INSTITUTO NACIONAL DE CIBERSEGURIDAD

Benchmark Internacional de Talento en Ciberseguridad

Agosto 2022

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

017 TU AYUDA EN CIBERSEGURIDAD incibe_

Contenido

1. Objetivos.
2. Metodología de realización.
3. Países parte del estudio:
   - EE.UU.
   - UK.
   - Israel.
   - Malasia.
   - China.
   - Canadá.
   - Francia.
   - Rusia.

Objetivos

El objetivo general perseguido con la elaboración de este análisis benchmark es **identificar a nivel internacional las mejores prácticas de gestión del talento en ciberseguridad**, de forma que se generen recomendaciones y acciones que permitan maximizar el impacto de las actuaciones a desarrollar en el marco del proyecto.

En este contexto, abordaremos los siguientes **objetivos específicos** contemplados en el estudio de la gestión del talento en ciberseguridad que lleva a cabo cada país.

- Plasmar de manera general la estrategia de ciberseguridad de cada país, haciendo énfasis en lo tendiente a fortalecer el ecosistema y la promoción del talento en ciberseguridad.
- Identificar los principal organismos de gestión que lideran y enmarcan las diferentes iniciativas en materia de talento en ciberseguridad.
- Identificar las principales iniciativas y actuaciones que se esperan implementar para la consecución de los objetivos.
- Profundizar en los diferentes *frameworks* de gestión del talento en ciberseguridad.
- Identificar cómo las iniciativas y actuaciones se adaptan e incorporan a la operativa interna de cada organismo y otras organizaciones.
- Identificar a los actores principales en donde se refleja el impacto o los resultados de las diferentes actuaciones.
- Precisar las posibles oportunidades y retos que catalizan o inhiben el fomento de una fuerza laboral de ciberseguridad competente y alineada con las necesidades de la demanda.
- Considerar los recursos económicos que se tienen previstos para la puesta en marcha de las iniciativas.
- Comparar la posición de cada uno de los países y evaluar bajo ciertos criterios, el estado de cada uno de ellos.
- Analizar las diferentes actuaciones para entender si las mismas son extrapolables a lo que quiere lograr INCIBE en España, aportando conclusiones y dando recomendaciones en función del análisis.

Metodología de realización

En cada país de estudio se realizará el análisis teniendo en cuenta los organismos, objetivos e iniciativas, así como los principales proyectos o actuaciones definidas para su implementación, el grupo en concreto al que se dirige, así como la financiación asociada (tanto directa como vía incentivos en caso de ser posible obtener esta información).

Trabajo previo

1. Identificación del objeto de estudio del *benchmark.*
2. Selección de áreas críticas de análisis del objeto.

Captura y análisis de información de prácticas de gestión de talento de ciberseguridad

3. Selección e identificación de variables de análisis.
4. Recopilación de información.
    - Fuentes secundarias
    - Fuentes primarias
        - Entrevistas
        - Encuestas
5. Organización y análisis de la información.

Aprendizaje

6. Elaboración de conclusiones.
7. Adaptación de las conclusiones al caso propio.
8. Extracción de prácticas a aplicar.

EE.UU.

EE.UU.

¿Qué orden seguiremos?

- Estrategia de ciberseguridad de EE.UU. → Énfasis en talento de ciberseguridad.
- ¿Qué organismos participan y tienen competencias o acciones relacionadas con el Talento de Ciberseguridad?.
- Organismos con competencias en talento en ciberseguridad.
- Análisis *benchmark.*
- Conclusiones y recomendaciones.

Estrategia de ciberseguridad de los Estados Unidos

Department of Homeland Security (DHS)

EE.UU.

Para analizar el talento de ciberseguridad de EE.UU. debemos comenzar analizando su estrategia de ciberseguridad, que la desarrolla el *Department of Homeland Security* (DHS).

La Estrategia de Ciberseguridad del Departamento de Seguridad Nacional establece cinco pilares de un enfoque de gestión de riesgos y proporciona un marco para ejecutar las responsabilidades de ciberseguridad y **aprovechar la gama completa de capacidades** del departamento para mejorar la seguridad y la resiliencia del ciberespacio.

Específicamente el pilar quinto se refiere a habilitar resultados de ciberseguridad, con lo que se espera principalmente fortalecer la seguridad y la confiabilidad de todo el ecosistema de ciberseguridad.

Talento en ciberseguridad

El objetivo principal de esta estrategia con relación al talento es mejorar el reclutamiento, educación, formación y retención para desarrollar una fuerza laboral en ciberseguridad de clase mundial.

¿Cual es la principal agencia de los Estados Unidos para lograr este propósito?

Cybersecurity & Infrastructure Security Agency (CISA)

Estrategia de Ciberseguridad de los Estados Unidos

Department of Homeland Security (DHS)

EE.UU.

El pilar quinto de la Estrategia de Ciberseguridad plantea unos **objetivos específicos relacionados con el talento** para lograr mejorar el reclutamiento, educación, formación y retención de la fuerza laboral.

Aunque la estrategia en sí no define acciones asociadas a estos objetivos, del análisis de los organismos e iniciativas en EE.UU podemos hacer una asociación con lo planteado por el **Instituto Nacional de Estándares y Tecnología (NIST)** y la **Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA)** y **la Casa Blanca**, como organismos principales en el desarrollo de políticas, iniciativas y actuaciones relacionadas con la fuerza laboral federal en ciberseguridad.

Objetivos específicos

a. Evaluar la participación y continuar el apoyo a las iniciativas de capacitación, concienciación, educación y retención cibernéticas para apoyar las instituciones de seguridad nacional.
b. Completar las actividades obligatorias de análisis y planificación de la fuerza laboral para obtener datos que impulsen los enfoques de contratación, retención y capacitación.
c. Mejorar las estrategias de contratación cibernética que apuntan a poblaciones altamente formadas y capacitadas para realizar actividades cibernéticas críticas.
d. Implementar la gama completa de flexibilidades de capital humano de ciberseguridad, autorizadas por el congreso para el DHS.
e. Desarrollar una protección de red y personal de investigación cibernética de alta calidad a través de una mayor formación, asignaciones detalladas y oportunidades de desarrollo avanzadas.

Acciones identificadas

1. **Identificar las necesidades de la fuerza laboral en ciberseguridad.** Mejorar el entendimiento de la fuerza laboral al identificar las capacidades clave y el gap para mejorar la planificación.
2. **Expandir la fuerza laboral a través de educación y capacitación.** Trabajar con instituciones educativas y expertos en programas de ciberseguridad en todos los niveles educativos para expandir el itinerario de talento capacitado.
3. **Reclutar y contratar talento altamente capacitado.** Participar en esfuerzos gubernamentales y específicos de agencias para expandir la fuerza laboral, agilizando el proceso de contratación y autorizaciones de seguridad.
4. **Retener y desarrollar talento altamente capacitado.** Promover un enfoque empresarial para esta finalidad, respaldando la mejora continua de la fuerza laboral en ciberseguridad.

Como resultado de la ejecución de las acciones planteadas, EE.UU ha logrado reclutar y capacitar a personal de ciberseguridad altamente calificado y desarrolla un cuadro de profesionales de ciberseguridad bien capacitados en todo el DHS y las instituciones de seguridad nacional.

Organismos con Competencias en talento de ciberseguridad

EE.UU.

El **DHS** tiene una misión vital: proteger a la nación de las muchas amenazas que enfrentan, lo que requiere la dedicación de más de 240.000 empleados. Sus deberes son muy variados pero su objetivo es claro: mantener a EE.UU. a salvo.

CISA lidera el trabajo estratégico y unificado de la nación para fortalecer la seguridad, la resiliencia y la fuerza laboral del ecosistema cibernético para proteger los servicios críticos y el estilo de vida estadounidense.

Ha identificado la ciberseguridad como uno de los desafíos nacionales más serios. Por tanto, han llevado a cabo una revisión exhaustiva de los esfuerzos federales para defender la infraestructura de información y comunicaciones y el desarrollo de un enfoque integral para asegurar la infraestructura digital.

El Departamento de Defensa colabora en diferentes iniciativas con el DHS y CISA para reforzar las capacidades. CyberCorps es un programa de becas en el que el DoD es patrocinador, entre muchos otros.

El Departamento de Comercio tiene la tarea de mejorar la concientización y la protección de la seguridad cibernética, proteger la privacidad, mantener la seguridad pública, apoyar la seguridad económica y nacional y capacitar a los estadounidenses para que administren mejor su seguridad en línea.

La **Agencia de Seguridad Nacional** se enorgullece de contribuir al desarrollo del talento y las herramientas para hacer que la nación sea más segura. La NSA también prepara a los futuros líderes cibernéticos. Una de sus iniciativas mas significativas son los Centros de Excelencia Academia (CAE).

El programa de ciberseguridad del **NIST** respalda su misión general de promover la innovación y la competitividad industrial de los EE. UU. Mediante el avance de la ciencia de la medición, los estándares y la tecnología relacionada a través de la investigación y el desarrollo en formas que mejoran la seguridad económica y mejoran nuestra calidad de vida.

La misión de NICE es dinamizar, promover y coordinar una comunidad sólida que trabaje en conjunto para promover un ecosistema integrado de educación, capacitación y desarrollo de la fuerza laboral en ciberseguridad.

Organismos con Competencias en Talento de Ciberseguridad

EE.UU.

Organismos

Iniciativas, actores y actuaciones

INICIATIVAS

- Cybersecurity Training and Excercises
- National Initiative for Cybersecurity Careers and Studies (NICCS)
- Stop. Think. Connect
- National Cybersecurity Awareness Month (NCSAM)
- CISA Publications / Library
- Cyber Resource Hub
- NSA Resources for Students and Educators
- National Cyber Education Program

ACTORES

ACTUACIONES

Organizaciones (18 Actuaciones Recogidas)

Cyber Storm
Continuous Diagnostics and Mitigation (CDM)
National Cyber Exercise and Planning Program
Incident Response Training
President's Cup cybersecurity Competition
CISA Tabletop Exercise Package
Federal Virtual Training Environment (FedVTE)
National Centers of Academic Excellence in Cybersecurity
CISA Cybersecurity Resources
CyberSecure My Business

Profesionales

Cybersecurity Careers and Resources
Cybersecurity Careers
NICCS Education and Training Catalog
Cybersecurity Advisories & Technical Guidance

Estudiantes

CYBER.ORG, anteriormente NICERC
Students, Launch your Cybersecurity Careers
CyberCorps: Scholarship for Service
Stop.Think. Connect Toolkit
NCSAM Resources
OnRamp II Scholarship Program

Profesores y/o Docentes

Cybersecurity in the Classroom by NICCS

Professional Development by the National Cyber Group

CYBER.ORG

Minorías

Women in Cybersecurity
Cybersecurity Basics Badge Activity
Veterans: Launch a New Career
AccessCSforAll
Minorities in Cybersecurity
International Consortium of Minority Cybersecurity Professionals

Variables de análisis para el *benchmark*

EE.UU.

VARIABLE	DETALLE
***Framework* para el talento de ciberseguridad**	Se busca evidencia de que los diferentes *frameworks* reflejen coherencia al categorizar, organizar y describir el ecosistema de la fuerza laboral en ciberseguridad.
Importancia del talento dentro de la estrategia de ciberseguridad	Analiza el protagonismo que se da a la gestión del talento en ciberseguridad dentro de la estrategia de ciberseguridad de cada país. Factores como apoyar políticas que favorezcan el ecosistema cibernético son clave.
Impacto en organizaciones (públicas y privadas)	Se analizan los programas y eventos para que las empresas sean más seguras online. Factores como la capacitación a empleados en múltiples áreas de la seguridad y el intercambio de información son clave.
Impacto en profesionales en ciberseguridad	Analiza el enfoque que tiene cada país al abordar el reclutamiento y retención del talento, así como la compensación promedio de los profesionales, tanto en el ámbito público como privado.
Impacto en estudiantes	Se valoran los países que identifiquen y estimulen el talento de ciberseguridad en los diferentes ciclos de estudio (K-12, universidades, otros centros de formación en ciberseguridad, etc.).
Impacto en profesores y/o docentes de ciberseguridad	Se tienen en cuenta programas y herramientas que empoderen a los profesores con los recursos y la capacitación necesaria para formar profesionales en ciberseguridad altamente cualificados.
Inclusión (mujeres y minorías)	Identificar actuaciones tendientes a grupos poco representativos dentro del mundo de la ciberseguridad, otorgándoles capacitación en línea gratuita, información sobre programas de grado relacionados con la ciberseguridad e información sobre becas.
Inversión	Identificar no solamente el esfuerzo presupuestal de cada iniciativa / actuación sino la forma en la que asignan eficiente y racionalmente esos recursos.

Framework talento ciberseguridad

EE.UU.

EE.UU. tiene implementado el *framework* NICE:

Proporciona un lenguaje común entre el gobierno, la academia y el sector privado.

Categoriza, organiza y describe el trabajo relacionado con ciberseguridad.

Ayuda a identificar, reclutar, desarrollar y retener el talento en ciberseguridad.

NICE Workforce Framework

NICE Framework Mapping Tool

Cyber Career Pathways Tool

La figura ilustra cómo el *framework* es una referencia central para ayudar a los empleadores a construir una fuerza laboral de ciberseguridad competente y preparada.

Framework talento ciberseguridad

EE.UU.

