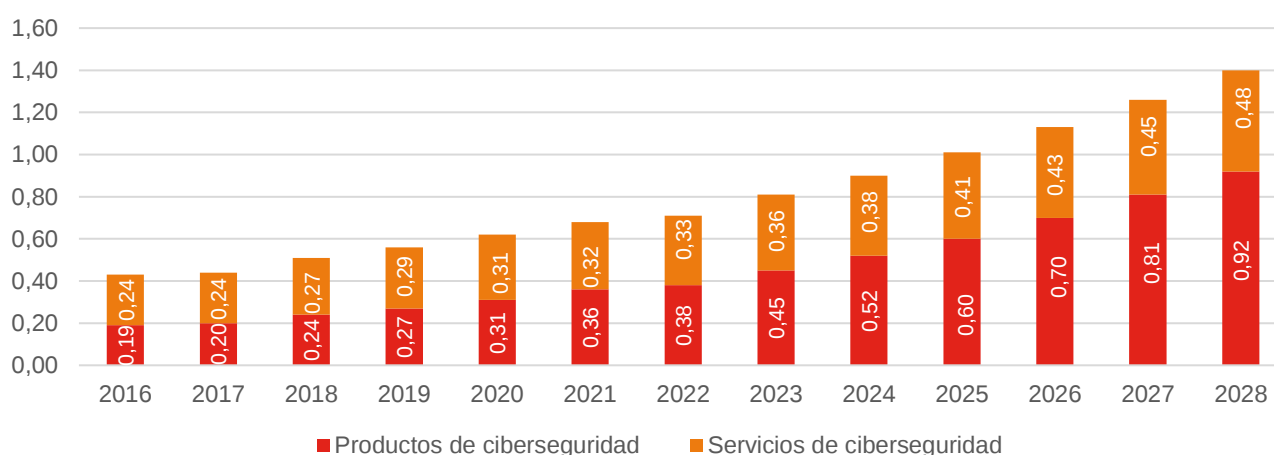
Según el Índice de Ciberseguridad Global 2020 (ICG) de la Unión Internacional de Telecomunicaciones, Suiza se sitúa en el puesto 42.º como país más comprometido con la ciberseguridad, detrás de países como Estonia (3.º), Singapur (4.º) o España (4.º). Según el ICG, Suiza destaca por las medidas técnicas y cooperativas tomadas. No obstante, como puntos débiles en el grado de compromiso de Suiza con la ciberseguridad, el informe destaca que la estrategia suiza de ciberseguridad no es práctica, que no existe una cooperación estable entre actores ni unos mecanismos adecuados para incentivar las acciones de ciberseguridad.

3.1.4. Tamaño del mercado

Según Switzerland Global Enterprise, en 2023 los ingresos domésticos en el sector fueron aproximadamente 808 millones de dólares. Como se puede observar en el Gráfico 1, a partir de 2021 los productos de ciberseguridad han sido los que más han venido contribuyendo a los ingresos del sector. Se estima que el crecimiento de los productos de ciberseguridad sobrepasará al de los servicios en el horizonte entre 2022 y 2028. En cualquier caso, los servicios también seguirán una tendencia ascendente en cuanto a volumen de facturación.

GRÁFICO 1. MERCADO DE LA CIBERSEGURIDAD EN SUIZA. EVOLUCIÓN Y PROYECCIÓN DE LOS INGRESOS POR SEGMENTO

En miles de millones de dólares



Fuente: Statista 2023.

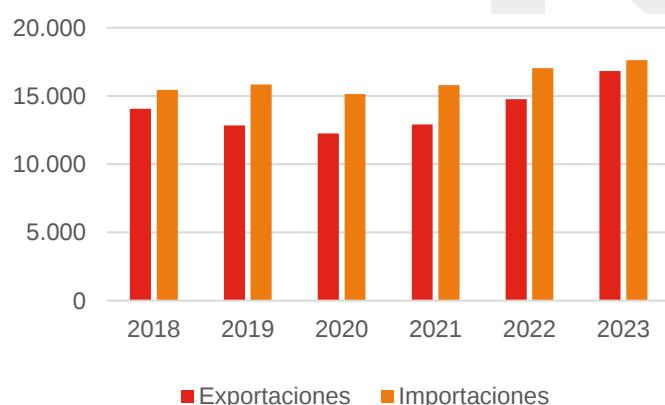
La ciberseguridad y los productos y servicios relacionados son parte del mercado de las TIC. En 2021 el mercado TIC de Suiza contribuyó al PIB del país en alrededor de 40.173 MCHF. Teniendo en cuenta que en ese año Experton Group estima que el mercado de la ciberseguridad alcanzó los 680 MCHF, el peso del segmento de la ciberseguridad en el mercado TIC fue del 1,7 %.

3.1.5. Comercio exterior

En Suiza, los datos oficiales de las exportaciones y las importaciones no presentan un apartado específico sobre ciberseguridad, por lo que su comercio debe estudiarse mediante las cifras referentes a los servicios TIC. Como se muestra en el Gráfico 2 y la Tabla 2, la balanza comercial suiza referente a las TIC es deficitaria. El volumen de importaciones para los años 2019-2022 fue bastante superior a las exportaciones. En 2022, la importación de servicios TIC experimentó una subida de casi un 15 % con respecto a 2021. Por otro lado, las exportaciones aumentaron un 30 % entre 2021 y 2023.

GRÁFICO 2. PRODUCTOS Y SERVICIOS TIC: EXPORTACIONES E IMPORTACIONES (2018-2023). MILLONES DE CHF Y TABLA 2. PRODUCTOS Y SERVICIOS TIC: EXPORTACIONES E IMPORTACIONES (2018-2023).

En millones de francos suizos



Productos y servicios TIC

Año	Exportaciones	Importaciones
2018	14.068	15.445
2019	12.830	15.845
2020	12.260	15.127
2021	12.915	15.794
2022	14.773	17.048
2023	16.831	17.615

Fuente: Banco Nacional Suizo

En cuanto a proveedores, los países que más exportan a Suiza son **Estados Unidos, Alemania y Reino Unido**, seguidos a cierta distancia de India y Países Bajos, como se puede ver en el Gráfico 4 y la Tabla 3. Estados Unidos viene siendo de forma consistente el país que más productos y servicios TIC exporta a Suiza, alcanzando una cifra superior a los 4.000 MCHF de exportaciones a Suiza en 2023.

En términos de evolución, los países que han aumentado en mayor medida sus exportaciones TIC en los últimos años son **Irlanda** que ha incrementado un 174 % (llegando a las 1.294 MCHF en 2023) y **Países Bajos** (pasando de exportar 414,4 MCHF en 2019 a 1.039 MCHF en 2023).

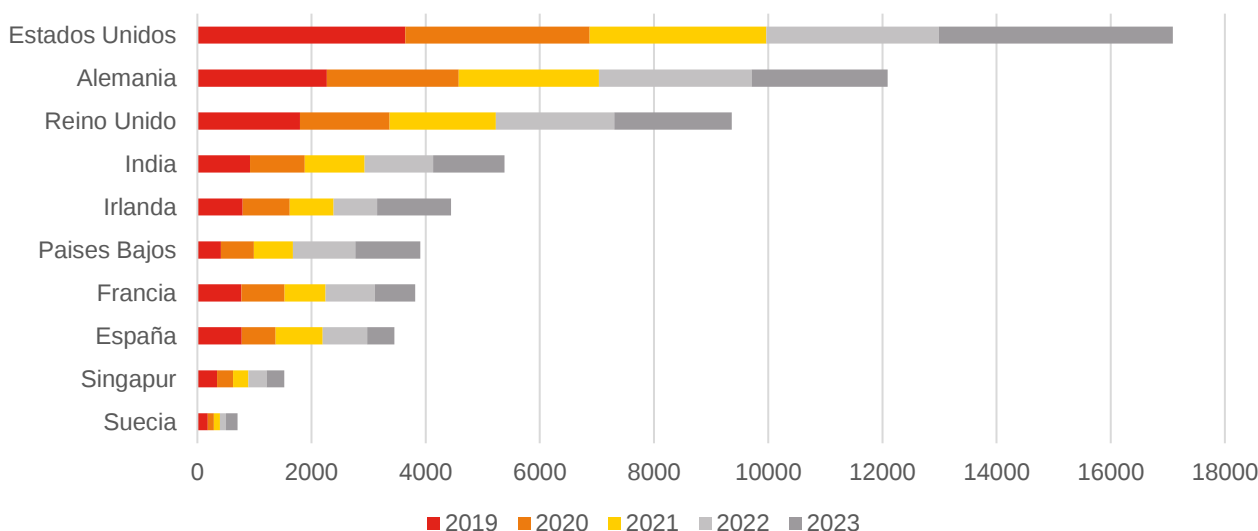
Por el contrario, los países que han sufrido una **disminución** de sus exportaciones a Suiza son **España** (de 774,5 MCHF en 2019 a 477 MCHF en 2023) y **Singapur** (de 344 MCHF en 2019 a 308 MCHF en 2023).

Otros actores importantes son; Reino Unido, cuyas exportaciones se han mantenido estables en los últimos años, recuperándose de la bajada en 2020; Alemania, que experimentó un gran aumento de sus exportaciones a Suiza entre 2019 y 2022, pero durante el último año muestra una tendencia descendente; y India, que ha incrementado sus exportaciones a Suiza entre 2019 y 2023 un 35,5 % hasta alcanzar 1.250 MCHF.

En cuanto a las importaciones suizas de España, la partida de servicios TIC ha sido la más dinámica de nuestro comercio bilateral con Suiza en los últimos años, habiéndose casi cuadruplicado las exportaciones españolas a Suiza bajo dicho concepto entre 2014 y 2021, pasando de 216 a 824 millones de francos. Aunque en los últimos dos años estas cifras han caído, hasta exportaciones por 477 millones de francos.

GRÁFICO 3. PAÍSES EXPORTADORES DE SERVICIOS TIC A SUIZA (2018-2022).

En millones de francos suizos

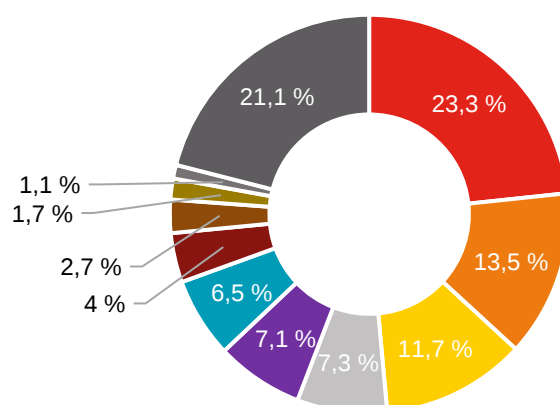


Fuente: Banco Nacional Suizo.

TABLA 3. IMPORTACIONES SUIZAS DE SERVICIOS TIC
En millones de francos suizos

Principales países de importación	2019	2020	2021	2022	2023	% de variación 2019-2023
Estados Unidos	3.642,9	3.231,5	3.093,6	3.017,5	4.098,6	12,5
Alemania	2.266,0	2.312,5	2.454,4	2.674,2	2.382,5	5,1
Reino Unido	1.799,8	1.569,2	1.860,8	2.073,3	2.058,9	14,4
Irlanda	791,5	827,5	768,3	762,7	1.294,4	63,5
India	923,0	960,0	1.049,0	1.198,0	1.250,3	35,5
Países Bajos	414,5	574,3	686,7	1.089,8	1.139,0	174,8
Francia	769,7	757,0	719,2	866,0	705,5	-8,3
España	774,5	595,7	824,1	782,8	477,0	-38,4
Singapur	344,0	280,0	270,0	318,0	308,1	-10,4
Suecia	185,0	102,1	109,4	107,0	200,3	8,3
Resto	2.134,3	3.916,8	3.958,8	4.154,2	3.700,0	73,4
Total	15.845,0	15.126,6	15.794,3	17.047,5	17.614,6	11,2

Fuente: Banco Nacional Suizo.