Para poder utilizar el *framework* como marco común de análisis se necesitan establecer unas **áreas** que nos ayuden a evaluar el contenido de los diferentes *framework* para la fuerza laboral.
Se proponen estas 6:

ENFOQUE

Conceptos más importantes en los que se enfoca el *framework* y las expectativas que se tienen en diferentes horizontes de tiempo.

ESTRUCTURA

Mide la claridad y la lógica con la que está organizado el *framework*, lo que se traduce en facilidad en la implementación.

INCLUSIÓN

Valora los diferentes actores o grupos de distinta tipología que se benefician del *framework*.

FLEXIBILIDAD

Determina si el *framework* se adapta a las necesidades de la fuerza laboral de cada organización.

BENEFICIOS

Considera la ayuda que reciben cada uno de los diferentes actores que hacen parte del ecosistema del talento de ciberseguridad.

INVERSIÓN

Tiene en cuenta las recursos económicos asignados para apoyar el despliegue del *framework*.

Análisis *benchmark*

Framework Talento Ciberseguridad

EE.UU.

Resultados del análisis

El *framework* se basa en el **lenguaje común** para **describir el trabajo en ciberseguridad** entre los diferentes niveles jerárquicos de las organizaciones, **logrando interoperabilidad y simplicidad**, en un tema bastante complejo. Habilita la comunicación en los temas más críticos, de tal forma que es **entendible para todos los *stakeholders*.**

Aborda un total de **(7) categorías, (33) áreas de especialidad, (52) roles de trabajo**, y una combinación de indicadores de capacidad en el proceso de formación de la fuerza laboral. Particularmente este *framework* cuenta con funcionalidades como el *Mapping Tool* y *Cyber Career Pathways Tool*, que permiten una mejor **experiencia de uso** y resultados. Esto es un **indicativo de la robustez** y de la alta probabilidad de que bajo esta herramienta, un profesional se **desempeñe con éxito** en roles de la ciberseguridad.

Los recursos asignados para el gestor del *framework*, es decir, CISA, alcanzan los 1,7 billones de dólares.

- **Explorar e identificar roles de trabajo, KSA (*Knowledge, Skills* and *Abilities*)**, y tareas valoradas por los empleadores.
- Identificar brechas críticas.
- Apoyo al diseño de carreras y planes de estudios.

Herramienta donde **confluyen múltiples actores**, entro los más destacados, estudiantes, educadores, empleadores, profesionales, proveedores de capacitación y formuladores de políticas. Adicionalmente, es de gran atractivo para **organizaciones de distinta tipología**: SMB, grandes organizaciones, *start-ups*; y a través de diferentes verticales.

Está diseñado para hacer uso de categorías (análisis, investigación, etc) **dependiendo de las necesidades de la fuerza laboral de cada organización.** Es fundamental la combinación que permite a las empresas entre diferentes competencias (*knowledge* + *skills*) que describen el sujeto, y las tareas a realizar con esas competencias (describen el trabajo). Esto permite comprender mejor los diferentes roles y finalmente poder diseñar **mejores estrategias en la gestión del talento.**

Framework talento ciberseguridad – Caso de uso JP Morgan

EE.UU.

El enfoque y la estructura del *framework*, es decir, la manera en que describe y categoriza el trabajo en ciberseguridad, permite que instituciones del gobierno y organizaciones privadas **identifiquen, capaciten, incluyan y retengan el talento clave** que necesitan en sus equipos de trabajo.

J.P.Morgan

La entidad financiera JP Morgan Chase utiliza el *framework* NICE como base para la formación de la fuerza laboral en ciberseguridad

FRAMEWORK NICE NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

- Para JP Morgan esta es una iniciativa relativamente nueva que utiliza una taxonomía común para describir roles de trabajo y establecer expectativas en los niveles de competencia, sin embargo, esto los está conduciendo a datos realmente interesantes que se derivan del análisis de su propia fuerza laboral.

- El mayor beneficio es poder visualizar un profesional en un rol de trabajo en particular, y utilizar eso para transcribir múltiples roles de trabajo y establecer las expectativas para esos roles de trabajo, una vez se contrasta con datos de *assessment* de los empleados, se puede comprender el desempeño del grupo de trabajadores en un rol en particular.

- En base al anterior análisis, otro de los resultados significativos es poder guiar el desarrollo de la fuerza laboral, tanto para reforzar como para fortalecer capacidades en base al análisis de los diferentes conocimientos y *skills* que se requieren para desempeñar tareas en los diferentes roles de trabajo.

- JP Morgan ha encontrado que este sistema fomenta la retención del capital humano y el desarrollo de planes de carrera, al permitir que el profesional se pueda proyectar a sí mismo en diferentes roles de trabajo dentro de la misma organización, en base a datos del *assessment*.

Framework talento ciberseguridad – Caso de uso JP Morgan

EE.UU

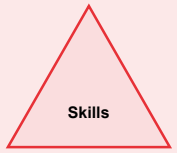
Punto de partida para comprender **qué se necesita en los roles** dentro de la ciberseguridad.

Describir las diferentes funciones en la organización, **alineado con las expectativas para ese rol** en particular.

Recopilar los datos de los empleados para **comprender dónde hay mejor 'fit'**, dentro de la organización.

PERFIL

Tarea



Análisis GAP para determinar la eficiencia en las funciones actuales del trabajo y proporcionar asistencia o formación para el desarrollo.

Planes de aprendizaje y presupuestos.

Mejor entendimiento del capital humano y estrategias más potentes.

Importancia del talento dentro de la estrategia de ciberseguridad

EE.UU.

El DHS refleja un compromiso enorme frente a los riesgos de la nación, y la creación de la CISA ha sido el mecanismo para defender el país contra múltiples amenazas, con el trabajo conjunto entre actores, instituciones, *partners*, para construir un ecosistema resiliente.

- El talento está en el centro del esfuerzo para proteger a los EE.UU. y para fortalecer ese talento como parte de la estrategia, **la CISA gestiona programas y servicios basados en un entendimiento exhaustivo del entorno de la ciberseguridad**.
- La estrategia reconoce abiertamente que existe una escasez crítica de talento en ciberseguridad a nivel mundial, ya que la demanda de personal con experiencia en ciberseguridad tanto en el sector público como en el privado supera con creces la oferta. Ante esto afirman que **"*la ejecución de las responsabilidades de ciberseguridad depende del reclutamiento y la retención de profesionales cibernéticos altamente capacitados*".**
- La estrategia explica cómo se deben ejecutar acciones de planificación y análisis de la fuerza laboral ordenadas por el Congreso y **mediante la implementación del sistema de fuerza laboral** autorizado centrado en ciberseguridad con **flexibilidad de contratación y compensación**.

A través de la ***Iniciativa Nacional para la Educación en Ciberseguridad*** **(NICE)**, desarrollada por **NIST**, y de diversos programas de **CISA**, es como la estrategia de EE.UU. apoya los esfuerzos de aumentar la oferta de talento.

Principales iniciativas que tienen impacto en los diferentes actores del ecosistema del talento en ciberseguridad

EE.UU.

Iniciativa 1. *Cybersecurity Training and Exercises*

La capacitación es esencial para preparar a la fuerza laboral de ciberseguridad del mañana y para mantener actualizados a los trabajadores de ciberseguridad actuales sobre habilidades y amenazas en evolución. El Departamento de Seguridad Nacional (DHS) se compromete a **brindar a la nación acceso a capacitación en ciberseguridad** y **ayudas para de desarrollo de una fuerza laboral cibernética** que permita una nación más resiliente y capaz.

Iniciativa 2. *National Initiative for Cybersecurity Careers and Studies (NICCS)*

Es el **principal recurso en línea de herramientas de capacitación, educación y desarrollo de la fuerza laboral en ciberseguridad.** NICCS conecta la industria de la ciberseguridad con empleados gubernamentales, estudiantes, educadores y empresas de todo el país.
Visión: proporcionar las herramientas necesarias para garantizar que los ciudadanos y la fuerza laboral de los EE. UU. tengan un conjunto de habilidades viables en ciberseguridad.

Iniciativa 3. *Stop. Think. Connect*

Campaña nacional de **concienciación pública** destinada a **aumentar el entendimiento de las amenazas cibernéticas** y **empoderar al público** estadounidense para que esté más seguro y protegido en línea. Es parte de un esfuerzo sin precedentes entre los gobiernos federales y estatales, la industria y las organizaciones sin fines de lucro para promover comportamientos y prácticas seguras en línea. Es una asociación público-privada única, implementada en coordinación con la *National Cyber Security Alliance* (NCSA).

Iniciativa 4. *National Cybersecurity Awareness Month (NCSAM)*

Mes de concienciación sobre la importancia de la ciberseguridad que se celebra cada octubre. Se creó como un **esfuerzo de colaboración** del gobierno para garantizar que todos los estadounidenses tengan los recursos que necesitan para mantenerse más seguros y protegidos en línea.

Iniciativa 5. *CISA Publications / Library*

Es el **banco de información publicada** cronológicamente a **todos los stakeholders**, con relación a los esfuerzos que está realizando la CISA en materia de ciberseguridad e infraestructuras. El objetivo principal es crear conciencia entre la sociedad para proteger los ciudadanos y la economía. De manera transparente y abierta actualizan toda la información relacionada a la seguridad, incluso en español.

Iniciativa 6. *Cyber Resource Hub*

Con el fin de ayudar a las agencias a tomar decisiones de riesgo basadas en datos, CISA puede realizar análisis de datos de evaluaciones y proporcionar esta información a sus socios. De esta forma la solicitud de servicios a la CISA puede **ayudar al ecosistema de ciberseguridad a ganar visibilidad** con las tendencias de vulnerabilidad, las actividades adversas y, lo más importante, las mitigaciones efectivas para implementar una mejor protección de sus redes.

Iniciativa 7. *NSA Resources for Students and Educators*

Para enfrentar los futuros desafíos de seguridad nacional, la **NSA se asocia con escuelas y universidades para desarrollar talento** y contar con las herramientas para: financiar programas de desarrollo de habilidades como campamentos de verano; promover el desarrollo de planes de estudio de ciberseguridad; patrocinar competencias de trabajos de investigación; acoger estudiantes en prácticas; conceder becas de investigación y financiar laboratorios y proyectos de Investigación.

Iniciativa 8. *National Cyber Education Program*

Sobre la base de la **escasez de talento en ciberseguridad**, donde se estima que los trabajos que no se pudieron cubrir en 2018 fueron más de 300.000, y esta cifra para 2021 podría ascender a 3,5 millones, este programa busca reducir esa brecha. La exposición al riesgo es un llamado urgente a tener profesionales capacitados. Esta iniciativa de educación en varias partes del K-12, se ha realizado en asociación con Discovery Education, que actualmente atiende a 30 millones de estudiantes de k-12 y 3 millones de maestros a través de su educación en línea.

Impacto en organizaciones (públicas y privadas)

EE.UU.

No.	Nombre de la Actuación	Organismo	Descripción	Estado	Resultados
1	**Cyber Storm: Securing Cyber Space**	DHS, CISA	**Ejercicios cibernéticos** que se dan periódicamente por ediciones y reúnen al sector público y privado para simular la respuesta a una crisis cibernética que afecta la infraestructura crítica de la nación.	Activo	La edición CS 2020 sirvió como catalizador para el aprendizaje significativo y el análisis operativo para la comunidad de respuesta a incidentes cibernéticos. • Examinó la eficacia del Plan Nacional de Respuesta a Incidentes (NCIRP), identificando áreas de mejora. • Evaluó el funcionamiento del Centro Nacional de Integración de Comunicaciones y Ciberseguridad (NCCIC), identificando áreas de mejora en la comunicación. • Incorporó una participación significativa de la alta dirección en los sectores público y privado (2000 participantes y 90 partners), demostrando beneficios de coordinación orientados a la acción.
2	**Continuous Diagnostics and Mitigation (CDM)**	CISA	Proporciona un enfoque dinámico para fortalecer la ciberseguridad de las redes y sistemas gubernamentales. **Múltiples herramientas de capacitación. Incluye certificaciones.**	Activo	Este programa está liderando los esfuerzos para reducir del riesgo cibernético y proveer visibilidad a través de las instituciones federales. • Ha reducido la superficie de amenaza de las agencias. • Ha aumentado la visibilidad de la postura de ciberseguridad. • Ha mejorado las capacidades de respuesta. • Ha agilizado los informes de la Ley Federal de Modernización de la Seguridad de la Información (FISMA). • Ha implementado dashboards a 23 CFO en agencias civiles federales, brindando una postura de seguridad de los ordenadores, servidores y otros dispositivos conectados a Internet.

Análisis *benchmark*

Impacto en organizaciones (públicas y privadas)

EE.UU.

No.	Nombre de la Actuación	Organismo	Descripción	Estado	Resultados
3	**Federal Virtual Training Environment (FedVTE)**	CISA, NICCS	**Sistema de capacitación en ciberseguridad**, en línea y bajo demanda. Brinda capacitación en ciberseguridad gratis a empleados del gobierno, contratistas federales y veteranos militares. **Incluye certificaciones.**	Activo	Esta plataforma ha estado disponible por más de una década, aportando a cultivar talento en ciberseguridad para proteger el ciberespacio. • Ha sido un recurso valioso para el gobierno federal al permitirle a las agencias ahorro de costes de capacitación. • En 2008, 16.730 usuarios activos y 120.000 horas de capacitación entregadas. • Desde sep 2012 - nov 2014: más de 153.000 capacitados y 62.380 cursos completados.
4	**National Cyber Exercise and Planning Program**	CISA, NCCIC	**Ejercicios cibernéticos.** Llevar a cabo un espectro completo de ejercicios en cooperación con el sector público y privado y socios internacionales, particularmente aquellos que apoyan la infraestructura crítica de los EE. UU.	Activo	Este programa fue creado en 2004 para desarrollar y gestionar el portafolio de ejercicios de todas las escalas, incluido Cyber Storm. • Ha fortalecido la resiliencia de la seguridad a través de la planificación y ejecución de ejercicios. • Ha mejorado las relaciones y la cooperación con los stakeholders. • Ha ampliado las oportunidades de participación den todo el espectro de stakeholders.

Impacto en organizaciones (públicas y privadas)

EE.UU.

No.	Nombre de la Actuación	Organismo	Descripción	Estado	Resultados
5	**CyberSecure My Business**	NCSA Iniciativa Stop, Think, Connect	Programa nacional que ayuda a las **pymes** a aprender a ser más seguras en línea. Se basan en el Framework NICE para realizar talleres de fácil comprensión.	Activo	El material es interactivo, incluyendo webinars con expertos de diferentes campos y un portal de recursos exclusivo para pymes. Su principal aporte está en: • Ayudar a lograr identificar y comprender los activos o recursos más valiosos para el negocio, y aprender a protegerlos. • Ayudar a responder con rapidez para minimizar el impacto de los ciberataques e implementar un plan de acción. • Aprender qué recursos son necesarios para recuperarse luego de un incidente.
6	**Cyber Resilience Review (CRR) Assesment.**	DHS, CISA Iniciativa Cyber Resource Hub	**Evaluación** no técnica, voluntaria y sin coste para evaluar la resiliencia operativa y las prácticas de ciberseguridad de una organización. Puede realizarse como una autoevaluación o como una evaluación onsite facilitada por profesionales de ciberseguridad del DHS.	Activo	Evaluación diseñada para medir la resiliencia organizacional existente, así como para proporcionar un análisis de brechas para mejorar basado en las mejores prácticas reconocidas. • Otorgar una conciencia más solida sobre la postura de ciberseguridad, haciendo énfasis en la necesidad de una gestión eficaz. • Revisar las capacidades esenciales para la continuidad de los servicios críticos durante los desafíos operativos y las crisis.

Impacto en organizaciones (públicas y privadas)

EE.UU.

Key *takeaways*

Los ejercicios cibernéticos de simulación han ido evolucionando desde inicios del año 2000 satisfactoriamente, convocando y reuniendo a diferentes jugadores relevantes de la industria para medir y fortalecer las capacidades que permiten una mejor respuesta a los incidentes actuales.

El enfoque central para fortalecer y aumentar la fuerza laboral está en poner a disposición de las organizaciones y profesionales los programas de estudio, cursos y herramientas necesarias, como lo demuestran programas como el *Continuous Diagnostics and Mitigation (CDM*) y el *FedVTE.*

Ayudarle a las pymes a entender los riesgos a los que están expuestos es una prioridad. Prueba de ello son los más de 10.000 participantes y 5.000 talleres realizados en el programa *Cyber Secure My Business*.

Que las organizaciones se autoevalúen en relación con prácticas de ciberseguridad probadas en el mundo real, es una manera óptima de conocer de manera detallada las áreas críticas de mejora de cada organización.

Implementar estas actuaciones es posiblemente la antesala a tener conversaciones realmente estratégicas a cerca del desempeño y la seguridad de las organizaciones públicas y privadas.

Gap de la fuerza laboral en ciberseguridad

EE.UU.

Para analizar el gap de la fuerza laboral en EE.UU. se ha consultado el estudio del (ISC)2 denominado 'Cybersecurity Workforce Study 2020'.

Este año, a pesar de los desafíos económicos por la COVID-19, por primera vez se vio disminuir el gap de la fuerza laboral en ciberseguridad

Global GAP 2019
4 M

- **La brecha en EE. UU. se redujo de 498.000 a 359.000**

- El menor gap del año 2020, a pesar de la incertidumbre y decrecimiento económico, no indica un menor número de aplicantes en ciberseguridad, es probable que la razón sea una entrada continua de profesionales junto con una demanda reducida debido a las condiciones difíciles en las organizaciones.

Global GAP 2020
3.12 M

- La mayoría de empleadores (excluidos las grandes empresas) están reportando menos inversión en contratación de profesionales en ciberseguridad. Este es el principal driver de estimación del gap.

Fuente: *(ISC)2 Cybersecurity Workforce Study*, 2020

Impacto en profesionales de ciberseguridad

EE.UU.

Para reducir este gap en talento y preparar mejor a los profesionales, EE.UU adopta las siguientes iniciativas y actuaciones:

La herramienta más robusta de la que se pueden beneficiar los profesionales es el ***framework*** **NICE**, considerando las herramientas dinámicas que permiten navegar el contenido de manera que puedan enfocarse en los conocimientos más idóneos para los diferentes planes de carrera.

- **NICE Workforce Framework**
  - **NICE Framework Mapping Tool**
    - **Cyber Career Pathways Tool**

CISA pone a disposición múltiples recursos de apoyo a los profesionales para orientarlos en su formación y capacitación, como lo demuestran algunas de las siguientes actuaciones:

Cybersecurity Resources

Herramientas para el empleo:
Tiene secciones que llevan a publicaciones en diferentes áreas de la ciberseguridad: Cybersecurity Workforce Challenges, CISA Workforce Resources and Tools, Education Resources, Cybersecurity Training Forces, Community College Training Resources and External Cybersecurity Resources.

I.2. NICCS
Organiza: CISA

NICCS Education and Training Catalog

Plataforma para la formación:
Catálogo con más de 5,000 cursos y cuenta con un mapa interactivo y filtros para una mejor experiencia de búsqueda. El objetivo es que el profesional pueda desarrollar habilidades, aumentar el nivel de experiencia, obtener certificaciones o incluso hacer la transición a una nueva carrera.

I.2. NICCS
Organiza: CISA

Cybersecurity Careers

Plataforma para el empleo:
En conjunto con USAJOBS, es una plataforma de empleo que lista diversas vacantes o posiciones disponibles en el mercado.

I.2. NICCS
Organiza: CISA

Cybersecurity Advisories & Technical Guidance

Documentos guía para la formación:
La NSA aprovecha su capacidad técnica de élite para desarrollar avisos y mitigaciones sobre las amenazas de ciberseguridad en evolución. Este es un repositorio con hojas de información, informes técnicos y avisos de riesgo.

Organiza: National Security Agency (NSA)

El éxito depende de una evaluación interna de los skills y conocimientos, identificar áreas críticas que requieran refuerzo, y construir programas personalizados que incluyen formación a nivel interno y externo, educación y mentoring.
Las estrategias de contratación diseñadas específicamente para llenar los gaps identificados en los diferentes perfiles, son clave.

Impacto en estudiantes

EE.UU.

En un contexto actual donde la virtualidad cobra absoluta relevancia, la importancia de la ciberseguridad, y la necesidad de un alto nivel de conciencia, son indiscutibles.

EE.UU se esfuerza por construir un futuro en el que las necesidades de ciberseguridad sean satisfechas por una fuerza laboral conocedora, capacitada y apasionada. Para ello tiene diferentes iniciativas, entre ellas destaca la tarea que lleva a cabo con cyber.org, que no solo es de gran valor para estudiantes y profesores, sino que realiza campañas de concienciación en temas como *ransomware*, *phishing*, y otros temas de interés en seguridad.

Uno de los pilares fundamentales del enfoque en EE.UU es **empoderar a los profesores a través del diseño de currículos de manera gratuita** (patrocinados por CISA), para que los estudiantes desarrollen las capacidades que serán demandadas para cubrir las necesidades de ciberseguridad de todo el país.

Los programas de becas patrocinados por el gobierno como CyberCorps, habilitan el desarrollo de competencias en ciberseguridad, otorgando beneficios al estudiante con la condición de que trabajen posteriormente para el gobierno, directamente en agencias federales como el mismo DHS, CISA, NSA, DoD, FBI, CIA, y demás.

CYBER.ORG, anteriormente NICERC

Formación para estudiantes y profesorado:
La misión es asegurar que cada estudiante de K-12 adquiera conocimientos y habilidades fundamentales y técnicos en ciberseguridad. Ha llegado a más de 18.000 profesores, e impactado a tres millones de alumnos en todo EEUU.

Organiza: CISA

Stop.Think. Connect Toolkit

Documentos guía para la formación de todos los stakeholders :
Recursos para todos los segmentos de la comunidad, incluso para niños, en todo tipo de temas (IoT, Internet Security, Phishing, etc.)

I.3. Stop. Think. Connect
Organiza: CISA

OnRamp II Scholarship Program

Programa de becas:
Programa que fomenta las asociaciones educativas entre la NSA y las instituciones académicas para promover la salud técnica y la diversidad de los estudiantes en ciencia, tecnología, ingeniería y matemáticas (STEM).

Organiza: NSA

CyberCorps: Scholarship for Service

Programa de becas:
Este programa ofrece becas para la educación de pregrado y posgrado (MS o PhD) en ciberseguridad financiadas a través de subvenciones otorgadas por la National Science Foundation (NSF).

I.2. NICCS
Organiza: CISA

NCSAM Resources (Publicaciones)

Documentos guía para la formación de todos los stakeholders:
Publicaciones con múltiples temáticas. Se anima a que estos recursos sean usados y compartidos para fomentar una ciberseguridad solida en todo el país.

I.4. NCSAM
Organiza: CISA

EE.UU se caracteriza por el contenido disponible online gratuito, haciendo uso de herramientas digitales para diseñar planes y estrategias de formación. La relevancia que tiene el mundo digital en las actividades cotidianas es fácilmente visible, pero la respuesta a los ciberataques no lo es, y ante esto NICCS resalta que el talento en ciberseguridad no es solo código y hacking, de tal forma que motive a los estudiantes a conocer las diferentes opciones de carrera.

Impacto en profesores y/o docentes de ciberseguridad

EE.UU.

En el contexto actual, la tecnología y la conectividad se encuentran presentes en casi todas las facetas de la vida, especialmente en los niños y jóvenes. **Ante esto, la ciberseguridad no puede tratarse como un tema aislado de las iniciativas de enseñanza, más aún cuando la virtualidad se consolida cada vez más.** Los profesores que comprenden esta realidad y abordan la ciberseguridad de manera integral, marcarán el camino para formar estudiantes más seguros y mejor preparados para el futuro.

Desde una perspectiva educativa, hay una escasez de acceso a profesores y currículos de ciberseguridad. En ese sentido, el DHS se esfuerza por proporcionar a los educadores los recursos necesarios para capacitar a los estudiantes, y que estos se conviertan en miembros de la fuerza laboral de ciberseguridad.

El programa CETAP *(Cybersecurity Education Training Assistance Program)*, promueve la ciberseguridad en las aulas de clase a través de currículos de estudio que según testimonios de los profesores, no solamente son entendibles, sino tienen un componente pragmático que permite su uso en **proyectos que reflejan escenarios del mundo real**.

Cyber.org es la iniciativa que busca empoderar a los docentes a través de planes de estudio diseñados para impactar las capacidades en ciberseguridad. **Ha logrado ayudar a más de 18.000 docentes.**

El desarrollo profesional aportado por el **National Cyber Group** a docentes, se basa en el mejoramiento de sus capacidades para entregar contenido en STEM y ciberseguridad.

CYBER.ORG, anteriormente NICERC

Formación para estudiantes y profesorado: La misión es asegurar que cada estudiante de K-12 adquiera conocimientos y habilidades fundamentales y técnicos en ciberseguridad. Ha llegado a más de 18.000 profesores, e impactado a tres millones de alumnos en todo EEUU.

Organiza: CISA

Cybersecurity in the Classroom

Formación:
Equipa a los profesores de K-12 con programas de estudio y herramientas de educación sobre ciberseguridad. A través de la subvención CETAP, Cyber.org, Bossier City, Louisiana, desarrolla y distribuye planes de estudios gratuitos sobre ciberseguridad, STEM y ciencias de la computación para educadores de K-12.
I.2. NICCS
Organiza: CISA

Professional Development

Formación:
Un conjunto de herramientas de desarrollo profesional "virtuales" estará disponible para todos los educadores, así como conferencias regionales anuales que reunirán a expertos del sector público / privado, educadores y consejeros de orientación.

I.8. National Cyber Education Program
Organiza: National Cyber Group

La transición al aprendizaje en línea causado por la COVID-19 y la vulnerabilidad del ecosistema hace necesario fortaleces las capacidades en ciberseguridad. Los profesores deben aportar a la seguridad de los estudiantes al transmitir las ventajas pero especialmente los riesgos del uso de Internet. Tener conversaciones transparentes y abiertas sobre la seguridad en línea son puntos de partida clave.

Análisis *benchmark*

Diversidad en tecnología

EE.UU.