GRÁFICO 4. DISTRIBUCIÓN DE LAS IMPORTACIONES POR PAÍSES DE PROCEDENCIA EN 2023
En porcentaje


■ EE.UU ■ Alemania ■ Reino Unido ■ Irlanda ■ India ■ Países Bajos ■ Francia ■ España ■ Singapur ■ Suecia ■ Otros

Fuente: Banco Nacional Suizo

En relación con las exportaciones suizas de productos y servicios TIC, destaca que su mayor cliente es Alemania, con un volumen mantenido entre 2018 y 2022 de en torno a 2.600 MCHF, pero repuntando un 25 % de 2022 a 2023 alcanzando los 3.292 MCHF. Asimismo, en los últimos las exportaciones suizas a Estados Unidos años han incrementado de forma similar a las alemanas (de 1.637 MCHF en 2019 a 2.518 MCHF en 2023). Irlanda ha sido con diferencia el país con mejor evolución, experimentando un crecimiento del 132 % entre 2019 y 2023 (de 261,5 MCHF en 2019 a 607,4 MCHF en 2023) siendo el quinto destino principal de las exportaciones TIC suizas.

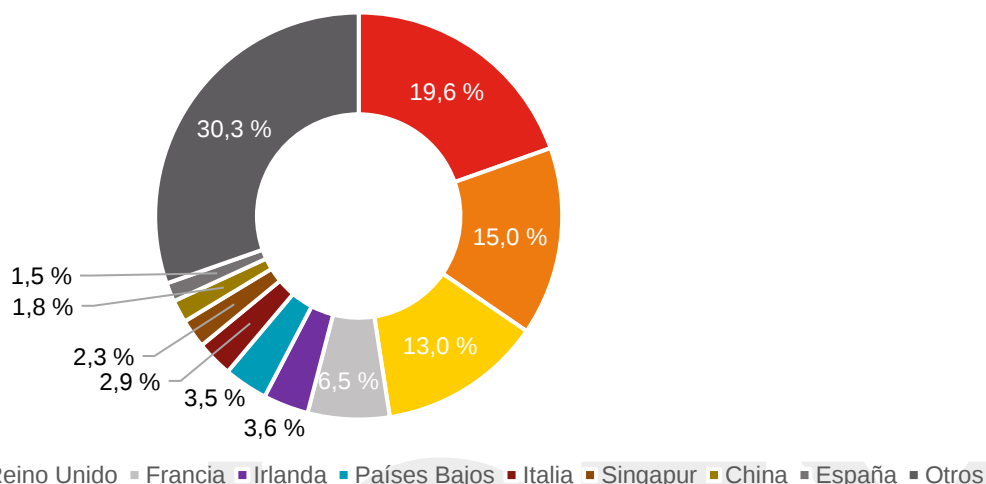
En cuanto a las exportaciones suizas a España, han caído de 360 MCHF en 2019 a 247 MCHF en 2023 (-31 %). Suiza importa más desde España de lo que exporta a España (Tabla 4), lo que viene arrojando un superávit bilateral en esta partida a favor de España, el cual alcanzó su máximo valor (564 MCHF) en 2021, pero ha caído en 2023 hasta 230 MCHF.

TABLA 4. EXPORTACIONES SUIZAS DE SERVICIOS TIC
En millones de francos suizos

Principales países de importación	2019	2020	2021	2022	2023	% de variación 2019-2023
Alemania	2.096,8	1.815,5	2.193,1	2.632,6	3.292,5	57,0
Estados Unidos	1.637,9	1.676,9	1.696,9	2.026,7	2.518,1	53,7
Reino Unido	1.478,7	1.387,7	1.289,6	1.328,9	2.187,3	47,9
Francia	928,1	873,5	859,5	948,1	1.100,3	18,6
Irlanda	261,5	221,5	266,7	564,0	607,4	132,3
Países Bajos	508,5	473,4	556,2	573,6	583,0	14,7
Italia	455,2	455,9	445,8	435,9	494,7	8,7
Singapur	204,9	191,0	211,7	328,3	388,0	89,4
China	628,3	645,6	671,0	736,6	295,9	-52,9
España	360,7	305,3	259,8	242,9	246,8	-32,7
Resto	4.116,1	4.044,3	4.311,5	5.048,1	5.116,8	24,3
Total	12.829,9	12.260,1	12.914,7	14.773,4	16.830,8	31,2

Fuente: Banco Nacional Suizo.

GRAFICO 5. DISTRIBUCIÓN DE LAS EXPORTACIONES POR PAÍSES DE DESTINO EN 2023
En porcentaje

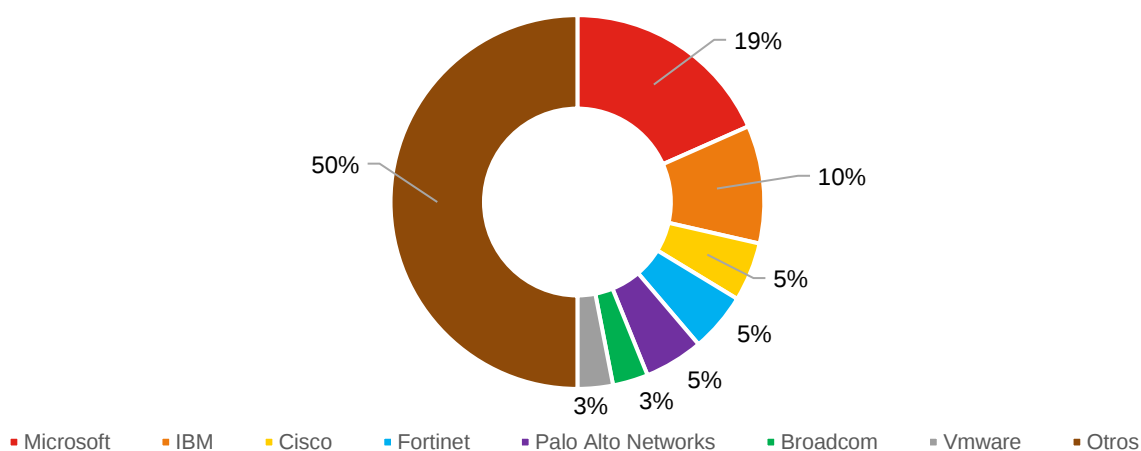


Fuente: Banco Nacional Suizo.

3.2. Empresas de ciberseguridad en Suiza

Un gran volumen de productos y servicios de ciberseguridad que se comercializan en Suiza son de empresas multinacionales ya consolidadas, como se aprecia en el siguiente gráfico sobre las principales empresas de ciberseguridad presentes en Suiza.

GRÁFICO 6. CUOTA DE MERCADO DE LAS PRINCIPALES EMPRESAS EN SUIZA
En porcentaje



Fuente: Statista 2023.

3.2.1. Empresas internacionales

Las empresas extranjeras presentes en Suiza que ofrecen servicios de ciberseguridad no se dedican en exclusiva a este sector, sino que han venido desarrollando esta parte de su negocio debido a las necesidades de empresas y particulares.

MICROSOFT

Fundado en 1975 y con sede en Redmond, Washington, Microsoft opera en 190 países y tiene más de 160.000 empleados. En 2023 obtuvo un beneficio de 88.000 millones de dólares. En Suiza ha desplegado una larga lista de iniciativas en el plano de la ciberseguridad, habiendo abierto en 2022 una nueva sede para su filial suiza en el aeropuerto de Zúrich en aras de reforzar su compromiso en continuidad de negocio, protección de datos y seguridad en la nube e iniciado junto a Adecco y Campbell & Jones un nuevo programa de aprendizaje Skills for Switzerland para que personas de todo tipo de especialidades participen en la formación digital. Entre su ofertamás destacable se encuentran los servicios de seguridad en la nube y los productos Microsoft Sentinel y Microsoft Defender.



ATOS

Fundada en 1988 en Francia, Atos se especializa en servicios *high-tech*, de comunicación, consultoría, *outsourcing*, *cloud*, *big data* y ciberseguridad. En 2023, sus ingresos fueron de 11.000 Mill. USD. Está presente en 72 países y emplea a 105.000 personas. Su actividad la diversifica mediante varias marcas: Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify y Worldline. En cuanto a ciberseguridad, Atos provee los siguientes productos y servicios: SOCs, Evidian (*software* desarrollado por Atos de gestión de acceso e identidad líder en Europa), y *Application Resource Islands* (ARI) para la protección de información crítica.



CISCO

Esta empresa estadounidense fundada en 1984 obtuvo unos ingresos de 58.000 Mill. USD en 2023. Cisco emplea a más de 57.000 personas y está presente en 73 países. Entre sus productos y servicios destacan los servicios de *cloud*, infraestructuras de software propio, hardware, servidores, centros de datos, infraestructuras de hiperconvergencia, soluciones de internet de las cosas, movilidad o seguridad. En relación con los servicios de seguridad, Cisco ofrece soluciones de seguridad de web, *firewalls*, gestión de la seguridad, sistemas de prevención de intrusiones, seguridad *endpoint*, VPN seguras, etc.





IBM

Fundada en 1911 en Estados Unidos, IBM comercializa productos y servicios relacionados con las TIC. Entre sus productos destaca Watson, una herramienta propia de inteligencia artificial que IBM enfoca al mundo empresarial. En 2022, la empresa registró un beneficio de 61.000 MEUR y empleó a 380.000 trabajadores en 170 países. En cuanto a ciberseguridad, IBM ofrece servicios de protección de dispositivos móviles, protección contra fraude y de datos, *forensics*, *virtual patching*, análisis de *malware* y de *endpoints*, y seguridad de aplicaciones e identidad y acceso.



FORTINET

Fortinet es una empresa multinacional de Estados Unidos con sede en Sunnyvale, California. Se dedica al desarrollo y la comercialización de software, dispositivos y servicios de ciberseguridad, como firewalls, antivirus, prevención de intrusiones y seguridad en dispositivos de usuario, entre otros. Cuenta con más de 13.000 empleados y unos ingresos en 2023 de 5.740 millones de dólares. Su filial suiza se encuentra en Zúrich.



3.2.2. Empresas nacionales

ELCA

ELCA es una empresa suiza de tecnología de la información y consultoría, fundada en 1968. Especializada en servicios de desarrollo de *software* a medida, consultoría TI, gestión de proyectos y soluciones digitales para una amplia gama de industrias, incluyendo banca, seguros, salud, telecomunicaciones y sector público. En 2023 empleaba a más de 1.700 trabajadores, un 20 % más que en 2022, y facturó 328 millones de francos suizos.



KUDELSKI

Fundada en 1951 en Lausana, Kudelski ofrece soluciones de [seguridad informática](#), con aplicación en televisión digital, acceso a infraestructuras públicas, internet de las cosas y ciberseguridad. Comercializa sus productos y servicios en América, Europa, y Oriente Medio, en esta última región por medio de su marca Nagra. En 2023, obtuvo unos ingresos de 761 MUSD y contaba con 3.152 empleados. En el campo de la ciberseguridad, Kudelski ofrece consultoría tecnológica y productos y servicios para gestión de riesgos, amenazas y vulnerabilidades, así como respuesta a incidencias y ciber resiliencia.