- El estudio refleja una disparidad de empleo en las minorías étnicas en el sector de tecnología.
- Hay ligeramente más mujeres que hombres en EE.UU, su participación en las 50 compañías top en roles de tecnología se encuentra en promedio en el 44%.
- La participación de mujeres en roles de tecnología en el congreso llega solamente al 20%.
- Empleados latinos y afroamericanos están, en general, muy poco representados, con participaciones que no llegan al 10%.
- Según datos de DataUSA, esto se encuentra alineado con la industria de ciberseguridad: Un estudio de 2016 para el puesto de analista de seguridad de la información muestra que para esta posición el 74% son trabajadores blancos, 11.9% afroamericanos y 7.9% asiáticos.
- La brecha salarial sigue siendo notable, mientras el salario promedio de un analista de seguridad en el caso de los hombres puede estar cercano a los $110K, el de las mujeres ronda los $88K.
- Un hecho que genera alarmas es que a pesar de la poca representación de las minorías, se presentan casos donde alguna persona de este grupo ocupa un cargo directivo en ciberseguridad, con mayores aptitudes y capacidades que sus homólogos, sin embargo, su salario es menor.

Fuente: Information is Beautiful y DataUSA

Inclusión

EE.UU.

Según datos de (ISC)2, las mujeres representan el 24% de la fuerza laboral en ciberseguridad para el año 2019. Si bien es cierto este porcentaje viene creciendo especialmente entre los millennials, aún existen brechas en la escala salarial con respecto a los hombres.
A través de Cyber.org, en asociación con Palo Alto y la iniciativa *Girl Scouts*, se han desarrollado 18 placas de ciberseguridad que se han llevado a más de 200.000 personas. Esta es una manera interactiva (sin fines de lucro) y de fácil uso que logra impactar considerablemente el gap de mujeres en ciberseguridad.

Por otra parte, la inclusión de personas con discapacidad es abordada en los EE.UU. en actuaciones como *AcessCSforAll,* en la que trabajan por aumentar la **participación exitosa de los estudiantes con discapacidades.** Esta asociación de investigadores y profesionales tiene socios a lo largo del país, como code.org, y prestan servicios a estudiantes sordos, ciegos y con otras discapacidades. El enfoque lo ponen en la ciencia de la computación, desarrollando recursos como motores de búsqueda de conocimientos, casos de estudio, mejores prácticas, guías para una educación accesible en el K-12 y servicios a la comunidad de educadores para compartir herramientas y planes de estudio para enseñar con eficacia.

Las principales iniciativas/actuaciones que van en esa dirección se aprecian a continuación:

girl scouts

AccessCSforAll Including Students with Disabilities in High School Computing Education

women in CYBERSECURITY WiCyS

MiC Minorities in Cybersecurity

International Consortium of Minority CYBERSECURITY PROFESSIONALS

**Salvo el grupo de mujeres y a pesar de los esfuerzos realizados, la fuerza laboral de ciberseguridad no refleja diversidad.
Aparentemente las organizaciones no son consientes de que un equipo diverso en ciberseguridad, donde los problemas se resuelven a través de tener perspectivas holísticas de los desafíos, puede mejorar los resultados de los equipos.**

ISC2: Consorcio internacional de certificación de seguridad de sistemas de información

Inversión

EE.UU.

Los recursos asignados a las diferentes iniciativas contenidas en el análisis son gestionados dentro del presupuesto del DHS para 2021.

El presupuesto total del DHS para 2021 es de 49,8 billones de dólares netos discrecionales
La inversión en CISA se presenta como respuesta a querer mejorar en defensa digital.

- 1,1billones de dólares para defender y asegurar el ciberespacio, que incluye fondos para el programa '*Continuous Diagnostics and Mitigations (CDM)'* con una asignación de 281millones de dólares, lo que proporcionará la base tecnológica para asegurar y defender la infraestructura de TI contra amenazas.

- 157,6 millones de dólares para comunicaciones de emergencia para entidades federales, estatales, locales, tribales y territoriales. Este programa permite mejorar los servicios de comunicaciones de seguridad pública a nivel nacional mediante la provisión de las herramientas, la capacitación y la información necesarias para comunicarse durante las operaciones de emergencia.

- 91,5 millones de dólares para fortalecer la infraestructura crítica y abordar el riesgo a largo plazo de las funciones críticas nacionales, incluidas las actividades relacionadas con la seguridad electoral, los pilotos 5G y el análisis de riesgos de la cadena de suministro.

El presupuesto total asignado para CISA asciende a 1,7 billones de dólares

Conclusiones

VARIABLE	USA	DETALLE
***Framework* para el talento de ciberseguridad**		Herramienta bastante robusta que a partir de un lenguaje común genera valor ecosistema de ciberseguridad. Sus principales atributos son la flexibilidad, interoperabilidad, y los bloques de KSA que alimentan casos de uso.
Importancia del talento dentro de la estrategia de ciberseguridad		Alta relevancia que obedece a reconocer la escasez crítica de talento actual. La estrategia refleja la dependencia del reclutamiento y la retención de profesionales capacitados para lograr la ejecución de sus responsabilidades.
Impacto en organizaciones (públicas y privadas)		El bloque de organizaciones, especialmente del gobierno es donde está más fortalecido el ecosistema del talento para la seguridad. La mayoría de actuaciones se encuentran enfocadas a este segmento.
Impacto en profesionales en ciberseguridad		El mayor impacto es a través del Framework NICE, y además hay acciones aparte que buscan lograr posicionar efectivamente a los profesionales, haciendo uso de plataformas digitales para el empleo y formación.
Impacto en estudiantes		Refleja una red integral de instituciones educativas en 48 estados, reconocidas por el DHS y NSA en temas de ciberseguridad. Esto es lo que refuerza las actuaciones para generar mejores planes de estudios y becas.
Impacto en profesores y/o docentes de ciberseguridad		Las iniciativas más visibles son alrededor de los currículos de estudios, para que los docentes tengan las herramientas adecuadas para la enseñanza. El foco lo ponen en mantener a salvo a los niños de cualquier ataque.
Inclusión (minorías, discapacitados, veteranos)		Hay diferentes actuaciones con diferentes grupos, el resultado reciente más positivo está en las mujeres, pero las minorías son poco representadas y su salario no es una motivación para generar un mayor interés.
Inversión		La cantidad de recursos se divide en ciberseguridad, infraestructura y comunicaciones. Se enfocan en defender hoy para asegurar el mañana, estableciendo alianzas para afrontar incidentes y entender riesgos.

 No iniciada

 Incipiente

 En proceso

 Desarrollada

 Muy desarrollada

Conclusiones y recomendaciones

- *La estrategia que esta implementando EE.UU. a través del DHS es robusta y está enfocada a la parte de seguridad nacional, sin embargo, es notable que el talento y el **desarrollo de capacidades en ciberseguridad es una parte fundamental** de esta estrategia.*
- *La estrategia está alineada con el framework para la gestión del talento, en tanto comparte una secuencia lógica en sus objetivos y acciones planteadas para **identificar, desarrollar, reclutar y retener** el talento.*
- *El **framework NICE** es el modelo que vertebra el trabajo en ciberseguridad en EE.UU. y además de aportar el lenguaje necesario para promover un fácil entendimiento, le otorga a las organizaciones una hoja de ruta clara y flexible de cómo nutrir el talento para beneficio de todos los actores del ecosistema.*
- *Es fundamental reconocer que los objetivos relacionados con el talento dentro de una estrategia de ciberseguridad solo se alcanzar a través de la **creación de agencias, iniciativas y asociaciones estratégicas** con partners. Prueba de esto es la misma CISA, NIST y coordinaciones con el DoD para programas de excelencia académica.*
- ***Las principales iniciativas que EE.UU. propone para fortalecer el desarrollo del talento** y mitigar riesgos giran alrededor de: ejercicios de simulación, programas educativos y de capacitación, herramientas para el desarrollo profesional, centros de recursos o guías informativas, programas de becas y campañas de concienciación enfocados esencialmente a profesionales en las organizaciones, estudiantes, docentes y minorías.*
- ***Identificar el gap del talento al interior de las organizaciones públicas y privadas** es el primer paso para lograr estrategias potentes de gestión del talento. Esto es visible en el caso de uso de JP Morgan, donde se establece el diagnostico de la fuerza laboral como punto de partida para encontrar áreas críticas.*
- ***Alinear las funciones que se requieren en las organizaciones con los roles de trabajo en ciberseguridad** del framework teniendo en cuenta las capacidades, skills y tareas a realizar es la clave para lograr un mejor fit entre los profesionales y las posiciones de trabajo, además de impulsar el desarrollo profesional.*
- ***Los resultados del trabajo en ciberseguridad son por lo general el resultado de esfuerzos conjuntos de grupos diversos de trabajo.** Por eso la necesidad de balancear la fuerza laboral de ciberseguridad y lograr la inclusión apropiada de diferentes grupos étnicos a través de una cultura diversa e inclusiva.*

Anexos EE.UU.

Cyber Storm: Securing Cyber Space

Iniciativa	1. Cybersecurity Training and Exercises	Organismo	CISA y DHS

Objetivos de la Actuación

- Evaluar qué tan preparados están en ciberseguridad y examinar los procesos de respuesta a incidentes, los procedimientos y el intercambio de información.
- Fortalecer la preparación cibernética en los sectores público y privado y de esta manera asegurar el espacio cibernético.
- Ejercer la toma de decisiones estratégicas y la coordinación entre agencias de respuesta a incidentes de acuerdo con las políticas y procedimientos a nivel nacional.
- Validar las relaciones de intercambio de información entre agencias.

Financiación

- Propia a través del Departamento Nacional de Seguridad (DHS)

Descripción

- Proporciona el framework ciberseguridad patrocinado por el gobierno más amplio de su tipo.
- Proporciona un lugar para que los jugadores simulen el descubrimiento y la respuesta a un ciberataque coordinado generalizado que afecte la infraestructura crítica de la nación.
- Tres días de ejercicios en vivo, Cyber Storm es la serie de ejercicios de ciberseguridad más extensa del país. Hay varias ediciones.

Foco

- Sector público y privado.
- Alcance nacional e internacional

Resultados / Impacto

El ejercicio VI llevado a cabo en 2018 logró evaluar capacidades de respuesta de la nación a los incidentes cibernéticos a la infraestructura. Se ha evaluado la planificación de respuesta y la resiliencia. En esta edición participaron sectores de manufacturing, transportation, ICT y hubo alcance estatal, federal e internacional.

Tipo de programa

- Ejercicios de simulación.
- Formación.
- Guías informativas.

Estrategia de Ciberseguridad de Estados Unidos

Department of Homeland Security (DHS)

¿Qué es?

La estrategia de ciberseguridad del DHS, establece cinco pilares de un enfoque de gestión de riesgos en todo el DHS y proporciona un marco para ejecutar las responsabilidades de ciberseguridad y aprovechar la gama completa de capacidades del departamento para mejorar la seguridad y la resiliencia del ciberespacio.

¿Qué busca esta estrategia?

- Crear un ciberespacio seguro para el pueblo estadounidense y proteger un Internet interoperable, abierto, seguro y resiliente.
- *El término ´ciberespacio' en esta estrategia se refiere a la red interdependiente de infraestructura de tecnología de la información, incluyendo Internet, redes de telecomunicaciones, ordenadores, sistemas de información y comunicaciones, y procesadores y controladores integrados.*

¿Cómo lo logra?

- Reducir el riesgo de ciberseguridad nacional requiere un **enfoque innovador que aproveche al máximo las capacidades colectivas** en todo el Departamento y en toda la comunidad de ciberseguridad. El DHS se esforzará por comprender mejor la postura de riesgo de ciberseguridad nacional y colaborará con socios clave para abordar colectivamente las vulnerabilidades, amenazas y consecuencias cibernéticas. Nos basaremos en los esfuerzos continuos para reducir y gestionar las vulnerabilidades de las redes federales y la infraestructura crítica para protegerlas contra los atacantes. Reduciremos las amenazas de la actividad delictiva cibernética mediante la intervención prioritaria de las fuerzas del orden. Buscaremos mitigar las consecuencias de los incidentes de ciberseguridad que se produzcan.
- Finalmente, **nos comprometeremos con la comunidad global de ciberseguridad para fortalecer la seguridad y la resiliencia de los ecosistemas cibernéticos** en general al abordar desafíos sistémicos como cadenas de suministro cada vez más globales; **fomentando mejoras en la colaboración internacional** para disuadir a los ciberactores malintencionados y **desarrollar capacidades**; **aumentando la investigación y el desarrollo y mejorando nuestra fuerza de trabajo cibernética**.

Framework para el talento CS

NICE Framework

Desarrollado con el DHS y el secretario de defensa, es el **plan para categorizar, organizar y describir el trabajo de ciberseguridad.** Establece un conjunto común de términos para describir el trabajo en ciberseguridad, lo que **facilita a los profesionales de la ciberseguridad la comunicación de conocimientos, habilidades, capacidades y tareas con empleadores, educadores y entre ellos**.

Proporciona a los estudiantes, educadores, empleadores, empleados, proveedores de capacitación y formuladores de políticas un sistema consciente y sistemático para organizar la forma en que se piensa y se hablar sobre el trabajo en ciberseguridad, y para identificar los conocimientos, habilidades y destrezas necesarias para realizar tareas de ciberseguridad.

El *framework* se compone de lo siguiente:

- **7 Categorías:** una agrupación de alto nivel de funciones de ciberseguridad comunes.
- **33 Áreas de especialidad:** Áreas distintas de trabajo en ciberseguridad.
- **52 Roles de trabajo:** Las agrupaciones más detalladas de trabajo de ciberseguridad que comprenden conocimientos, capacidades y habilidades específicas *(knowledge, skills, and abilities)* necesarias para realizar tareas en un rol de trabajo.
- **Indicadores de capacidad:** Una combinación de educación, certificación, capacitación, aprendizaje experimental y atributos de aprendizaje continuo que podrían indicar una mayor probabilidad de éxito para un determinado rol de trabajo.

Organiza: Cybersecurity & *Infrastructure Security Agency* (CISA).

Iniciativa: *National Initiative for Cybersecurity Careers and Studies* (NICCS).

Tipo de Programa: *Framework* para la fuerza laboral.

NICE Framework Mapping Tool

Conecta las posiciones de ciberseguridad con el *framework* NICE. La herramienta de mapeo **permite a los profesionales de recursos humanos crear descripciones de puestos** a través del conocimiento, habilidades, capacidades y tareas del *framework* NICE. Ayuda a los managers a determinar los mejores conjuntos de habilidades y posibles brechas para sus equipos de ciberseguridad. El mapa interactivo filtra cursos por ubicación, área de especialidad, proveedor y nivel de habilidad.

Organiza: Cybersecurity & *Infrastructure Security Agency* (CISA).

Iniciativa: *National Initiative for Cybersecurity Careers and Studies* (NICCS).

Tipo de Programa: Herramienta del NICE *framework*.

Cyber Career Pathways Tool

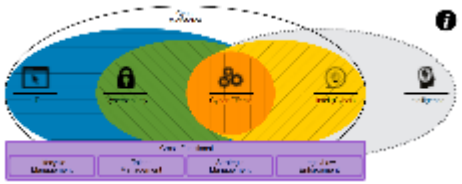
Ayuda a las personas a **identificar, construir y navegar una posible trayectoria profesional en cibernética** al aumentar la comprensión del conocimiento, las capacidades y las habilidades necesarias para comenzar, hacer la transición o avanzar en una carrera cibernética. **Las personas de diversos orígenes y grupos de edad pueden usar la herramienta para comprender mejor la fuerza de trabajo cibernética, además de los diferentes tipos de roles de trabajo cibernético y su relación entre ellos**. La herramienta se creó y se mantiene en asociación con el grupo de trabajo interagencial Federal Cyber Career Pathways, dirigido por CISA, el Departamento de Defensa y el Departamento de Asuntos de Veteranos.

Presenta una forma nueva e interactiva de explorar los roles laborales dentro del *framework* NICE. **Describe a la fuerza laboral cibernética como cinco comunidades de habilidades distintas pero complementarias. También destaca los atributos centrales entre cada uno de los 52 roles laborales** y ofrece información útil para empleadores, profesionales e individuos que estén considerando una carrera en cibernética.

Organiza: Cybersecurity & *Infrastructure Security Agency* (CISA).

Iniciativa: National Initiative for Cybersecurity *Careers and Studies* (NICCS).

Tipo de Programa: Herramienta del NICE *framework*.



Actores del ecosistema - EEUU

- Empresas y organizaciones
- Profesionales en ciberseguridad
- Estudiantes
- Profesorado
- Minorías

1.1 Actuaciones mpresas y organizaciones

1. Cyber Storm: Securing Cyber Space

Ejercicios de simulación:
Ejercicios cibernéticos que reúnen al sector público y privado para simular la respuesta a una crisis cibernética que afecta la infraestructura crítica de la nación.

I.1. Cybersecurity training and excercises
Organiza: CISA y DHS.

2. Continuous Diagnostics and Mitigation (CDM)

Formación:
Múltiples recursos de formación - Proporciona un enfoque dinámico para fortalecer la ciberseguridad de las redes y sistemas gubernamentales. Incluye certificaciones.

I.1. Cybersecurity training and excercises
Organiza: CISA.

3. National Cyber Exercise and Planning Program

Formación y ejercicios de simulación:
CISA desarrolla y respalda planes integrados de respuesta a incidentes cibernéticos, y orientación y ejercicios centrados en el ciberespacio para socios gubernamentales y de infraestructura crítica.

I.1. Cybersecurity training and excercises.
Organiza: CISA.

4. Incident Response Training

Formación:
Capacitación sin coste sobre respuesta a incidentes de seguridad cibernética para empleados y contratistas del Gobierno, y está abierto a actividades educativas y socios de infraestructura crítica.

I.1. Cybersecurity training and excercises.
Organiza: CISA

5. President's Cup Cybersecurity Competition

Competencia:
Competencia cibernética nacional que tiene como objetivo identificar, reconocer y recompensar a los mejores talentos en ciberseguridad en la fuerza laboral federal.

I.1. Cybersecurity training and excercises.
Organiza: CISA

6. CISA Tabletop Exercise Package

Documentos guía para la formación:
Diseñado para ayudar a los propietarios y operadores de infraestructura crítica a desarrollar sus propios ejercicios de mesa para satisfacer las necesidades específicas de sus instalaciones y las partes interesadas.

I.1. Cybersecurity training and excercises.
Organiza: CISA.

1.2 Actuaciones empresas y organizaciones

7. Federal Virtual Training Environment (FedVTE)

Formación:
Sistema de capacitación en ciberseguridad gratuito, en línea y bajo demanda. Brinda capacitación en ciberseguridad a empleados del Gobierno, contratistas federales y veteranos militares.

I.2. NICCS
Organiza: CISA

8. Become a Provider

Herramienta de promoción:
Proveedores e instituciones pueden incluir cursos en el catálogo en el sitio web, mientras sean ofrecidos por organizaciones proveedoras de recursos de calidad.

I.2. NICCS
Organiza: CISA

9. National Centers of Academic Excellence in Cybersecurity

Programa con Universidades:
El DHS y la NSA están buscando colegios y universidades interesados en avanzar en el estudio de la ciberseguridad para defender los sectores de infraestructura, negocios y Gobierno de EE.UU.

I.2. NICCS
Organiza: NSA,DHS y CISA

10. CISA Cybersecurity Resources

Formación:
Para disminuir los riesgos de seguridad cibernética y protegerse, CISA ofrece recursos para compartir en sus comunidades y con sus partes interesadas durante todo el año.

I.4. NCSAM
Organiza: CISA

11. NCSAM Sample Social Media Posts and Graphics

Formación:
Se muestran ejemplos de publicaciones y gráficos en redes sociales para promover NCSAM en las organizaciones.

I.4. NCSAM
Organiza: CISA

12. Cybersecurity Governance Publications

Formación:
Estudios que identifican cómo los estados han utilizado políticas, etc. para ayudar a gobernar mejor la ciberseguridad como un tema estratégico de en los Gobiernos estatales y organizaciones del sector público y privado.

I.5. CISA Publications / Library
Organiza: CISA

1.3 Actuaciones empresas y organizaciones

13. RVA Mapped To The Mitre Att&Ck Framwork Infographic

Formación:
La CISA analizó y mapeó los hallazgos de *Risk and Vulnerability Assessments* (RVA) del año 2019 para proporcionar a las entidades de infraestructura crítica listas de rutas de ataque exitosos observados.

I.6. Cyber Resource Hub
Organiza: CISA

14. Cyber Hygiene Services

Formación:
Se ofrecen servicios de análisis y pruebas para ayudar a las organizaciones a reducir su exposición a amenazas, adoptando un enfoque proactivo para mitigar los vectores de ataque.

I.6. Cyber Resource Hub
Organiza: CISA

15. Cyber Resilience Review (CRR)

Programa de evaluación:
Evaluación no técnica, voluntaria y gratuita para evaluar la resiliencia operativa y las prácticas de ciberseguridad de una organización. Puede ser autoevaluación o una evaluación on-site facilitada por el DHS.

I.6. Cyber Resource Hub
Organiza: CISA

16. CyberSecure My Business

Programa para las pymes:
CyberSecure My Business es un programa nacional que ayuda a las pequeñas y medianas empresas (pymes) a aprender a ser más seguras en línea.

I.3. Stop. Think. Connect
Organiza: NCSA

17. Data Privacy Day

Concienciación empresarial:
El Día de la Privacidad de Datos es un esfuerzo internacional para empoderar a las personas y alentar a las empresas a respetar la privacidad, salvaguardar los datos y generar confianza.

I.3. Stop. Think. Connect
Organiza: NCSA

18. Identity Management Day

Concienciación empresarial:
Día para educar a los líderes empresariales, y de TI sobre la importancia de la gestión de identidades y los componentes clave, las mejores prácticas de seguridad centradas en la identidad, etc.

I.3. Stop. Think. Connect
Organiza: NCSA

2.1 Actuaciones profesionales

1. Cybersecurity Resources

Herramientas para el empleo:
Tiene secciones que llevan a publicaciones en diferentes áreas de la ciberseguridad: Cybersecurity Workforce Challenges, CISA Workforce Resources and Tools, Education Resources, Cybersecurity Training Forces, Community College Training Resources and External Cybersecurity Resources.

I.2. NICCS
Organiza: CISA

2. Cybersecurity Careers

Plataforma para el empleo:
USAJOBS, es una plataforma de empleo que lista diversas vacantes o posiciones disponibles en el mercado.

I.2. NICCS
Organiza: CISA

3. NICCS Education and Training Catalog

Plataforma para la formación:
Catálogo con más de 5.000 cursos relacionados con la ciberseguridad. Cuenta con un mapa interactivo y filtros para buscar cursos ofrecidos para que puedan agregar a su conjunto de habilidades, aumentar su nivel de experiencia, obtener una certificación o incluso hacer la transición a una nueva carrera.

I.2. NICCS
Organiza: CISA

4. Cybersecurity Advisories & Technical Guidance

Documentos guía para la formación:
La NSA aprovecha su capacidad técnica de élite para desarrollar avisos y mitigaciones sobre las amenazas de ciberseguridad en evolución. Este es un repositorio con hojas de información, informes técnicos y avisos de riesgo.

Organiza: National Security Agency (NSA)

3.1 Actuaciones de estudiantes

1. CYBER.ORG, anteriormente NICERC

Formación para estudiantes y profesorado:
La misión es asegurar que cada estudiante de K-12 adquiera conocimientos y habilidades fundamentales y técnicos en ciberseguridad. Ha llegado a más de 18.000 profesores, e impactado a tres millones de alumnos en todo EE.UU.

Organiza: CISA

2. Students, Launch Your Cybersecurity Careers

Documentos guía para la formación:
Ofrece perfiles de trabajo de ciberseguridad, clases recomendadas para tomar e información sobre la fuerza laboral actual.

I.2. NICCS
Organiza: CISA

3. CyberCorps: Scholarship for Service

Programa de becas:
Este programa ofrece becas para la educación de pregrado y posgrado (MS o PhD) en ciberseguridad financiadas a través de subvenciones otorgadas por la *National Science Foundation* (NSF).

I.2. NICCS
Organiza: CISA

4. Stop.Think. Connect Toolkit

Documentos guía para la formación de todos los *stakeholders* :
Recursos para todos los segmentos de la comunidad, incluso para niños, en todo tipo de temas (IoT, Internet Security, *phising*, etc.)

I.3. Stop. Think. Connect
Organiza: CISA

5. NCSAM Resources (Publicaciones)

Documentos guía para la formación de todos los *stakeholders*:
Publicaciones con múltiples temáticas. Se anima a que estos recursos sean usados y compartidos para fomentar una ciberseguridad sólida en todo el país.

I.4. NCSAM
Organiza: CISA

6. OnRamp II Scholarship Program

Programa de becas:
Programa que fomenta las asociaciones educativas entre la NSA y las instituciones académicas para promover la salud técnica y la diversidad de los estudiantes en ciencia, tecnología, ingeniería y matemáticas (STEM).

Organiza: NSA

4.1 Actuaciones del profesorado

El DHS se esfuerza por proporcionar a los educadores los recursos necesarios para capacitar a los estudiantes para que se conviertan en miembros de la fuerza laboral de ciberseguridad con conocimientos digitales, utilizando la tecnología de manera segura.

1. CYBER.ORG, anteriormente NICERC

Formación para estudiantes y profesorado:
La misión es asegurar que cada estudiante de K-12 adquiera conocimientos y habilidades fundamentales y técnicos en ciberseguridad. Ha llegado a más de 18.000 profesores, e impactado a tres millones de alumnos en todo EE.UU.

Organiza: *CISA*

2. Cybersecurity in the Classroom

Formación:
Equipa a los profesores de K-12 con programas de estudio y herramientas de educación sobre ciberseguridad. A través de la subvención CETAP, Cyber.org, o Bossier City, Louisiana, desarrolla y distribuye planes de estudios gratuitos sobre ciberseguridad, STEM y ciencias de la computación para educadores de K-12 en todo el país. Estos programas se enfocan en el crecimiento y la educación de la fuerza laboral ciberalfabetizada de próxima generación.

I.2. NICCS
Organiza: *CISA*

3. Professional Development

Formación:
Un conjunto de herramientas de desarrollo profesional 'virtuales' estará disponible para todos los educadores, así como conferencias regionales anuales que reunirán a expertos del sector público/privado, educadores y consejeros de orientación.

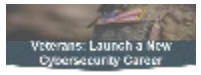
I.8. National Cyber Education Program
Organiza: National Cyber Group

5.1 Actuaciones de minorías

Veterans: Launch a New Cybersecurity Career

Formación:
Ofrece capacitación y educación en ciberseguridad para veteranos: una guía de usuario para quienes sirvieron anteriormente en las Fuerzas Armadas de EE.UU. Esta guía incluye una serie de herramientas y recursos para ayudar a los veteranos a comenzar una carrera en ciberseguridad, incluida capacitación en línea gratuita, información sobre programas de grado relacionados con la ciberseguridad e información sobre becas.