INFOGUARD

Esta empresa suiza con sede en Zug y oficinas en Berna se fundó en 1988 y emplea a 100 especialistas en seguridad. En 2023, facturó más de 66 millones CHF. Entre sus clientes se encuentran bancos, aseguradoras, empresas industriales, de energía, sanitarias y proveedores de servicios. Ofrece servicios de *cloud* y cuenta con un Centro de Operaciones de Seguridad (SOC) para sus clientes, *forensics*, análisis de vulnerabilidades, monitorización, y el Infoguard *Blue Team*, un grupo de expertos en ciberseguridad.



ERGON

Fundada en 1984 y una de las empresas de servicios informáticos más destacadas de Suiza junto a ELCA, es proveedora de productos/servicios de ciberseguridad a grandes clientes y mayoristas del sector.



RUAG

Fundada en 1998, RUAG es una empresa tecnológica con departamentos especializados en sector espacial, aviación y defensa. Tiene su sede en Berna, está presente en 12 países y en 2023 facturó 620 MCHF. Dentro de su división de defensa, RUAG desarrolla soluciones de ciberseguridad bajo su marca Clearswift.

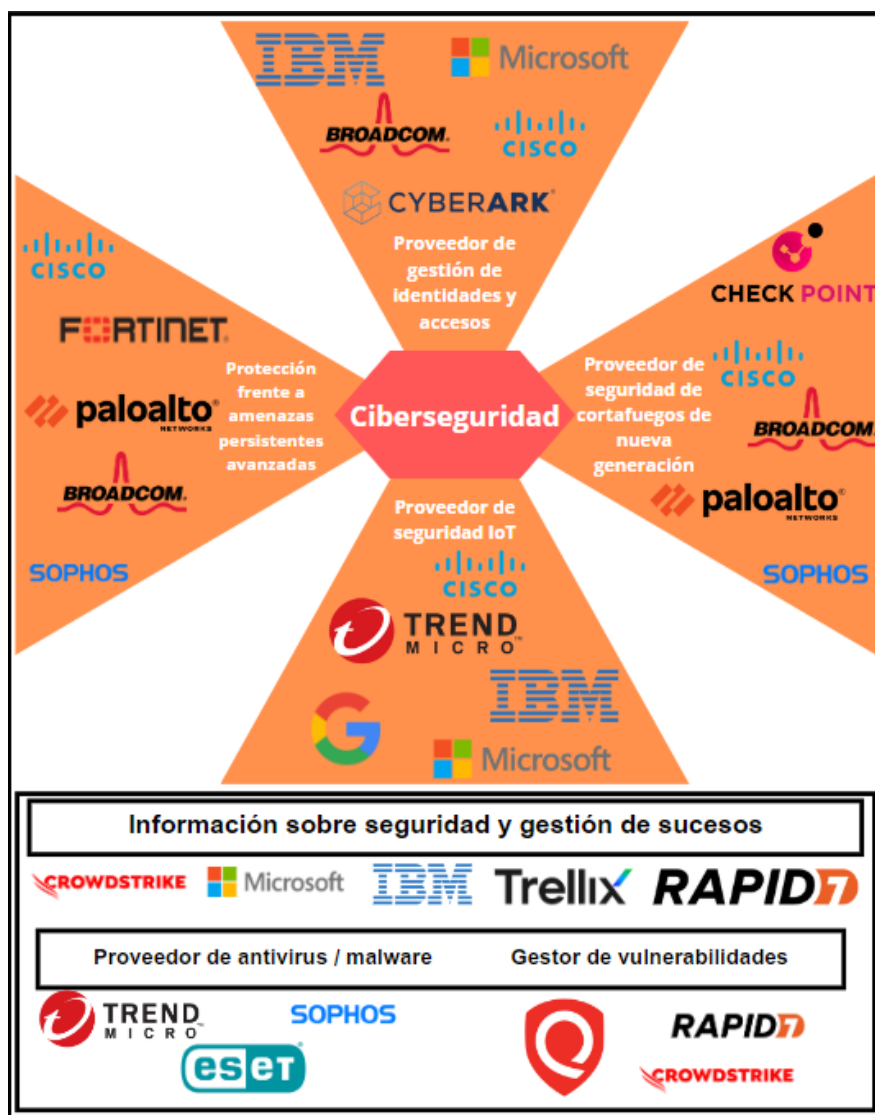


A continuación, se muestra un listado de otras empresas que ofrecen productos y servicios de ciberseguridad en Suiza.

Immuniweb	Nozomi Networks	Nexthink	Black Box	Cryptix AG
Silent Circle	Agam Security	Biowatch	Seargin	Akana
Cyberhaven	Futurae	eSkills	Dreamlab Technologies	Kaduu AG
Exeon	Infoteam	Hacknowledge	Lucy Security	Arcondis Group
Security Guardian	Inpher	Kyos	Artmotion AG	KMU Informatik Support
Net4all	Nextprivacy	OneVissage	Bogli ICT	Astarios
Pryv	Psynd	ScanTrust	Rocketlab	Cipherspace

Fuente: [The Manifest 2024](#).

IMAGEN 2. COMPENDIO DE EMPRESAS INTERNACIONALES DE CIBERSEGURIDAD



Fuente: Markets and Markets.

3.2.3. Empresas suizas inversoras en el sector TIC en España

Como se ha indicado anteriormente, la partida más dinámica de la balanza de pagos bilateral entre España y Suiza ha sido en los últimos años la de las exportaciones españolas de servicios TIC, las cuales se cuadruplicaron entre 2014 y 2021. Esta evolución es reflejo de la creciente opción de grandes empresas suizas por centralizar en sus filiales en España la gestión TIC o el desarrollo de software para el conjunto del grupo o de empresas suizas de todos los tamaños por externalizar dichos servicios con empresas españolas.

A continuación, se refleja el listado de empresas suizas que han realizado inversiones TIC de relieves en los últimos años.

F. Hoffman- La Roche Ltd	Axpo Holding AG	Arxada AG	FunPlus International AG	Galderma Group	AXA Investment Managers
ABB Asea Brown Boveri Ltd	Ypsomed Holding	ERNI Schweiz AG	Bystronic Sales AG	Zurich Insurance Group	Nestlé S.A
Also Schweiz AG	Pix4D SA	Holcim Ltd	Avaloq Group	Yokoy Group AG	Kudelski Group
WISeKEY	ELCA	Sandsix Switzerland	LGT Private Banking	Swiss Reinsurance Company	

De entre todas estas inversiones suizas TIC en España se destacan a continuación las de ciberseguridad.

Entidad de Suiza	Swiss Reinsurance Company Ltd
Sede local (España)	Swiss Re International S. E.
Dirección	Torre Europa Paseo de la Castellana 95 Planta 11 & 14 28046
Provincia	Madrid
Ciudad	Madrid
Relación	Centro Tecnológico (Datos y Ciberseguridad)
Sector	Seguros
Subsector de inversión	Creación de un Hub Tecnológico en Madrid
Referencia	Swiss Recontratará 150 empleados en Madrid para crear un 'hub' tecnológico (elconfidencial.com)

Entidad de Suiza	Kudelski Group
Sede local (España)	[Aún no constituida]
Dirección	[Aún no constituida]
Provincia	Madrid
Ciudad	Madrid
Relación	Cyber Fusion Center (CFC)
Sector	Seguridad Informática
Subsector de inversión	Ciberseguridad
Referencia	Kudelski Security Launches Cyber Fusion Center in Spain to Address Rising Cyber Threats

Entidad de Suiza	WISeKEY
Sede local (España)	WISeKEY Spain SL
Dirección	C. Jose Ortega Y Gasset 28, 28006
Provincia	Madrid
Ciudad	Madrid
Relación	Implantación en la Región de Murcia de un centro de diseño y personalización de chips de altas prestaciones en ciberseguridad
Sector	Seguridad Informática
Subsector de inversión	Ciberseguridad
Referencia	WISeKey and Odin Spearhead the Establishment of an Innovative Semiconductor Center in Murcia; The Project Foresees a Financing of €60M for its Execution - WISeKey

Entidad de Suiza	ELCA
Sede local (España)	ELCA Spain
Dirección	C. del Marqués de la Ensenada, 2, Genil, 28004
Provincia	Madrid y Granada
Ciudad	Madrid y Granada
Relación	Apertura de dos filiales en España
Sector	Soluciones Empresariales y Tecnológicas
Subsector de inversión	Consultoría de IT, Desarrollo y Mantenimiento de software e Integración de sistemas de IT
Referencia	ELCA Spain

3.2.4. Asociaciones nacionales de ciberseguridad

A continuación, se ofrece un listado de asociaciones nacionales de seguridad en internet y de software suizo:

- **[Digitalswitzerland](#)**: Es una iniciativa intersectorial suiza cuyo objetivo es fortalecer y convertir a Suiza en una nación digital líder. Bajo el paraguas de Digitalswitzerland, más de 170 organizaciones, compuestas por miembros de asociaciones y socios de fundaciones políticamente neutrales, colaboran de forma transversal para lograr este objetivo.
- **[Swiss made software](#)**: Asociación suiza que reúne a más de 400 empresas que distribuyen 470 productos y servicios con sello “Swiss made software”.
- **[Information Security Society Switzerland – ISSS](#)**: La ISSS es la asociación profesional líder en seguridad de las TIC en Suiza y actualmente cuenta con más de 1.100 profesionales de la seguridad y personas interesadas en la seguridad de los negocios, la administración y la ciencia.
- **[ICTSwitzerland](#)**: Organización suiza para la industria de las TIC. Formada por 29 empresas y grandes y medianas 21 asociaciones, ICTSwitzerland representa sus intereses ante el público, las autoridades y otras asociaciones. Su objetivo principal es promover y desarrollar las tecnologías digitales, así como la educación y la formación de especialistas en TIC.
- **[Security Interest Group Switzerland](#)** – SIGS: Organización independiente peer- to- peer dedicada a ayudar a los profesionales de seguridad de la información en temas relacionados con la gestión de riesgos de TI, privacidad y cumplimiento normativo.
- **[Cyber-safe.ch](#)**: La asociación para la certificación en ciberseguridad se estableció en 2018 con el objetivo de promover la gestión responsable de la ciberseguridad en pequeñas y medianas empresas en Suiza. En particular, mediante el desarrollo y la provisión de un sello de calidad.



- **Foro Suizo sobre Protección de Datos:** apoya activamente el debate sobre la protección de datos entre las partes interesadas de todas las disciplinas de la empresa, la administración pública y la ciencia, proporciona información sobre la protección y la seguridad de los datos, ofrece formación y educación adicional en el ámbito de la protección y la seguridad de los datos, mantiene contactos con organizaciones con los mismos objetivos.

icex

4. Demanda

4.1. Factores de la demanda

Con los datos más recientes disponibles, Suiza contaba en 2022 con 8,81 millones de habitantes, un PIB de 781.500 MCHF y una renta per cápita de 88.706 CHF, la cuarta más elevada del mundo. Según la Oficina Federal de Estadísticas de Suiza, en 2021, el 93 % de la población nacional tenía acceso a internet, con aproximadamente 865 ordenadores por cada 1000 habitantes. Hoy en día, Suiza es el líder mundial en distribución de ordenadores per cápita.

De acuerdo con el informe PandaLabs Annual Report 2017, de una lista de países con mayores probabilidades de ser atacados, Suiza se posiciona en la posición 89 entre 100 países. Este dato induce a pensar que Suiza no es un país que demanda grandes volúmenes de productos y servicios de ciberseguridad. No obstante, se debe tener en cuenta el gran número de empresas del sector bancario localizadas en el país helvético y las grandes medidas de protección que deben presentar para asegurar tanto su operativa y datos como los de sus clientes. De hecho, los datos del primer cuatrimestre de 2023 muestran un ascenso muy pronunciado en las incidencias de ciberseguridad, con más de 13.000 ataques reportados.

Según la NCSC suiza, el número total de denuncias aumentó en 2023 un 30 % con respecto a 2022. Con casi 50.000 denuncias en 2023 frente a 34.527 en 2022. El aumento en cifras absolutas fue ligeramente superior al de 2021, con 15.000 denuncias. El nuevo aumento se debió principalmente al incremento de fenómenos como las ofertas de trabajo fraudulentas y las llamadas telefónicas falsas que dicen ser de la policía. La proporción entre las denuncias del público en general (88 %) y las de empresas, asociaciones y autoridades (12 %) se mantuvo estable. Los delitos de fraude más frecuentemente denunciados por las empresas experimentaron un aumento en los fenómenos de fraude de CEO (2023: 484; 2022: 116) y fraude de manipulación de facturas (2023: 118; 2022: 36). También aumentaron las denuncias relativas a ataques DDoS (2023: 40; 2022: 24). El número de informes sobre ataques de *ransomware* a empresas se mantuvo estable.

A continuación, se muestran diferentes resultados de encuestas realizadas a empresas suizas como parte de informes acerca de la ciberseguridad en Suiza.

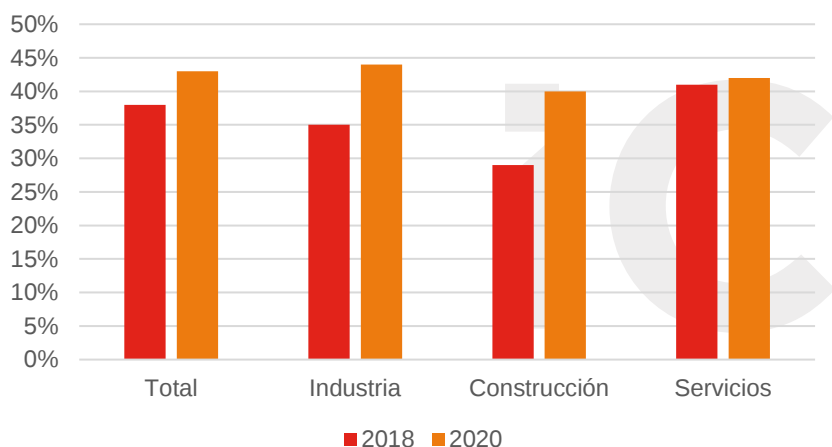
- Según el informe Clarity on Cybersecurity de KPMG, el 88 % de las empresas encuestadas sufrieron un ataque en 2018. Las principales consecuencias de los ataques fueron la interrupción de los procesos vigentes (42 %), daño en la reputación (25 %), pérdidas financieras (75 %), exposición de información confidencial de la empresa (33 %) y de los clientes (27 %). Tan solo el 28 % de las empresas encuestadas tenían una póliza de ciberseguridad. El 64 % de las empresas no contratan un seguro por su elevado precio y por su limitada cobertura.

- Según el Instituto Económico de Suiza (KOF), el coste de reparación de los ataques sigue en aumento. Cuando se producen problemas de seguridad, las empresas parecen sufrir más con el paso del tiempo. En el conjunto de la economía, en 2019 y 2020 alrededor del 16 % de las empresas informaron de un nivel medio a alto de costes de reparación tras un problema de seguridad. Esta proporción ha aumentado desde el período más reciente de referencia en 2017 y 2018. Todas las categorías muestran un aumento en el coste de reparación de daños tras un problema de seguridad. Por tanto, debe seguir dándose gran importancia a la ampliación de la protección de la infraestructura digital.
- De acuerdo con EY Global Information Security Survey 2021, el 43 % de las empresas encuestadas sostuvieron que nunca habían estado tan preocupadas con su habilidad de gestionar ciberataques y un 68 % habían planteado enormes inversiones en ciberseguridad en 2022. Además, el 49 % no tenían capacidades de identificar vulnerabilidades (o las que tenían era insuficiente). Un 37 % afirmaba que no tener un sistema de protección correcto era su mayor vulnerabilidad, un 64 % creía que la falta de formación en seguridad por parte de los empleados era un riesgo importante y un 38 % veía la pérdida de un dispositivo móvil un alto riesgo relacionado con la pérdida de datos. En cuanto a gasto en sistemas de seguridad, el 36 % admiten que es cuestión de tiempo que sufran un ciberataque y que podría haber sido evitado con una mayor inversión en sistemas de ciberseguridad.
- En cuanto a SwissVR Monitor II de 2017, el 91 % de las empresas del sector financiero encuestadas consideran que la ciberseguridad es de vital importancia para el desarrollo de sus actividades (83 % de las empresas químicas, 79 % de las empresas de comunicación y 77 % de las empresas proveedoras de servicios). Sólo el 35 % del total de las empresas preguntadas disponen de una estrategia de ciberseguridad clara y un 28 % no disponen de ella. Casi el 40 % de las encuestadas no cree que la ciberseguridad sea una prioridad.
- Aprovechando las épocas festivas donde los *e-commerce* frecuentemente ganan importancia, los ciberdelincuentes ven en las fiestas la oportunidad perfecta para cometer ataques. Por ejemplo, los ataques de *ransomware* aumentan un 30 % durante las fiestas en comparación con los meses normales.

4.1.1. Empresas e infraestructuras críticas suizas: demanda de productos y servicios

Una vez se tiene una imagen general de las vulnerabilidades, el siguiente paso es saber en qué productos y servicios relacionados con la ciberseguridad invierten las empresas y las instituciones gubernamentales. Como se puede observar en el Gráfico 7, con datos del instituto de previsiones de coyuntura económica de la universidad politécnica de Zúrich (KOF), se aprecia que menos de la mitad de las empresas suizas invierten en ciberseguridad y que el sector servicios ha venido siendo el que más ha invertido en el mismo, aunque superado recientemente por la industria.

GRÁFICO 7. PORCENTAJE DE EMPRESAS SUIZAS CON GASTO EN PRODUCTOS Y SERVICIOS DE CIBERSEGURIDAD POR SECTOR ENTRE 2018 Y 2020

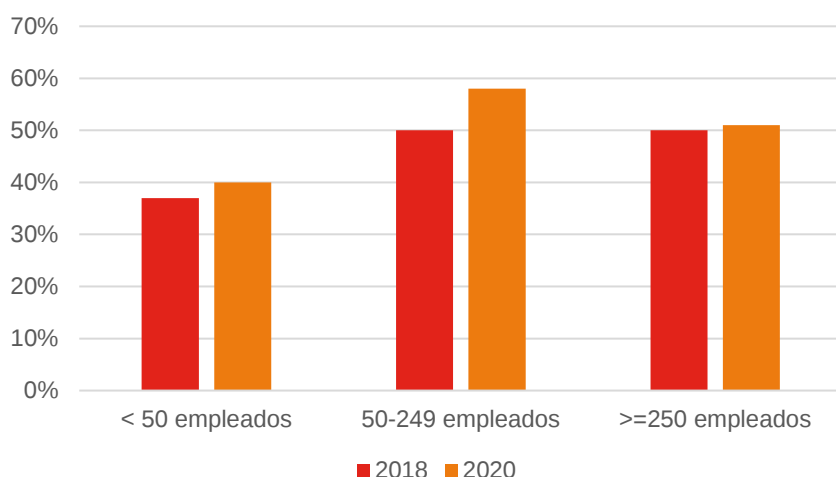


Fuente: KOF (2023).

Muchas empresas contratan seguros para reducir el riesgo de sufrir una pérdida significativa de ingresos debido a incidentes de seguridad informática. La proporción de empresas con este tipo de seguro ha aumentado en los dos últimos años. Más del 40 % de las empresas del conjunto de la economía contaban con un seguro contra incidentes de seguridad informática en 2020.

A diferencia de los porcentajes correspondientes a las estrategias de seguridad y los responsables de ciberseguridad, la prevalencia de los seguros no difiere especialmente por sector y categoría de tamaño. Las cifras correspondientes se sitúan en torno al 40 % para todas las categorías. Como se observa en el gráfico 8, las empresas medianas están aseguradas contra incidentes de seguridad informática con más frecuencia (casi el 60 %).

GRÁFICO 8. PORCENTAJE DE EMPRESAS SUIZAS CON GASTO EN PRODUCTOS Y SERVICIOS DE CIBERSEGURIDAD POR TAMAÑO ENTRE 2018 Y 2020



Fuente: KOF (2023).

Además, según el IT-Sourcing Studie de PWC 2015, los demandantes de servicios de TI en Suiza consideran que lo más importante a la hora de elegir un proveedor es la calidad de los servicios, la experiencia consolidada que aporta y que el mismo proveedor pueda ofrecer una amplia gama de servicios (para que la empresa no tenga que contratar a diferentes proveedores para diferentes necesidades). El precio no es el factor más relevante, lo que denota que los suizos anteponen la calidad al coste del servicio.

Las empresas suizas se enfrentan a ciberataques cada vez más sofisticados, frecuentes, complejos y versátiles. Además, se enfrentan a la falta de recursos cualificados y a la dificultad de actualizar constantemente los conocimientos especializados. Están encontrando el tipo de servicios de seguridad gestionada externalizados (Managed Security Services, MSS) que puede ayudarles a afrontar este reto.

Las empresas medianas, más afectadas por la escasez de especialistas en ciberseguridad que las grandes, confían cada vez más en el apoyo de proveedores de servicios externos para superar estos retos crecientes. Estas empresas medianas están cada vez más interesadas en los MSS externalizados de los proveedores de servicios de Centros de Operaciones de Seguridad (Security Operation Center, SOC), que en el pasado han sido utilizados principalmente por empresas más grandes.

4.2. Comercio exterior

Como ya se ha descrito en apartados anteriores, el principal país proveedor de productos y servicios TIC para Suiza es Estados Unidos, si bien está perdiendo peso respecto a otros países como Alemania, Reino Unido e Irlanda. Según se observa en la Tabla 5, las importaciones suizas se mantuvieron estables en torno a 15.500 millones de francos de media entre 2018 y 2022, mientras que entre 2021 y 2022 han aumentado casi un 8 % y entre 2022 y 2023 ha vuelto a repuntar un 3 % para situarse en torno a los 17.000 MCHF.

TABLA 5. IMPORTACIONES SUIZAS DE PRODUCTOS Y SERVICIOS TIC

	2019	2020	2021	2022	2023
Total, de importaciones TIC suizas (MCHF)	15.845	15.126,6	15.794,3	17.047,5	17.614,6

Fuente: Banco Nacional Suizo (2024).

icex

5. Precios

Los importes de los servicios de ciberseguridad no son fáciles de establecer. Las empresas ofrecen diferentes precios dependiendo de la calidad de sus servicios, los tiempos de realización de estos y tanto la naturaleza del producto ofertado como la del comprador.

Tanto las infraestructuras de *hardware* como las soluciones de *software* son productos altamente globalizados y homogéneos en lo que respecta a sus prestaciones y a las necesidades que satisfacen. Su naturaleza globalizada los hace accesibles desde cualquier parte del mundo, lo que implica que su precio dependerá de la oferta y demanda mundiales. Por su homogeneidad, el precio de estas soluciones de ciberseguridad es uniforme independientemente del país del cliente final. Esto se da especialmente en soluciones de ciberseguridad básicas, como los antivirus o cortafuegos.