I.2. NICCS
Organiza: *CISA*



Women in Cybersecurity

Comunidad de profesionales. Red de apoyo:
Iniciativa que aborda la diversidad de género. Ayuda a empoderar a las mujeres que a menudo se sienten aisladas o excluidas en el lugar de trabajo al construir una comunidad profesional con la que puedan identificarse. No excluye un género sobre otro. Busca promover la diversidad en la industria de la ciberseguridad.

Iniciativa independiente con partners
Organiza: Women in Cybersecurity (privada)

Minorities in Cybersecurity

Comunidad de Profesionales. Red de apoyo:
MiC es una corporación sin fines de lucro dedicada al liderazgo y desarrollo profesional de su miembros. Se esfuerzan por crear una comunidad de profesionales de la ciberseguridad que apoyará, desarrollará, y ayudará a preparar a sus miembros para que no solo se destaquen en el campo de la ciberseguridad, sino que también logren su nivel personal de éxito profesional.

Organiza: Minorities in Cybersecurity (privada)

Cybersecurity Basics Badge Activity

Concienciación:
Como parte del bloque temático STEM, se realizan actividades de corto tiempo alrededor de diferentes temas, otorgando una placa como reconocimiento. Con toda la información que se comparte en internet, esta actuación busca en mujeres de temprana edad, llevarlas a pensar de una manera más consciente y cuidadosa sobre la privacidad y la protección de la información personal.

Iniciativa Independiente con partners
Organiza: Cyber.org y Girlscouts.org

AccessCSforAll

Formación:
En AccessCSforAll trabajan por aumentar la participación exitosa de los estudiantes con discapacidades en computación durante el K-12. Esta asociación de investigadores y profesionales tiene socios a lo largo del país, como code.org, y prestan servicios a estudiantes sordos, ciegos y con otras discapacidades.

Iniciativa Independiente con partners
Organiza: Universidad de Washington

International Consortium of Minority Cybersecurity Professionals

Comunidad de Profesionales. Red de apoyo:
El objetivo es lograr una representación consistente de mujeres y minorías en la ciberseguridad a través de programas diseñados para fomentar el reclutamiento, la inclusión y la retención. Funciona bajo membresía, y los servicios que ofrece es acceso a becas, desarrollo profesional y recursos para la formación.

Iniciativa Independiente con partners
Organiza: *ICMCP*

Anexo 1.1 Actuaciones EE.UU.- Empresas

1. Cyber Storm: Securing Cyber Space

- **Ejercicios cibernéticos que reúnen al sector público y privado para simular la respuesta a una crisis cibernética que afecta la infraestructura crítica de la nación**.
- Estos ejercicios pretenden evaluar qué tan preparados están en ciberseguridad y examinar los procesos de respuesta a incidentes, los procedimientos y el intercambio de información. También fortalecer la preparación cibernética en los sectores público y privado y de esta manera asegurar el espacio cibernético
- **Proporciona el *framework* patrocinado por el Gobierno más amplio de su tipo.** Proporciona un lugar para que los jugadores simulen el descubrimiento y la respuesta a un ciberataque coordinado generalizado. Tres días de ejercicios en vivo, Cyber Storm es la serie de ejercicios de ciberseguridad más extensa del país con tres días de ejercicios en vivo. Cuenta con varias ediciones.
- **Los participantes del programa Cyber Storm llevan a cabo las siguientes actuaciones:**
  - Examinar la **capacidad de las organizaciones** para prepararse, protegerse y responder a los efectos potenciales de los ciberataques.
  - Ejercer la toma de decisiones estratégicas y la coordinación entre agencias de respuesta a incidentes de acuerdo con las políticas y procedimientos a nivel nacional.
  - Validar las **relaciones de intercambio de información** y las rutas de comunicación para recopilar y difundir información sobre la situación, la respuesta y la recuperación de los incidentes cibernéticos.
  - Examinar los medios y procesos a través de los cuales compartir información confidencial a través de fronteras y sectores sin comprometer los intereses de seguridad nacional o de propiedad.
- **Cada Cyber Storm se basa en las lecciones aprendidas de incidentes anteriores del mundo real**, lo que garantiza que los participantes se enfrenten a ejercicios más sofisticados y desafiantes cada dos años.

2. Continuous Diagnostics and Mitigation (CDM)

- **Múltiples recursos de formación:** proporciona un enfoque dinámico para fortalecer la ciberseguridad de las redes y sistemas gubernamentales. **El programa CDM ofrece herramientas de ciberseguridad**, servicios de integración y paneles de control que **ayudan a las agencias** participantes a mejorar su postura de seguridad al:
  - Reducir la superficie de amenaza de la agencia.
  - Aumento de la visibilidad de la postura de ciberseguridad federal.
  - **Mejora de las capacidades de respuesta de ciberseguridad federal.**
  - Optimización del Federal Information Security Modernization Act (*FISMA*) reporting.
- **El CDM informa a los CIO, CISO, oficiales de seguridad del sistema de información y administradores de red** sobre el estado de la postura cibernética de sus redes.
- Se otorgan **certificaciones** por participar en webinars y otros eventos.

Anexo 1.2 Actuaciones EEUU - Empresas

3. National Cyber Exercise and Planning Program

- CISA **desarrolla y respalda planes integrados de respuesta a incidentes cibernéticos**, y orientación y ejercicios centrados en el ciberespacio para socios gubernamentales y de infraestructura crítica. Realiza un espectro completo de ejercicios en **cooperación con el sector público y privado y socios internacionales**, particularmente aquellos que apoyan la infraestructura crítica de los EE.UU.
- **Los objetivos son**:
  - Fortalecer la resiliencia de la ciberseguridad nacional a través de la planificación y ejecución de ejercicios cibernéticos.
  - Fomentar las relaciones y la cooperación con los *stakeholders*.
  - Ampliar las oportunidades de participación en todo el espectro de *stakeholders*.
- **Los productos claves de planeación disponibles incluyen:**
  - Cyber capabilities *planning framework*.
  - Sector-Specific *operations playbooks.*
  - State, Local, Territorial, Tribal (SLTT) Cyber Incident Annex Template.

4. Incident Response Training (Programa)

- Para respaldar la **capacidad denominada 'Defend Today, Secure Tomorrow'** en ciberseguridad de las organizaciones, CISA ha desarrollado una **capacitación sin coste** sobre respuesta a incidentes de seguridad cibernética para **empleados y contratistas del Gobierno** en todo elGobierno federal, estatal, local, tribal y territorial, y está abierto a actividades educativas y socios de infraestructura crítica.
- El **plan '*Identify, Mitigate, Recover* (IMR)'**, proporciona una gama de ofertas de capacitación para ciberprofesionales principiantes, intermedios y avanzados que abarcan concienciación en ciberseguridad, mejores prácticas, demostraciones de defensa de la red en vivo que emulan en tiempo real escenarios de respuesta a incidentes y cursos prácticos de capacitación de rango cibernético para profesionales de respuesta a incidentes. Los tipos de cursos incluyen: Awareness Webinars, Cyber Range Training, Cyber Range Challenges, y Observe the Attack.

5. President's Cup Cybersecurity Competition

- Establecida en respuesta a la Orden Ejecutiva 13870, es una competencia cibernética nacional que tiene como objetivo **identificar, reconocer y recompensar a los mejores talentos en ciberseguridad en la fuerza laboral federal**.
- Incluye desafíos en casi todo el espectro de la ciberseguridad y se da tanto en equipos como de manera individual.

Anexo 1.3 Actuaciones EE.UU. - Empresas

6. CISA Tabletop Exercise Package

- CISA Tabletop Exercise Package (*CTEP*) está diseñado para ayudar a los propietarios y operadores de infraestructura crítica a desarrollar sus propios ejercicios de mesa para satisfacer las necesidades específicas de sus instalaciones y partes interesadas. *CTEP* permite a los usuarios aprovechar las plantillas de ejercicios prediseñados y los escenarios examinados para crear ejercicios de mesa para evaluar, desarrollar y actualizar procesos de intercambio de información, planes de emergencia, programas, políticas y procedimientos.

7. Federal Virtual Training Environment (FedVTE)

- Es un **sistema de capacitación en ciberseguridad gratuito, en línea y bajo demanda**. Con cursos que van desde el nivel principiante hasta el avanzado, puede fortalecer o desarrollar las habilidades de ciberseguridad a un ritmo personalizado, FedVTE brinda capacitación en ciberseguridad a empleados del Gobierno federal, estatal, local, tribal y territorial, contratistas federales y veteranos militares.
- Los aspectos más destacados incluyen:
  - **Cursos de preparación para certificación:** prepara y capacita para la certificación de los cursos Certified Ethical Hacker, Cybersecurity Analyst (*CySA +),* Network + Security + Certified Information Security Manager (*CISM*) y Certified Information Systems Security Professional (*CISSP*).
  - **Acceso:** los cursos de FedVTE se pueden completar a ritmo personalizado, en cualquier momento utilizando un PC, ordenador portátil u otros dispositivos móviles.
  - **NICE Cybersecurity workforce *framework*:** todos los cursos se asignan a las categorías y áreas de especialidad del *framework* NICE para ayudar a identificar los cursos que se necesitan para el trabajo o aspiración.

8. Become a Provider

- Los proveedores e **instituciones interesados en incluir cursos** en el catálogo pueden postularse en el sitio web, cumpliendo ciertos criterios para asegurar que los cursos enumerados en el catálogo sean ofrecidos por organizaciones reconocidas como proveedoras de recursos de calidad.

Anexo 1.4 Actuaciones EE.UU. - Empresas

9. National Centers of Academic Excellence in Cybersecurity (*NCAE-C*)

- El (DHS) y la (NSA) están buscando colegios y universidades interesados en avanzar en el estudio de la ciberseguridad en un esfuerzo nacional para defender los sectores de infraestructura, negocios y Gobierno de EE.UU.
- El DHS y la NSA patrocinan conjuntamente el programa de los (*NCAE-C*). El objetivo del programa es reducir la vulnerabilidad en la infraestructura de información nacional mediante la **promoción de la educación superior y la experiencia en ciberseguridad**. Hay más de 300 colegios y universidades de primer nivel en 48 Estados, el distrito de Columbia y el Estado Libre Asociado de Puerto Rico designados como *NCAE* en ciberseguridad.

10. CISA Cybersecurity Resources

- Para disminuir los riesgos de seguridad cibernética y protegerse en línea, CISA ofrece los siguientes recursos para compartir en sus comunidades y con sus partes interesadas. Estas herramientas no solo son valiosas durante el mes NCSAM, sino durante todo el año.
  - *CISA's Telework Resources* – Telework Guidance and Best Practices.
  - *CISA's Cybersecurity Hub* – Assessments, Prevention, and Response Resources.
  - *CISA's Cyber Essentials* – Cybersecurity Awareness and Best Practices Resources.
  - *CISA's #Protect 2020* – Election Security and Disinformation Resources.
  - *National Risk Management* – Mitigating Cyber Risks To The Nation's Critical Infrastructure.

11. NCSAM Sample Social Media Posts and Graphics

- Se muestran ejemplos de publicaciones y gráficos en redes sociales para promover NCSAM en las organizaciones. CISA y NCSA promueven publicar en los canales de comunicación online antes y durante octubre para **difundir el mensaje de concienciación sobre ciberseguridad.**
  - Sample Twitter Posts.
  - Sample Facebook/LinkedIn Posts.

12. Cybersecurity Governance Publications (casos de estudio por Estado)

- El informe y los estudios de caso identifican cómo los estados han utilizado leyes, políticas, estructuras y procesos para ayudar a gobernar mejor la ciberseguridad como un tema estratégico de toda la empresa en los Gobiernos Estatales y otras partes interesadas del sector público y privado. El informe y los estudios de caso exploran los mecanismos de gobernanza entre empresas utilizados por los estados en una variedad de áreas comunes de ciberseguridad y ofrecen información sobre tendencias y conceptos útiles para otros Estados y organizaciones que se enfrentan desafíos similares.

Anexo 1.5 Actuaciones EE.UU. - Empresas

13. RVA Mapped To The Mitre Att&Ck *framework* infographic

- La CISA analizó y mapeó los hallazgos de risk and Vulnerability Assessments (*RVA*) del año 2019 para proporcionar a las entidades de infraestructura crítica listas de rutas de ataque exitosos observados. Así se puede ver cómo los adversarios se desvían y escalan, y el porcentaje de éxito de cada táctica y técnica. CISA anima a los administradores de red y profesionales de TI a revisar la infografía y aplicar las estrategias defensivas recomendadas para protegerse contra las tácticas y técnicas observadas.

14. Cyber Hygiene Services

- Estos servicios de análisis y pruebas se ofrecen para ayudar a las organizaciones a reducir su exposición a amenazas, adoptando un enfoque proactivo para mitigar los vectores de ataque.
- Vulnerability Scanning.
- *Phishing* Campaign Assessment.
- Web Application Scanning.
- Remote Penetration Test.