El caso de los servicios de consultoría de ciberseguridad es diferente. En este tipo de soluciones, la mano de obra es un factor significativo en el coste total del producto. La diferencia se acentúa cuando escasea la mano de obra cualificada en el país. Además, el precio también se incrementa en función de los requerimientos técnicos de la solución demandada. Al tener que desarrollar soluciones a medida para cada cliente, se justifica un precio diferente en cada caso.

En las grandes empresas, sus necesidades concretas pueden proporcionar un mayor poder de negociación a la hora de fijar el precio de las soluciones de ciberseguridad. Además, y dado que es imposible ofrecer una solución completa de ciberseguridad frente a cualquier tipo de amenaza, la inversión que estén dispuestas a hacer estas grandes compañías dependerá también del nivel de riesgo que deseen asumir y del propio análisis coste/beneficio que cada cliente se plantee.

El riesgo de experimentar filtraciones de datos que pongan en peligro la seguridad nacional o que revelen datos sensibles de gobiernos o instituciones públicas a raíz de un ataque cibernético, provoca que los organismos gubernamentales estén dispuestos a invertir cada vez más recursos en ciberseguridad.

En cuanto a las pymes y a los particulares, se prevé que su demanda se centre en soluciones de ciberseguridad básicas, como paquetes de antivirus o cortafuegos, ya que la probabilidad de que sean receptores de amenazas severas es bastante baja (más allá de *softwares* espías comunes y virus informáticos habituales). Para este segmento de clientes, el precio será uno de los factores de compra más decisivos, por lo que proporcionar un precio competitivo será fundamental.

Para el sector análogo de *Software as a Service* (SaaS), el estudio realizado por CloudZero señala que el margen más habitual para estos servicios es del 80 %. Sin embargo, para las *startups*, este

margen se estrecha al 50 % debido a que aún no se benefician de las economías de escala de las que disfrutaban las empresas SaaS en fases posteriores. Además, las empresas SaaS suelen invertir mucho por adelantado en investigación, desarrollo y penetración en el mercado.

En aras de dar una imagen aproximada de los costes que se dan en el sector, a continuación, se exponen los precios del alquiler de oficinas y los salarios de los empleados de TI y ciberseguridad relativos a los diferentes puestos de trabajo que se ofertan en Suiza en el momento de realización de este estudio. Es preciso comentar que, debido al elevado nivel de renta per cápita del país, los precios suizos se encuentran entre los más altos del mundo, con un nivel que viene a resultar el doble que la media europea.

En concreto, los precios de los alquileres de las oficinas difieren según la ciudad de establecimiento. La media aproximada del alquiler de 1m² en Suiza es de 275 CHF al mes (1.640 CHF al año). Sin embargo, se debe tener en cuenta que los alquileres en Zúrich y en Ginebra son los más caros, normalmente en torno a un 10 % más elevados que los de los cantones de Lausana y Berna.

Por otro lado, en la Tabla 7 se muestran los salarios de diferentes puestos de TI y ciberseguridad predominantes en Suiza.

TABLA 6. SALARIOS TI Y CIBERSEGURIDAD EN SUIZA EN CHF (2023)

Salarios medios anuales en francos suizos

Puesto	Horquilla salarial
Ingeniero de ciberseguridad	110.000 a 130.000
Consultor de ciberseguridad	110.000 a 160.000
Analista de ciberseguridad	90.000 a 110.000
Respondedor de incidentes cibernéticos	111.000 a 130.000
Probador de seguridad	110.000 a 130.000
Director de seguridad	160.000 a 200.000
Asesor de vulnerabilidad	110.000 a 130.000
Information Security Officer	130.000 a 150.000
Chief Information Security Officer	150.000 a 220.000

Fuente: Swiss Cyber Institute 2023.

6. Percepción del producto español

Según el Índice Global de Ciberseguridad (Global Cybersecurity Index) de 2020, España se sitúa en el puesto 4.º, solo por detrás de EE. UU., Reino Unido, Arabia Saudí y Estonia e igualado a puntuación (98,52 sobre 100) con Corea del Sur y Singapur. Teniendo esto en cuenta, España se encuentra entre los tres mejores países de Europa según el GCI. Suiza, por otro lado, ocupa el puesto 42.º con una puntuación de 86,97. En términos de ciberseguridad, España presenta legislación a este respecto, CERTs y agencias nacionales, mucho talento y buenas relaciones y tratados con otros países.

Junto a estos buenos resultados en comparativa internacional, y como se mencionó anteriormente en el apartado 3.2.3 de este estudio, España está siendo un destino cada vez más importante de inversiones suizas en este sector. En concreto, con cada vez mayor frecuencia grandes empresas suizas optan por centralizar en sus filiales en España la gestión TIC o el desarrollo de software para el conjunto del grupo, mientras que empresas suizas de todos los tamaños optan por externalizar dichos servicios en empresas españolas. Este fenómeno de los últimos años se ve favorecido por las siguientes fortalezas de la oferta española:

- **Talento y recursos humanos:** El 48 % de la población de entre 25 y 34 años tiene estudios superiores, siendo el 21,9 % licenciados en STEM (muy por encima de la media europea del 13,6 %). Los costes laborales son inferiores a los de otros países vecinos e inferiores y a la media europea. La amplia red de universidades españolas y centros de formación profesional ofrecen estudios reglados en TIC todo el territorio español, colaborando estrechamente con empresas para el fomento de cursos relacionados con competencias digitales.
- **Infraestructura tecnológica:** Según la edición de 2021 del Digital Economy and Society Index de la Comisión Europea, España ocupa la tercera posición en la UE en términos de conectividad y la séptima en términos de servicios públicos digitales, con niveles muy superiores a la media de la UE. Así, España cuenta con la mayor red de fibra óptica en la UE y la tercera en la OCDE, siendo el 88,3 % de las conexiones de alta velocidad de 100 Mbps o más y el 96,2 % de 30 Mbps o más. En telefonía móvil, España cuenta con más de 56 millones de terminales y 172.000 estaciones de comunicación móvil. En cuanto a supercomputación, España alberga la supercomputadora Mare Nostrum 4, la tercera más poderosa de Europa y la decimotercera en el mundo. Como nodo estratégico para cables submarinos, una extensa red conecta España con Europa, África y América.

- **Mercado doméstico muy atractivo y en fuerte expansión:** El sector TIC representa en España en torno al 5 % del PIB y al 4 % de las exportaciones, con un ecosistema de más de 37.000 empresas que emplean a más de 580.000 trabajadores y con multinacionales españolas de prestigio como Telefónica, Amadeus, Indra o Everis liderando proyectos en mercados internacionales. En términos de tendencia, viene creciendo a tasas interanuales de doble dígito en los últimos años, habiendo recuperado ya su posición anterior a la pandemia. De los 47 millones de habitantes con los que cuenta España, más de 33 millones son usuarios de Internet, con una ratio de penetración del móvil del 120 %.
- **Apoyo gubernamental:** España es el país que más fondos recibirá del Plan de Recuperación, Transformación y Resiliencia (NextGenerationEU), en concreto hasta 140.000 millones de euros entre 2021 y 2026, de los que el 23,1 % se destinarán a la modernización y digitalización de la industria, las pymes y el turismo, así como al fomento del emprendimiento. El compromiso nacional al respecto se refleja en el [Plan España Digital 2026](#), que cuenta con estrategias específicas para impulsar tecnologías cruciales para el país en ámbitos concretos como 5G, ciberseguridad, "big data" o inteligencia artificial.

No obstante, esta excelente imagen como país destino de inversión no se traduce en igual medida en la presencia directa de empresas españolas del sector en Suiza. Así, la mayoría de las empresas de ciberseguridad españolas no están presentes en Suiza, por lo que no se tiene percepción clara de los productos ni servicios que ofrecen. Por analogía con la percepción de los productos y servicios TIC en general, cabe presumir que la de los del ámbito de la ciberseguridad estaría quizá en términos de calidad y rendimiento por debajo de la alemana, la israelí y la estadounidense, pudiendo equipararse con los italianos o los franceses.

La falta de empresas españolas de renombre en suelo suizo puede deberse a que el mercado suizo constituye un mercado de escaso interés para España o que no se hayan podido aprovechar oportunidades de mercado que pudieran haber fortalecido la imagen de España en Suiza.

7. Canales de distribución

En el sector de la ciberseguridad en Suiza, lo más recomendable es apostar por un socio comercial local o que tenga una presencia consolidada en Suiza. No se recomienda exportar directamente porque el consumidor suizo prefiere comprar productos que hayan sido producidos localmente y que los proveedores sean empresas que tengan experiencia en el mercado nacional.



**swiss made
software**

Dados que los productos de ciberseguridad se relacionan con la protección de datos, las empresas y consumidores finales suizos de estos productos se decantan por proveedores de renombre, que cuenten con una buena imagen de marca y que estén establecidos en Suiza. Además, es preciso mencionar que todo producto o servicio que se comercialice en Suiza tendrá más a su favor si presenta un sello o logo de la asociación, institución u organización suiza relativa al sector. En el caso de los productos de ciberseguridad, este

“sello de garantía” (se muestra en la imagen contigua) podría ser el que otorga la asociación *Swiss Made Software*.

Esta asociación, presentada anteriormente en este informe, permite a los comerciantes y desarrolladores de software en Suiza ser miembros de la misma para disfrutar de ventajas, como el uso del logo en los productos; aparecer en la lista de empresas, productos y servicios de software de la asociación, además de en la *Swiss IT Magazine*; obtener más fácilmente la certificación ISO-25001 para la comercialización de software en Suiza; buscadores de empresas de la iniciativa *Digital Switzerland*; o asistencia a eventos organizados por la asociación; entre otros.

En el catálogo de empresas que ofrece la página web⁴, en la que se pueden buscar empresas dedicadas a la ciberseguridad, es posible encontrar socios comerciales que puedan servir como importadores de los productos que se quieran exportar a Suiza. No obstante, esta fuente no debería ser la única consultada, pues no presenta un listado completo de las empresas de ciberseguridad de Suiza.

Para el consumidor suizo el sello nacional ("Swissness", reflejado mediante la inclusión de la bandera nacional en el etiquetado del producto) es considerado sinónimo de calidad. Este sentimiento general supone, trasladado al sector de la ciberseguridad, la preferencia por servicios de seguridad gestionados en un centro de operaciones de seguridad (SOC) en Suiza, especialmente en sectores que manejan datos sensibles, como el bancario.

⁴ Catálogo de empresas registradas en la asociación *Swiss Made Software*: <https://www.swissmadesoftware.org/en/products-and-cloud-services.html> ; <https://www.swissmadesoftware.org/en/services-and-consulting.html>

7.1. Acceso a potenciales socios

El mercado TIC, por sus características intrínsecas en cuanto a globalización, especialización y diferenciación, está muy saturado. Consecuencia de ello es que prácticamente la única posibilidad para iniciar los primeros contactos y crear sinergias sea a través de los encuentros personales que tienen lugar en los puntos específicos para el *networking*: ferias, simposios, seminarios, conferencias, o incluso, *webinarios*.

Las fechas y lugares de celebración de estos encuentros pueden consultarse en los enlaces mencionados en el apartado siguiente.

Las comunicaciones escritas que lleven consigo la negociación, personalizadas y con el tratamiento de cortesía, deben ser sobrias y sin exceso de frases hechas y ostentosas, pues el suizo antepone hechos y datos a palabras. Se deben conceder plazos de respuesta razonables.