15. Cyber Resilience Review (*CRR*)

- El CRR es una evaluación no técnica, voluntaria y sin coste para evaluar la resiliencia operativa y las prácticas de ciberseguridad de una organización. El CRR puede realizarse como una autoevaluación o como una evaluación *onsite* facilitada por profesionales de ciberseguridad del DHS. El CRR evalúa los programas y prácticas empresariales en una variedad de diez dominios, incluida la gestión de riesgos, la gestión de incidentes, la continuidad del servicio y otros. La evaluación está diseñada para medir la resiliencia organizacional existente, así como para proporcionar un análisis de brechas para mejorar **basado en las mejores prácticas reconocidas**.
- Recibir una revisión de resiliencia cibernética proporcionará a una organización una **conciencia más sólida de su postura de seguridad** cibernética al proporcionar y facilitar lo siguiente:
  - **Mayor conciencia** en toda la empresa de la necesidad de una gestión eficaz de la ciberseguridad.
  - Una **revisión de las capacidades esenciales** para la continuidad de los servicios críticos durante los desafíos operativos y las crisis.
  - Comparaciones integradas de desempeño de otros pares, para cada uno de los 10 dominios cubiertos en la evaluación.
  - Un informe final completo que incluye opciones de mejora.

Anexo 1.6 Actuaciones EE.UU. - Empresas

16. CyberSecure My Business

- Es un programa nacional que ayuda a las pequeñas y medianas empresas (pymes) a aprender a ser más seguras en línea. El programa es una serie de talleres en persona, altamente interactivos y fáciles de entender basados en el *framework* de ciberseguridad del Instituto Nacional de Estándares y Tecnología (*NIST*) para educar a las pymes.

17. Data Privacy Day

- El día de la privacidad de datos es un esfuerzo internacional para empoderar a las personas y alentar a las empresas a respetar la privacidad, salvaguardar los datos y generar confianza.

18. Identity Management Day

- En colaboración con la Identity Defined Security Alliance (*IDSA*), y a realizar por primera vez en 2021, la misión de este día es educar a los líderes empresariales y a los tomadores de decisiones de TI sobre la importancia de la gestión de identidades y los componentes clave, incluido el Gobierno, las mejores prácticas de seguridad centradas en la identidad, los procesos y la tecnología, con un enfoque especial en los peligros de no proteger adecuadamente las identidades y las credenciales de acceso.

UK

UK

¿Qué orden seguiremos?

- Estrategia de Ciberseguridad y Estrategia de Talento en Ciberseguridad de UK.
- ¿Qué organismos participan y tienen competencias o acciones relacionadas con el talento de ciberseguridad?.
- Organismos con competencias en talento de ciberseguridad.
- Análisis *benchmark*.
- Conclusiones y recomendaciones.

Estrategia de ciberseguridad de UK

HM Government

UK

En primer lugar, la estrategia de ciberseguridad del Reino Unido define la ciberseguridad como la protección de los sistemas de información (*hardware, software e infraestructuras asociadas*), los datos en ellos, y los servicios que brindan, ante el acceso no autorizado, daño o uso indebido.

Objetivos de la estrategia

DEFENDER

UK cuenta con los medios para defenderse contra las amenazas cibernéticas en evolución, para responder de manera eficaz a los incidentes y garantizar que las redes, los datos y los sistemas estén protegidos y sean resilientes. Los ciudadanos, la empresa privada y el sector público tienen el conocimiento y las habilidades para defenderse.

DESARROLLAR

UK tiene una industria de ciberseguridad innovadora y en crecimiento, respaldada por I+D de clase mundial. Expresan que **cuentan con una tubería de talento autosostenible que proporciona las capacidades para satisfacer las necesidades del sector público y privado**. Se espera que los análisis y experiencia puntera permitan enfrentar y superar las amenazas y desafíos futuros.

DISUADIR

UK será un blanco difícil para todas las formas de agresión en el ciberespacio. Detectan, entienden, investigan y desarticulan las acciones hostiles, persiguiendo y procesando a los infractores. Tienen los medios para emprender acciones ofensivas en el ciberespacio, si así lo deciden.

La estrategia se centra en elevar los costos de organizar un ataque, tanto a través de defensas más fuertes como por medio de **mejores habilidades cibernéticas**. Ya no se trata solamente de algo que atañe al departamento de TI, **los *skills* cibernéticos tienen que tenerlas todas las profesiones.**

El impulso para **atraer a los talentos jóvenes más prometedores al ámbito de la ciberseguridad** se llevará a cabo desde el rol de liderazgo del Gobierno, pero fomentando un ecosistema de negocios más amplio que reconozca oportunidades de innovación para el sector de forma rápida.

Esta estrategia señala que utilizarán la autoridad y la influencia del Gobierno británico para **invertir en programas que respondan a la escasez de habilidades** en ciberseguridad, desde las escuelas y universidades, hasta toda la fuerza laboral.

Talento en ciberseguridad

Reconociendo que los ataques cibernéticos en el Reino Unido son cade vez más frecuentes, sofisticados y perjudiciales, la estrategia de ciberseguridad nacional presenta un **plan para alcanzar la confianza, capacidad y resiliencia** en un mundo digital que evoluciona rápidamente.

¿Cual es la principal iniciativa de esta estrategia para lograr este propósito?

National Cyber Security Centre

Estrategia de ciberseguridad de UK

HM Government

UK

El bloque de **DESARROLLO** de la estrategia establece **cómo conseguirán y fortalecerán las herramientas y capacidades** que necesita el Reino Unido para protegerse.

Uno de los resultados transformadores que espera alcanzar UK es asegurar que exista el mejor pipeline posible de talento en ciberseguridad.

Para este y otros fines se plantean los siguientes objetivos y acciones específicas en relación con el talento.

Objetivos

1. **Desarrollar e implementar una estrategia de talento autónoma que construya sobre el trabajo realizado e integre la ciberseguridad en el sistema educativo.**
2. **Reducir la brecha creciente** entre oferta y demanda de talento en ciberseguridad.
3. **Definir acciones a corto y largo plazo** que necesitan el Gobierno, las empresas y el sector educativo para establecer una tubería de **profesionales competentes y certificados**.
4. **Desarrollar y atraer skills y capacidades especializadas** que permitan seguirle el paso a la tecnología y gestionar los riesgos asociados.
5. **Responder al desequilibrio de género** en la profesión de ciberseguridad, llegando a ámbitos más diversos, asegurando que aprovechan un grupo de talento más amplio.
6. **Establecer claramente los roles del Gobiernos y las organizaciones.** Esto incluye las administraciones descentralizadas para crear un entorno adecuado y actualizar el sistema educativo para que refleje las necesidades de la demanda.
7. **Lograr que los organismos públicos y privados formen, capaciten y concienticen a los empleados y a los jóvenes que entran a la profesión.**
8. **Reforzar las iniciativas del Gobierno para incrementar el número de graduados en carreras a fin con la ciberseguridad.**
9. **Asegurar que las *start-up*s de ciberseguridad prosperen** y reciban la inversión y apoyo que necesitan.
10. **Establecer planes de carrera y rutas de formación en la profesión de ciberseguridad** que permitan un mayor *engagement* con los profesionales.

Acciones

1. **Establecer el NCSC.** Como un mecanismo que permite coherencia y una alianza eficaz entre el gobierno, empresas, profesionales, sector educativo y ciudadanos para apoyar el despliegue de una estrategia de largo plazo enfocada al talento.
2. **Establecer programas escolares para crear un cambio radical en la educación** y capacitación especializada en ciberseguridad, para jóvenes de 14 a 18 años (que incluye actividades en el aula, sesiones extracurriculares con mentores expertos, proyectos desafiantes y escuelas de verano).
3. **Crear asesoramiento sectorial experto que permita aprendizaje relevante** al Gobierno y sectores críticos como las telecomunicaciones, energía y financiero.
4. **Crear un fondo para reciclar talento** en la fuerza laboral, que evidencia un alto potencial para la profesión de ciberseguridad.
5. **Identificar y respaldar una educación de pre y posgrado de calidad –** reconociendo el rol clave que juegan las universidades en este proceso.
6. **Apoyar la acreditación del desarrollo profesional docente en ciberseguridad**.
7. **Desarrollar desde el gobierno una Academia Cibernética de Defensa** como un centro de excelencia para la capacitación y simulación cibernética.
8. **Invertir en oportunidades de colaboración público-privadas** en capacitación y educación. Esto refuerza el sistema educativo a todo nivel con un enfoque integral.
9. **Trabajar con las organizaciones para** expandir el programa CyberFirst, para **identificar y nutrir el grupo diverso de jóvenes talentos** para defender la seguridad.
10. **Brindar comunicaciones**. Creando conciencia en las organizaciones del sector público y privado sobre cómo lidiar con temas de ciberseguridad. Ejemplo: cyberaware.gov.uk

Adaptación y flexibilidad en la ejecución.

Department for Digital, Culture, Media & Sport

INITIAL NATIONAL CYBER SECURITY SKILLS STRATEGY

Estrategia de talento en ciberseguridad de UK

Department for Digital, Culture, Media & Sport – HM Government

UK

En el core de la Estrategia de Talento en Ciberseguridad de UK se encuentra **garantizar la combinación y el nivel adecuados de capacidades** en ciberseguridad en toda la economía. Establece sobre la base de la investigación y compromiso, la comprensión del Gobierno del contexto estratégico sobre el talento en ciberseguridad y el plan para desarrollar las capacidades de ciberseguridad a largo plazo.

La estrategia define el talento en ciberseguridad como la combinación de conocimientos y habilidades técnicas esenciales y avanzadas, habilidades de gestión estratégica, habilidades de planificación y organización y habilidades blandas complementarias que permiten a las organizaciones: **(1)** Entender el riesgo actual y futuro al que se enfrentan; **(2)** Crear y difundir *awareness* en ciberseguridad, buenas prácticas y las reglas a seguir en las organizaciones; **(3)** Implementar el control técnico y ejecutar las tareas para proteger a las organizaciones, basado en el nivel de amenazas; **(4)** Cumplir con los requisitos impuestos por la ley competente; **(5)** Investigar y responder efectivamente a los ataques actuales y futuros.

Components

Definition of Cyber Security Skills

BoK – Cyber Security

UK Cyber Security Council

1 **Asegurar que U.K. tenga una profesión bien estructurada y fácil de navegar que represente, respalde e impulse la excelencia en las diferentes especialidades de ciberseguridad, y sea sostenible y sensible al cambio.**

2 **Asegurar que U.K. tenga sistemas de educación y capacitación que proporcionen los componentes básicos adecuados para ayudar a identificar, capacitar y ubicar talentos de seguridad cibernética nuevos y sin explotar.**

Inspiring the workforce to retrain or upskill

NCSC – Certified Degrees Formal Education – Schools

Work with Developed Administrations (Wales)

Extracurricular Activities

Objetivos

Embedding basic cyber security universally

Embedding cyber security within professional decision making

Embedding cyber security within professional disciplines

3 **Garantizar que la fuerza laboral tenga la combinación adecuada y el nivel de habilidades necesarias para lograr una economía digital segura, con organizaciones resilientes con sede en U.K. en todos los sectores.**

4 **Asegurar que U.K. siga siendo un líder mundial en ciberseguridad con acceso al mejor talento, con un sector público que lidere los esfuerzos de desarrollo de capacidades cibernéticas.**

The public sector leading by example

Engaging Globally

El éxito de esta estrategia se basa en la colaboración que permite el trabajo conjunto y eficiente entre el Gobierno y *partners* de la industria

Organismos con competencias en talento de ciberseguridad

UK

National Cyber Security Centre

Brinda apoyo a los entes más críticos de UK en materia de ciberseguridad. Es posiblemente el organismo que mejor entiende la ciberseguridad, destila este conocimiento en acciones prácticas a disposición de su ecosistema y utiliza la experiencia académica y de la industria para fomentar las capacidades en Cyber.

HM Government

GCHQ

Agencia de inteligencia más grande de UK
Lidera el campo de la ciberseguridad. Ofrece apoyo y programas de mentoring para el desarrollo de skills en cyber, además de promover planes de carrera.

Government Security Profession

Organismo gubernamental que reúne a los profesionales de la seguridad que trabajan en el Gobierno para ayudarlos a adquirir habilidades y conocimientos.

UK CYBER SECURITY COUNCIL

Es el organismo al que el Gobierno ha encargado "**el desarrollo de un marco que habla de las diferentes especialidades**, estableciendo una alineación integral de trayectorias profesionales, incluidas las certificaciones y calificaciones requeridas en ciertos niveles.

ISACA

El propósito de esta comunidad **es ayudar a los profesionales de la tecnología a entender el** potencial de la tecnología. **Ofrecen múltiples recursos de formación. Operan bajo membresía.**

Llywodraeth Cymru
Welsh Government

El Gobierno de Gales, fomenta el desarrollo de clusters alrededor de la Ciberseguridad y es considerado un partner estratégico en UK para apoyar el desarrollo de capacidades en los estudiantes que garantice una oferta sostenible en el futuro.

Chartered Institute of Information Security

(CIISec) es la única institución que ha obtenido el estatus de *Royal Charter* y se dedica a elevar el nivel de profesionalismo en ciberseguridad. Gestionado por sus miembros, garantiza estándares para la capacitación, cualificaciones y prácticas operativas.

Department for Digital, Culture, Media & Sport

El **DCMS** tiene como prioridad el crecimiento de la economía, la conectividad en UK, promover el país en el exterior y ayudar a los negocios a través de la inversión en innovación. Analiza la industria de la ciberseguridad.

DIGITAL SKILLS PARTNERSHIP

A través de *Digital Skills Partnership* (DSP), lanzada en julio de 2017, trabajan para **unir a organizaciones de todos los sectores para abordar la brecha digital.** Una prioridad clave es apoyar la formación de DSP locales en las regiones, que diseñarán, desarrollarán y ofrecerán programas innovadores de habilidades digitales para promover la inclusión digital y mejorar las habilidades de la fuerza laboral actual.