El correo electrónico, por su simplicidad y flexibilidad, es el medio de comunicación más idóneo para el cruce de correspondencia. La redacción puede ser en alguno de los idiomas oficiales, aunque dentro del contexto de la informática y telecomunicaciones, es casi preferible el inglés.

En las reuniones concertadas es conveniente llegar siempre unos minutos antes y en caso de que se prevea algún retraso, se deberá informar con la debida antelación. Para los suizos, el humor no encaja demasiado en los negocios, por lo que se ha de prescindir de bromas y chistes, al menos durante las primeras negociaciones.

Las normas de protocolo y la observancia de las formas son de obligado cumplimiento: mantener cierta distancia física en las conversaciones y no tratar temas personales y familiares, ni utilizar frases altisonantes.

Aunque los regalos no son muy comunes en las negociaciones, se puede hacer entrega de algún pequeño detalle.

La oferta inicial no debe diferir en demasía de los precios finales a los que se quiera cerrar el trato. De otro modo, puede generar desconfianza.

Se debe prestar especial atención a los detalles cuando se negocie con un socio suizo. Los acuerdos, contratos o condiciones de venta y colaboración deben especificar todas las condiciones y, en especial, quién asume qué costes. Todo servicio o gasto imprevisto que deba realizar la empresa suiza será repercutido, sin discusión, a su contraparte (y los servicios en Suiza son extremadamente caros).

7.2. Ferias del sector

- [Swiss Cyber Security Days](#): Es la feria líder del país en el sector de la ciberseguridad, abarcando las tecnologías de información, la ingeniería y el diseño de soluciones parciales e integrales. La última edición fue el 20/21 de febrero de 2024, y se prevé que la próxima tenga lugar el 18/19 de febrero de 2025. Con el cambio de localización de Friburgo a Berna se ha reforzado su carácter institucional, gracias a la asistencia de numerosos ponentes de alta calidad de órganos tan relevantes para la seguridad colectiva como la OTAN o el FBI, así como representantes del sector público suizo. Además, el día previo al comienzo de la feria se organizó un encuentro de los participantes en el Parlamento suizo con actores políticos relevantes para el sector.
- [Swiss Cyber Storm Konferenz](#): Conferencia de seguridad en TIC que reúne invitados tanto nacionales como internacionales en Lucerna. Próxima edición en octubre de 2024.
- [Swiss IT Business](#): Feria que se celebra en Saint Gallen que reúne a empresas y profesionales de los sectores del *big data*, *cloud computing*, ciberseguridad, infraestructuras TIC y *e-business*. Próxima celebración el 11 de abril de 2024.

7.3. Publicaciones del sector

A continuación, se muestra una lista de revistas online relativas al sector de las TIC en las que se pueden encontrar noticias relativas al campo de la ciberseguridad en Suiza:

- [Swiss IT Magazine](#)
- [Calendario de eventos del sector](#)
- [Inside-IT.ch](#)
- [IT-Markt](#)
- [Computer World Suiza](#)
- [Swiss IT-Reseller](#)
- [ITbusiness](#)

8. Acceso al mercado – Barreras

Suiza cuenta con una política de libre comercio que crea un contexto óptimo para el intercambio de bienes y servicios, y para el establecimiento de empresas.

Los países europeos que quieran acceder al mercado suizo pueden beneficiarse del tratado de libre comercio entre la Unión Europea y Suiza bajo la convención de la AELC (Asociación Europea de Libre Comercio). Conforme a él, la importación de bienes industriales está exenta de aranceles y cupos si se demuestra que la importación se ha realizado desde un país comunitario. Además, las declaraciones en aduanas están automatizadas mediante las aplicaciones informáticas E-Tec y NTCS.

A tratarse de servicios, en Suiza se debe contactar con la empresa proveedora para poder contratar dichos servicios.

8.1. Aspectos a tener en cuenta

- **IVA a la importación:** la importación de bienes y servicios relacionados con la ciberseguridad se gravan al tipo de IVA normal, que en enero de 2024 subió al 8,1 %. En aduanas, los impuestos son gestionados por la [Administración Federal de Aduanas](#) y los impuestos indirectos por la [Administración Federal Tributaria](#).
- **Registro de las actividades:** A partir del 1 de enero de 2018, las operaciones de comercio exterior de bienes y servicios deben estar registradas a efectos del IVA ante la Administración Tributaria suiza si la renta universal de la empresa que realiza dichas actividades es superior a 100.000 CHF. Además, es necesario disponer de un representante fiscal con establecimiento en Suiza.
- **Acuerdo de Libre Circulación:** En el caso de que una empresa tenga que mandar trabajadores a Suiza para prestar un servicio, el ALC prevé el derecho de prestar servicios de corta duración en Suiza hasta un máximo de 90 días laborables por año natural, independientemente del número de trabajadores que se desplacen a Suiza para prestar el servicio. Es obligatorio comunicar a las autoridades suizas la entrada de los trabajadores en el país con una antelación mínima de 8 días a partir de la fecha de comienzo de la prestación del servicio. Dentro de este acuerdo, también se debe tener en cuenta las medidas de protección salarial y de las condiciones de trabajo en Suiza (*flanking measures*) que fijan y limitan las condiciones para prestar servicios

para las empresas que no cuenten con un establecimiento permanente⁵. Las empresas extranjeras deben equiparar las condiciones de trabajo y los salarios de los trabajadores que vayan a trasladarse a Suiza con a las condiciones y salarios suizos.

- **GDPR:** Las empresas suizas estarán sujetas a la nueva regulación de protección de datos de la UE si éstas están establecidas en la UE o, si estando establecidas en Suiza, procesan datos personales de sujetos sometidos a la regulación de datos de la UE. Las empresas suizas que tengan una presencia local en la UE o tengan empresas subsidiarias en el espacio comunitario tendrán que someterse a la GDPR. Por ejemplo, tendrá que cumplir la nueva regulación⁶:
 - Una empresa suiza que desarrolle alguna actividad en un país de la UE;
 - Una empresa establecida en Suiza que oferte bienes y servicios vía internet a sujetos cometidos a la regulación de protección de datos de la UE;
 - Una empresa establecida en Suiza que recoja datos de comportamiento online por razones de marketing si esos sujetos están sometidos a la regulación de datos de la UE.

La GDPR se basa en principios muy parecidos a los de la Ley de Protección de Datos suiza. No obstante, las empresas deben adaptarse a la regulación europea. El Consejo Federal suizo y la División Federal de Justicia y Policía están redactando en la actualidad una Ley de Protección de Datos actualizada para integrar las nuevas medidas incluidas en la GDPR. Si las empresas suizas no cumplen la nueva regulación europea podrían enfrentarse a multas millonarias.

8.2. Criterios de inversión en Suiza

A la hora de invertir en bienes tecnológicos, los **inversores suizos tradicionales** buscan negocios que reúnan algunas de las siguientes características:

- **Equipo con experiencia en el sector:** buscan que las empresas estén lideradas por equipos que cuenten con miembros con experiencia previa en el sector tecnológico.
- **Diferenciación:** los productos y servicios ofertados por las empresas que quieran instalarse en Suiza deben proveer un bien exclusivo, es decir, que no se oferten en el mercado nacional. Como se ha mencionado con anterioridad, si hay bienes de producción nacional que ofrezcan los mismos servicios que la empresa internacional que quiera establecerse en el país, los suizos optarán por los productos y servicios de origen nacional. Los inversores suizos buscan que los

⁵ Para más información, visitar los siguientes enlaces: *The State of EU-Switzerland Relations in the EMPL Areas of Responsibility*: <http://bit.ly/2oIKYrw> ; *Free movement of personal – functioning and current state of play*: <http://bit.ly/2EQHO5f>

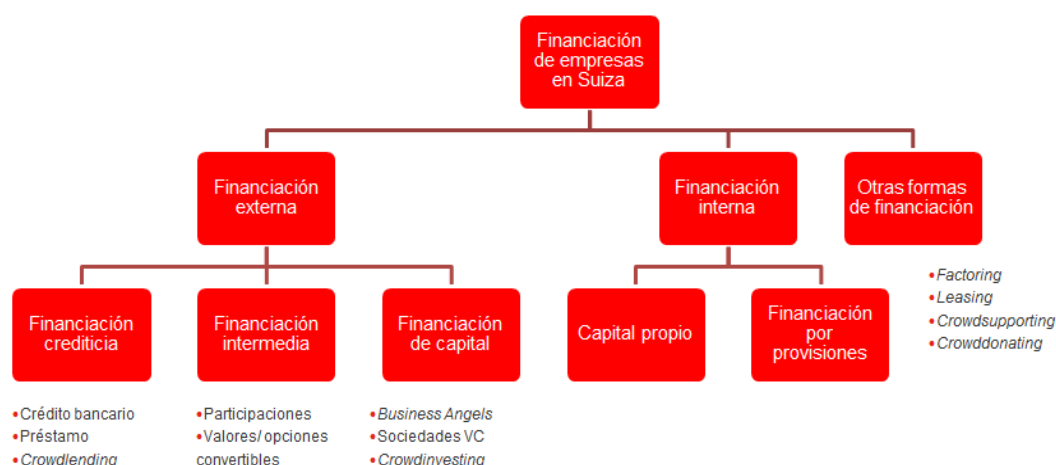
⁶ Iron Mountain – *The Impact of GDPR on Swiss Companies*: <http://bit.ly/2EOgKru>

productos exhiban una ventaja competitiva, es decir, que se les ofrezcan licencias y relaciones exclusivas, protección de propiedad intelectual o el desarrollo íntegro de los bienes.

- **Estado financiero:** Es imprescindible saber que a los inversores suizos no les gusta el riesgo. Por ello, buscan invertir en negocios bien establecidos y con músculo financiero. Por un lado, es esencial que las empresas que busquen inversión exhiban unos estados financieros que demuestren liquidez, rentabilidad y flujos de beneficio. Además, deben presentar proyectos de inversión bien organizados. Por otro lado, es importante haber entablado una relación previa con el inversor y así poder adaptar la propuesta de inversión a los requisitos de este.
- **Potencial del proyecto:** Los inversores suizos quieren ver que los proyectos sean rentables, que la empresa en cuestión haya conseguido o esté en conversaciones para conseguir financiación de diferentes fuentes, y que ésta tenga en mente expandirse por Europa o que ella esté presente en el mercado europeo.

Los criterios de inversión de los *business angels* y *venture capitalists* (VC) de Suiza difieren en algunos aspectos a los de los inversores suizos tradicionales. Los *business angels* buscan una buena relación con la empresa en la que quieren invertir, pues trabajarán más estrechamente con ella que los inversores tradicionales; mientras que los VC prefieren que la empresa no cuente con muchos accionistas. Además, estos actores no pondrán trabas a invertir en empresas que presenten riesgo, siempre y cuando ofrezcan grandes beneficios. Por último, por un lado, los *business angels* suizos suelen invertir en productos y servicios que ofrezcan soluciones a necesidades presentes en grandes mercados y con gran potencialidad. Por otro lado, los VC tienen más en cuenta las características del mercado, como el crecimiento y el volumen de competencia, y la inmediatez de los resultados.

IMAGEN 3. FINANCIACIÓN DE EMPRESAS EN SUIZA



Fuente: KMU Portal (2020).

Para más información sobre la financiación de empresas en Suiza se puede visitar la página oficial de [financiación del gobierno suizo](#).

En el caso en el que se quiera desarrollar servicios en Suiza, se muestra las fases del proyecto, las actividades a desarrollar, el tiempo de desarrollo, el tipo de inversor necesario y el volumen de capital que se necesita⁷.

TABLA 7. DESARROLLO DE SERVICIOS EN SUIZA. CAPITAL, DURACIÓN Y TIPO DE INVERSOR

Fase de financiación	Actividad	Importe de la financiación CHF	Meses	Tipo de inversor
Concepto	Desarrollo de la idea de negocio	1.000 – 5.000	1 - 6	Fundador, 3F (Amigos, Familia, Otros)
Fase temprana				
Semilla	Elaboración del plan de negocio, financiación, estudio de viabilidad	10.000 – 50.000	3 - 24	Fundador, 3F
Start-up	Desarrollo del producto o servicio, preparación de la entrada al mercado	50.000 – 500.000	3 - 12	Business Angels, banco cantonal
Fase 1	Entrada al mercado	500.000 – 2.000.000	3 - 12	Business Angels, VC
Fase de expansión				
Fase 2	Pre-consolidación	1.000.0000 -5.000.000	12 - 48	VC
Fase 3	Expansión en el mercado	1.000.0000 -5.000.000	12 - 48	VC
Puente	Financiación provisional para una futura salida bolsa	500.000 – 1.000.000	6 - 12	VC

Fuente: KMU Portal (2017).

8.3. Concursos públicos y licitaciones

La reglamentación relativa a los concursos públicos y las licitaciones está regida por la Ley de Mercado de Valores de Suiza (**BEHG**) y tres ordenanzas: la emitida por el Consejo Federal, otra por la Autoridad Supervisora del Mercado Financiero Suizo (**FINMA**) y la Comisión de OPAs de Suiza (UEK). La información de los procedimientos se puede encontrar en el informe Switzerland – Takeover guide⁸ publicado por el Colegio de Abogados Internacional (International Bar Association).

⁷ Fases de financiación para servicios y conceptos tecnológicos en Suiza: <https://www.kmu.admin.ch/kmu/de/home/praktisches-wissen/finanzielles/finanzierung/grundlagen/kosten-fuer-dienstleistungs-oder-technologiekonzepte.html>

⁸ Switzerland – Takeover guide: <http://bit.ly/2ovEnKa>

Hay que tener muy en cuenta que más del 80 % de las licitaciones publicadas en Suiza tienen como adjudicataria a una empresa suiza. No es fácil conseguir licitaciones en este país por el sesgo nacional omnipresente. En cuanto a las licitaciones de suministro de bienes y servicios que se publican, el umbral mínimo para su publicación es de 230.000 CHF para las de la Confederación y 250.000 CHF para las de los cantones, y que cuenten con las condiciones de los acuerdos internacionales de la Organización Mundial del Comercio (OMC). De todas formas, se recomienda ver las condiciones de cada cantón, pues pueden variar. Además, no es obligatoria la publicación de licitaciones de libre adjudicación y negociadas.

Otro dato importante es que las licitaciones publicadas por la Confederación relacionadas con infraestructuras críticas (IKT) no pueden ser adjudicadas a empresas extranjeras que no tengan un establecimiento permanente en Suiza.

En cuanto a listas de licitaciones y concursos, se recomienda visitar las siguientes páginas:

- **Simap.ch** – [Simap](#) es el sistema de información de los concursos públicos en Suiza que no están dentro de las condiciones de los acuerdos internacionales de la OMC.
- **[Tender Electronic Daily \(TED\)](#)** – Diario de la UE en el que se pueden encontrar las licitaciones públicas suizas que cumplen las condiciones de los acuerdos internacionales de la OMC.
- **ITTenders:** [General](#), [públicas](#).

8.4. Certificación



La certificación relativa a los bienes de software que se comercializan en Suiza es la **ISO 25001**. Obtener esta certificación otorga una imagen de calidad, de confianza y de bajo riesgo a los productos y servicios que la presenten. Para conseguir esta ISO, el bien tiene que someterse a una verificación del sistema y a una verificación de implementación. La primera etapa tiene una duración de un día y la segunda de uno a cinco días. Para proyectos de mayor envergadura, el proceso de verificación puede alargarse hasta los 10 días.

Para obtener más información sobre la certificación **ISO 25001**, las empresas pueden ponerse en contacto con la [Société Générale de Surveillance \(SGS\)](#) o con [Swiss Made Software](#).

9. Perspectivas del sector

9.1. Tendencias en el mercado de la ciberseguridad a nivel global

El empleo de las TIC se está incrementando. La relevancia de la conectividad entre cada vez más dispositivos, instituciones, empresas y ciudadanos; el aumento de las redes y la producción de datos están dando lugar a ciudades inteligentes y al auge del *Big Data*. Las nuevas tendencias en TIC, como el *cloud computing*, el internet de las cosas (IoT), los *smart grids*, las redes 5G, la tecnología blockchain o los nuevos modelos de pago, hacen que las personas cada vez estén más expuestas y aumenta la probabilidad de que su seguridad se vea comprometida por ciberataques. En este contexto, la ciberseguridad se ha convertido en una herramienta imprescindible para garantizar la protección de una sociedad conectada las 24 horas del día.

El tamaño del mercado de ciberseguridad se estima en 203 mil millones de dólares en 2024, y se espera que alcance los 350 mil millones de dólares en 2029. Entre las tendencias de ciberseguridad para los próximos años, INCIBE destaca el *cloud computing* como principal objetivo de las ciberamenazas debido al gran volumen de datos que almacena. Los proveedores de este tipo de servicios necesitan asegurar la seguridad de la información que sus clientes depositan en la nube y, para ello, crear estrategias y soluciones de ciberseguridad. Otros segmentos que resaltar son la protección de las infraestructuras críticas, de las redes industriales, de los sistemas de comunicación vía satélite y de los vehículos aéreos no tripulados.

Después del COVID-19 los ciberataques se han disparado más de un 50 % a nivel mundial. Para remediar los futuros daños, los países están invirtiendo cada vez más en ciberseguridad. EE. UU. encabeza la lista con un presupuesto de 5.600 MEUR, seguido de China con 1.200 MEUR y Reino Unido con 360 MEUR. Con dicho presupuesto, los gobiernos están creando centros nacionales de ciberseguridad y reclutando y entrenando a “ciber soldados”. Como ejemplo, EE. UU. cuenta con 9.000 de estos soldados y China con 20.000. No obstante, los cibercriminales no se están quedando atrás, ya que también están mejorando sus capacidades y tienen acceso a cada vez más recursos, tanto monetarios como para el desarrollo de nuevo *malware* o nuevas y creativas formas de *hackeo*. A esto se le suma el aumento del pago en criptomonedas de los rescates de información y datos. La principal ventaja de estas divisas es que no dejan rastro en la web y aseguran el anonimato de los atacantes.

Además, PandaLabs advierte de la creciente importancia de proteger los *endpoints* como ordenadores, teléfonos móviles, tabletas y cajeros, entre otros. La seguridad de estos dispositivos es esencial para que los atacantes no puedan acceder a datos de red, credenciales, autenticaciones o información sensible para acceder a otros dispositivos y llevar a cabo nuevos ataques.

TABLA 8. GASTO MUNDIAL EN PRODUCTOS Y SERVICIOS DE CIBERSEGURIDAD

Productos		Servicios	
Perímetro	9.600 Mill. EUR	Consultoría	17.000 Mill. EUR
Identidad	3.700 Mill. EUR	Integración	16.200 Mill. EUR
Endpoints	3.080 Mill. EUR	SOC:	
Web	2.100 Mill. EUR	• Prevención	16.200 Mill. EUR
Otros	9.000 Mill. EUR	• Detección	
		• Respuesta	

Fuente: PandaLabs (2018).

9.2. Tendencias en el mercado de la ciberseguridad en Suiza

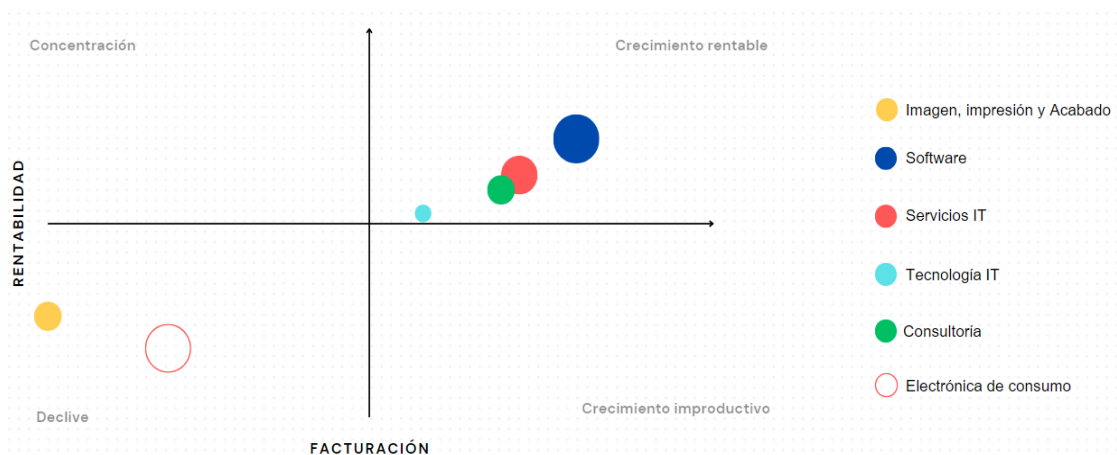
Según Experton Group, el mercado de la ciberseguridad en Suiza alcanzó la cifra de 810 MCHF en 2023 y se espera que llegue a los 1.400 millones en 2028, lo que supone un crecimiento de casi 73 % en cinco años.

Los principales objetivos de los ciberataques en Suiza son las infraestructuras críticas, las instituciones gubernamentales y las grandes empresas. El ciberespionaje, el robo de información y su posterior venta, y el control y la interrupción de los sistemas son los tipos de ataques más susceptibles de ser llevados a cabo contra estos actores.

Especialmente sensibles son los sectores bancarios, de seguros y médico/farmacéutico y todas las aplicaciones, herramientas y dispositivos relacionados con ellos. El fraude es uno de los mayores peligros a los que se enfrenta el sistema, junto con el robo de información confidencial y el *hackeo* de aplicaciones *Fintech*.

Según el estudio de Swico Index de 2024, en el mercado TIC en Suiza, el software (productos) y las tecnologías y servicios de mantenimiento TIC son los que experimentaron un mayor crecimiento durante los últimos cinco años y se espera que lo sigan haciendo hasta finales de la década.

IMAGEN 4. MERCADO TIC EN SUIZA POR SECTORES (2024)



Fuente: Swico Index (2024).

icex

10. Oportunidades

El mercado suizo está creciendo rápidamente, con oportunidades clave para las soluciones de ciberseguridad en la protección de infraestructuras críticas y los sectores comerciales. Esta expansión se ve impulsada por las autoridades suizas, las cuales han aprobado en los últimos años legislación y han publicado una estrategia al respecto.

Además, la pandemia de COVID-19 y la consiguiente cultura del teletrabajo han transformado la forma en que las empresas suizas ven la ciberseguridad. El aumento de las comunicaciones y el paso a operar los procesos empresariales a distancia han incrementado al mismo tiempo el riesgo de ciberataques en un orden de magnitud.

La adopción de la comunicación de máquina a máquina y las conexiones “Internet de las cosas” (*Internet of Things*, IoT) exigen una mayor ciberseguridad en las organizaciones. Esto está impulsando el mercado, ya que a los nuevos modelos de negocio y aplicaciones se une la disminución de los costes de los dispositivos, lo que ha sido clave para impulsar la adopción de IoT, y el número de dispositivos conectados. En el primer semestre de 2021, el Centro Nacional de Ciberseguridad de Suiza (NCSC) registró alrededor de un 25 % más de informes de incidentes cibernéticos que en los 6 meses anteriores. Para mantenerse a la cabeza en la carrera contra las amenazas complejas, muchos proveedores están ampliando sus Centros de Operaciones de Seguridad (SOC) para convertirlos en centros integrales de ciberdefensa dentro del país helvético.

Bajo este contexto, las empresas suizas se decantan por los servicios de seguridad externalizados, especialmente por el grave déficit de trabajadores cualificados en el sector de la seguridad.

El mayor campo de la ciberseguridad en Suiza es la seguridad de las redes. En Ginebra se encuentra un reconocido centro de competencia en el ámbito de la gobernanza de Internet, con organizaciones centrales de la Sociedad de Internet, la Unión Internacional de Telecomunicaciones (UIT) y la Secretaría del Foro para la Gobernanza de Internet. De hecho, el origen de Internet se encuentra en el trabajo del científico británico Tim Berners-Lee en el CERN (Organización Europea para la Investigación Nuclear), situado en Ginebra y más del 50 % de las actividades mundiales de Internet tienen su domicilio en dicho cantón. Además, los datos y la propiedad intelectual se han convertido en activos corporativos importantes y, en algunos casos, significativos para la fuerte industria financiera del país. Suiza es especialmente vulnerable a los ciberataques debido a su infraestructura de alta tecnología y a su sector de servicios financieros. Estos elevados riesgos están impulsando aún más el número de nuevas empresas suizas de ciberseguridad y, por consiguiente, generando un semillero de innovación en Suiza.

Como ya se ha mencionado, los sectores más prometedores para la ciberseguridad en Suiza son el sector bancario, de seguros y médico/farmacéutico, además de las infraestructuras críticas y las instituciones gubernamentales. A continuación, se destacan las principales oportunidades que ofrece el sector de la ciberseguridad en Suiza:

- **Sector bancario:** este sector contribuyó al 5,6 % del PIB nacional en 2021. Suiza es líder mundial en banca privada y la seguridad de sus clientes es su leitmotiv. La protección de este sector es vital para la imagen suiza en el mundo y constituye una gran oportunidad para empresas extranjeras de ciberseguridad, puesto que los bancos suizos están comenzando a modernizarse y a introducirse en el mundo Fintech. La seguridad de los datos gestionados por estas aplicaciones y por el sistema propio de cada institución bancaria abre la puerta a empresas extranjeras que puedan suplir sus necesidades de seguridad en la red.
- **Instituciones gubernamentales e infraestructuras críticas:** según PandaLabs, Suiza es uno de los países que menos ciberataques recibe. A pesar de ello, los sistemas de protección suizos han probado no ser suficientes a la hora de contrarrestar ataques contra importantes instituciones y empresas (como pasó en enero de 2018 con el robo de datos 800 millones de clientes de Swisscom). Como ya se ha mencionado, la legislación suiza con respecto a la ciberseguridad acaba de ser centralizada, lo que hace que la coordinación no esté totalmente consolidada. Además, afirma que necesitan desarrollar e invertir en mejores herramientas de ciberseguridad, pues saben que con sus actuales infraestructuras de protección no serían capaces de contrarrestar un ataque a gran escala. Es más, aunque estén entrenando a “cíbbersoldados”, la propia NCS asegura que un entrenamiento de unos meses no va a convertir a estos soldados en expertos en ciberseguridad.
- **Falta de personal especializado:** en Suiza falta mano de obra especializada en ciberseguridad. A pesar de que el país cuente con algunas de las mejores universidades del mundo, los especialistas suelen migrar a otros países en los que el sector de la ciberseguridad está más desarrollado. Esto crea una alta demanda de expertos, según la NCS, lo que constituye una gran oportunidad para trabajadores en este sector, además de que los salarios suizos son muy superiores a la media.
- **Centro Global de Ciberseguridad en Ginebra:** Constituido en 2018 bajo los auspicios del Foro Económico Mundial, como organización autónoma. Su objetivo principal es el de establecer la primera plataforma mundial para que los gobiernos, empresas y expertos de cualquier país puedan colaborar en materia de ciberseguridad, dado que las ciberamenazas constituyen un problema que no entiende de fronteras. Las nuevas tecnologías como la inteligencia artificial, el internet de las cosas y la robótica y su aplicación en áreas como las finanzas, la sanidad o las telecomunicaciones hacen que sea imprescindible la colaboración internacional. Este centro contará con la ayuda de Interpol y de grandes empresas de ciberseguridad del mundo, y hará de Suiza un punto de encuentro de especialistas en

ciberseguridad de todo el mundo, lo que constituye una gran oportunidad para las empresas del sector.

- **Pequeño volumen de empresas en el sector de la ciberseguridad en Suiza:** como se ha mencionado anteriormente, Suiza no presenta un gran número de empresas en el sector. Las grandes empresas nacionales (como ELCA y Kudelski) e internacionales (como Microsoft y Atos) son las que acaparan el mercado. No obstante, siempre hay espacio para las empresas que ofrecen productos y servicios innovadores que todavía no estén presentes en el mercado.
- **Suiza como centro de innovación mundial:** según el INSEAD, Suiza es el país más innovador del mundo y Zúrich es la ciudad más innovadora. La presencia en Suiza ofrece una muy buena oportunidad para estar en contacto con empresas punteras de todo el mundo que pueden dar lugar a acuerdos comerciales. Además, Suiza ofrece incentivos fiscales para empresas que realicen actividades de I+D.

iCEX

11. Información práctica

Suiza cuenta con una economía de mercado moderna, bajo nivel de desempleo, una fuerza de trabajo altamente cualificada, cuentas públicas saneadas y un PIB per cápita entre los más altos del mundo y que permite afrontar el futuro con relativo optimismo, a pesar de los efectos que produce en su economía la incertidumbre reinante en los mercados internacionales, su política cambiaria y el debate suscitado con la UE sobre la inmigración masiva.

Tiene una superficie de poco más de 41.000 Km² y una población de 8,8 millones de habitantes. Su privilegiada situación geográfica en el centro de Europa, junto a su estabilidad económica y seguridad, son argumentos de peso que han contribuido a que grandes empresas internacionales hayan sentado sus bases en el país.

Las oportunidades de negocio para el exportador español se derivan, por tanto, de su cercanía y de ser un país desarrollado con mercados maduros con alta capacidad. Para el inversor español tiene importancia su integración en el amplio mercado europeo, así como la disponibilidad de mano de obra altamente cualificada y gran número de posibles socios suizos locales: hay en Suiza muchas pymes con un alto nivel de preparación tecnológica deseosas de establecer alianzas internacionales.

Suiza dispone de una infraestructura de transportes muy desarrollada. En lo que a carreteras se refiere, la Confederación Helvética se encuentra muy bien comunicada –incluso en tramos de montaña-. Los peajes en autopistas no existen y la circulación de estas se realiza mediante el pago anual de una viñeta que cuesta 40 CHF.

La velocidad máxima a la que se puede circular por carreteras nacionales es 80 km/h, 100km/h en autovías y 120 km/h en autopistas, pero con muchos tramos a velocidades inferiores.

La empresa estatal de ferrocarriles suizos, SBB tiene una extensa red de 9.000 km que comunica todas las regiones, por lo que es el medio de transporte interior más utilizado.

Al ser un país de interior, su único puerto fluvial está en Basilea sobre el río Rin, que la comunica con otros puertos fluviales de Alemania.

En lo que concierne al tráfico aéreo, existen tres aeropuertos internacionales en las ciudades de Zúrich, Ginebra y Basilea. Berna, a pesar de ser la capital, tiene un muy pequeño aeropuerto con apenas media docena de vuelos diarios.

11.1. Perfil del dirigente suizo

En un contexto macrosocial, las diferencias entre España y Suiza no son muy grandes. Valores democráticos como la igualdad, justicia libertad o políticas de economías de mercado son afines en ambos países. Incluso las formalidades protocolarias no difieren a las de cualquier otro país occidental, aunque coexisten ciertas pautas del comportamiento suizo emanados de su propia cultura que es menester considerar, a fin de adoptar posturas convenientes en las futuras negociaciones comerciales

En Suiza confluyen tres micro culturas bien diferenciadas que coinciden prácticamente con sus regiones idiomáticas y geográficas. La zona germánica, que es la predominante (2/3), comprende el área desde el centro del país al Norte y Este, la francófona abarca el Oeste-centro y la italiana, la más pequeña, el Sur.

Estas micro culturas, aun manteniendo su propia identidad están, pues, fuertemente influenciadas por las de los tres países vecinos, en relación directa con la proximidad o alejamiento de las respectivas fronteras. Aunque en el análisis de los diferentes aspectos culturales se haga hincapié en la micro cultura germanófila, por su preponderancia, habrá que tener en cuenta este punto.

Los aspectos culturales más característicos del ciudadano medio suizo vienen marcados por una comunicación verbal de bajo contexto (información sobria y directa), mono crónico (realización de tareas de forma secuencial, no realizan varias tareas al mismo tiempo y no hay cabida a la improvisación), individualista (perseverancia de la esfera íntima y abundancia de relaciones y contactos muy superficiales) y baja distancia jerárquica (lo que en el seno de una empresa representará que cualquier decisión que se adopte será muy consensuada, incluso con los escalafones inferiores).

Con los aspectos culturales anteriormente tratados juntos a otros conceptos más o menos estereotipados surgidos de su propia historia y geografía, se puede conformar el perfil típico de un negociador suizo que puede presentar las siguientes características:

- **Multicultural y políglota:** Suiza es ya de por sí un mosaico cultural, está habituado al contacto cotidiano con personas de diversas nacionalidades. Suele hablar al menos dos de los idiomas oficiales, aunque también es corriente el uso del inglés en las negociaciones.
- **Estricta observancia de las normas:** La ruptura de las normas es considerada como una falta de consideración y no como actitud innovadora. El orden es fundamental, alcanzando su máxima expresión en la obsesión por la puntualidad.
- **Estricta observancia de las formas:** Destaca por su austeridad y poca ostentación. Discreto en la expresión de sus emociones, son corteses, pero no efusivos. Muestran respeto por el estatus, pero no le condiciona en sus decisiones. El ser tratado por su nombre y título es muy valorado.

Utilizan una comunicación de bajo contexto y escasa asertividad, por lo que las conversaciones se encaminan rápidamente a la cuestión a tratar y las realizan en un tono bajo de voz y carente de agresividad. Aprecian las actuaciones directas, francas y honestas. El ámbito familiar y personal debe mantenerse alejado en las conversaciones.

- **Cautela:** Es recatado por naturaleza y escéptico ante cualquier novedad, teniendo en cuenta que tienen muy grabado que “lo” que es suizo, por el mero hecho de serlo, es lo mejor. Las decisiones que adopte serán tras un profundo análisis de todos los factores. Esto le llevará tiempo, y aún más si tocan algún argumento proteccionista, valor muy implantado en la sociedad suiza.
- **Habilidad en los negocios:** Sabe proteger sus intereses como pocos. Consiguen sus propósitos, o al menos lo intentan, utilizando tácticas poco agresivas y exigentes. Los negociadores suizos se conocen por lograr lo que desean sin tácticas agresivas ni exigentes. El regateo no se debe utilizar con los suizos
- **Concienciación por el medio ambiente:** Amante y respetuoso con el medio ambiente y la naturaleza, cualquier negociación cuyo tema pudiera estar en discordancia con las reglas básicas de aquéllos está prácticamente condenada al fracaso.



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](#)

www.icex.es