University of South Wales Prifysgol De Cymru

Cyber Security Challenge UK

LT HARPER Cybersecurity Recruitment

NeuroCyber

Institute for Apprenticeships & Technical Education

Organismos con competencias en talento de ciberseguridad

UK

Organismos

National Cyber Security Centre · GCHQ · HM Government · Department for Digital, Culture, Media & Sport · Department for Education · ISACA · Teach Computing · TECHTALENT CHARTER · CISSE UK

Iniciativas, actores y actuaciones

INICIATIVAS

- CyberFirst Initiatives
- Education and Skills, Advise and Guidance By NCSC
- CyBOK
- National Centre for Computing Education (NCCE)
- CISSE UK CSIIF UK
- Chartered Institute of Information Security (CIISec)
- UK Cyber Security Council
- Tech Talent Charter (TTC)

ACTORES

ACTUACIONES

Sector público y empresa privada

Critical National Infrastructure (CNI) Apprenticeships
Deliverables of UK Cyber Security Council
CyberFirst Apprenticeships
NCSC Advise and Guidance
Government Security Profession (GSP)
Cyber Skills Immediate Impact Fund (CSIIF) for Training Providers
Open Playbook by TTC
Digital Skills Partnerships (DSP)

Escuelas y universidades

CyberFirst Schools / Colleges Scheme
Cyber Security for Schools Resources
NCSC – (ACE-CSE) and Certified Degrees
Cyber Security Education Workshop 2021 for Teachers
Teach Computing – for Teachers

Estudiantes

Cyber Discovery Programme
Bursary and Degree Apprenticeship
CyberFirst Trailblazers and Adventurers - (Also Teachers)
CyberFirst Defenders, Futures & Advanced
National Cyber Security Academy (NCSA)
T Levels Courses

Profesionales cyber

Development by (CIISec)
CSX® – Cybersecurity Nexus Training and Credentialing by ISACA
Deliverables of UK Cyber Security Council
European Cyber Security Challenge – UK
NCSC Resources for Cyber Security Professionals

Minorías

CyberFirst Girls Competition
Women in Cyber Security
Diversity and Inclusion (LT Harper)
Cyber Skills Immediate Impact Fund (CSIIF)
Cyber Neurodiversity

Variables de análisis para el benchmark

UK

VARIABLE	DETALLE
***Framework* talento en seguridad para el Gobierno de UK**	Se busca evidencia de que los diferentes *frameworks* reflejen coherencia al categorizar, organizar y describir el ecosistema de la fuerza laboral en ciberseguridad.
***Body of Knowledge* (CyBOK) de ciberseguridad**	Se busca evidencia de cómo esta herramienta robusta es realmente un recurso para para la promoción y desarrollo del talento.
Impacto en organizaciones (públicas y privadas)	Se analizan los programas y eventos para que las empresas sean más seguras online. Factores como la capacitación a empleados en múltiples áreas de la seguridad y el intercambio de información son clave.
Impacto en profesionales de ciberseguridad	Analiza el enfoque que tiene cada país al abordar el reclutamiento y retención del talento, así como la compensación promedio de los profesionales tanto en el ámbito público como privado.
Impacto en estudiantes	Se valoran los países que identifiquen y estimulen el talento de ciberseguridad en los diferentes ciclos de estudio.
Impacto en escuelas y universidades	Se tienen en cuenta programas y herramientas que reflejen el compromiso con la excelencia académica, la innovación y el empoderamiento de los profesores como la base para lograr competitividad en los estudiantes.
Inclusión (mujeres y minorías)	Identificar actuaciones tendientes a grupos poco representativos dentro del mundo de la ciberseguridad, otorgándoles capacitación, información sobre programas de grado relacionados con la ciberseguridad e información sobre becas.
Inversión	Identificar no solamente el esfuerzo presupuestal de cada iniciativa / actuación sino la forma en la que asignan eficiente y racionalmente esos recursos.

Framework de talento en seguridad para el Gobierno

UK

Este *framework* es el primero en su tipo, como **guía esencial para respaldar el desarrollo, construir experiencia y apoyar más carreras** a través del Gobierno. Es un indicativo de cómo la fuerza laboral en ciberseguridad es una **comunidad diversa de más de 11.500 profesionales** que desarrollan y aportan conocimientos para gestionar y reducir los riesgos.

Ayuda a los profesionales de la seguridad a identificar las necesidades de aprendizaje y proporciona un enfoque estructurado para la formación y el desarrollo.

Dentro de la gestión de este framework se contempla darle más formalidad a la profesión, esto incluye **aprendizaje vinculado a mentores de la industria y acreditación profesional**.

Ha sido clave para **atraer, desarrollar y retener profesionales** altamente cualificados en seguridad que necesita UK.

Brinda un sentido real de pertenencia al usar un **lenguaje común en todas las especialidades** técnicas para eliminar barreras, reducir el trabajo en silos e inspirar a las personas a verse a sí mismas como parte de una comunidad más amplia y diversa.

Representa el esfuerzo y colaboración de 300 expertos en más de 40 grupos de trabajo.

El framework busca transformar la forma en que el gobierno aborda la problemática de la seguridad nacional.

Nota: Publicado el 13 de Febrero de 2020, este *framework* no es específico para ciberseguridad, sino que abarca 4 especialidades (cibernética, física, técnica y de personal).

Framework de talento en seguridad para el Gobierno

UK

Para poder utilizar el *framework* como marco común de análisis se necesitan establecer unas **áreas** que nos ayuden a **evaluar el contenido de los diferentes *framework* en cada país**.
Se proponen estos 6:

ENFOQUE

Conceptos más importantes en los que se enfoca el *framework* y las expectativas que se tienen en diferentes horizontes de tiempo.

ESTRUCTURA

Mide la claridad y la lógica con la que está organizado el *framework*, lo que se traduce en facilidad en la implementación.

INCLUSIÓN

Valora los diferentes actores o grupos de distinta tipología que se benefician del *framework*.

FLEXIBILIDAD

Determina si el *framework* se adapta a las necesidades de la fuerza laboral de cada organización.

BENEFICIOS

Considera la ayuda que reciben cada uno de los diferentes actores que hacen parte del ecosistema del talento de ciberseguridad.

INVERSIÓN

Tiene en cuenta las recursos económicos asignados para apoyar el despliegue del *framework*.

Análisis benchmark

Framework talento en seguridad para el Gobierno

UK

Resultados del análisis

El *framework* ayuda a los profesionales en su **desarrollo profesional a partir de la definición de unos roles** y sus respectivas habilidades a desarrollar para garantizar un adecuado desempeño. Adicionalmente, busca **homogeneizar el lenguaje** de la seguridad para eliminar barreras y alcanzar una comunidad más amplia y diversa.

Aborda principalmente los siguientes componentes: ***Career Pathways, Skills & Development:***

- 46 roles críticos de seguridad, de los cuales **25 son de ciberseguridad**, incluidos en 9 familias de roles.
- **25 *skills*** cada una con 4 niveles.
- Ciclo de planificación para el **desarrollo personal**.
- Apoyo al **proceso de reclutamiento.**

4 especialidades: • seguridad física • personal de seguridad • ciberseguridad • seguridad técnica.

INVERSIÓN

No especifica.

BENEFICIOS

- Ayuda a que los profesionales tengan **una hoja de ruta más clara** en la profesión de seguridad dentro y fuera del gobierno.
- Ofrece la oportunidad de **desarrollar habilidades y construir experiencia**, en base a conceptos definidos y en consonancia con otros *frameworks*.
- Identifica brechas críticas.
- **Promueve atraer, reclutar y retener talento** para el gobierno especialmente.
- Proporciona **criterios para el reclutamiento** a las áreas de recursos humanos.

FLEXIBILIDAD

El *framework* permite **navegar entre los diferentes roles y habilidades con sus respectivos niveles** ,lo que lleva a una mayor comprensión el momento de buscar un buen *fit* entre los profesionales y las diferentes posiciones. De igual forma, **algunos testimonios reflejan que ha habido un ambiente seguro para el desarrollo** y la duración de las diferentes capacitaciones en algunos casos se lleva a ritmo propio.

INCLUSIÓN

Esta herramienta como su nombre lo indica pone el **foco en las trayectorias de los profesionales para el gobierno**, en consecuencia, el foco está puesto en todo el personal gubernamental que trabaja en un rol de seguridad, o para cualquier persona que desee saber más sobre lo que se requiere para los diferentes roles.
No enfatiza en estudiantes ni empresas del sector privado.

Análisis *benchmark*

Framework talento en seguridad para el Gobierno

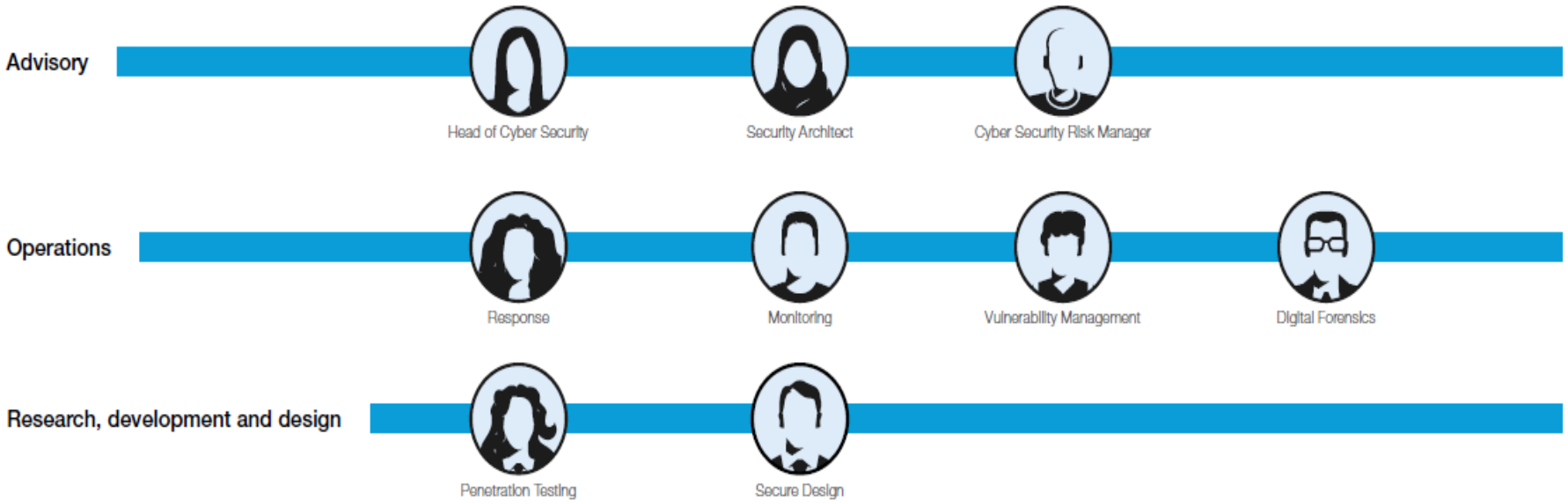
UK

El *framework* se puede utilizar como base para **abordar los planes de carrera** para los profesionales, así como **planificar cómo el personal puede acceder a las oportunidades** de aprendizaje y desarrollo, y las **descripciones de funciones** pueden usarse para formar la base de las **descripciones de los puestos** al momento de la contratación.

Government Security Profession

Este *framework* es ideal para generar coherencia entre las descripciones de los roles y los niveles de capacidad. Esto impulsa las trayectorias profesionales, guía el desarrollo y con el tiempo de lograrán las acreditaciones asociadas. Se considera una herramienta clave para las áreas de RR.HH., proporcionando los criterios a utilizar en todo el **proceso de *recruiting.***

- ***Career Pathways.*** Representación visual de las especialidades, las familias de roles y los **roles de ciberseguridad**.



- **9 familias de roles y 25 roles en ciberseguridad, y los roles a su vez tienen niveles jerárquicos: *Associate, Lead* y *Principal.***
- **Trayectorias profesionales por cada rol, con rutas indicativas de entrada y de salida hacia otros roles y especialidades.**
- Promueve el movimiento horizontal para los profesionales.
- *Grade To Role Mapping.* Este mapeo es un indicativo de los grados relacionados con los roles. Incluye grados del *Civil Service* y grados militares. Así se logra adherir a pautas de otras guías.
- Incluye ejemplos de perfiles reales de profesionales en el ámbito de la ciberseguridad y cómo se han movido horizontalmente.

Framework talento en seguridad para el Gobierno

UK

- ***Skills.*** **Hay 25 habilidades** en el *framework*, compartidas en los 46 roles. Cada habilidad tiene **4 niveles**: *Awareness, Working, Practitioner* y *Expert*.

Las habilidades o *skills* se refieren a la experiencia o aptitud en una capacidad que se necesita para hacer o llevar a cabo algo con éxito. Estas se utilizan para indicar el conocimiento y la experiencia típicos requeridos para cada uno de los roles del *framework*.

Cyber Security operations

Skill	Skill source	Skill type
Cyber Security operations	CIISEC Framework E2 skill	Cyber Security

Skill definition

Cyber Security operations are the secure configuration and maintenance of information, controls and communications equipment in accordance with relevant security policies, standards and guidelines. This includes the configuration of information security devices (e.g. firewalls) and protective monitoring tools (e.g. Security Information and Event Management (SIEM)). Principles include implementing security policy (e.g. patching policies) and security operating procedures in respect of system and/or network management, maintaining security records and documentation in accordance with security operating procedures, and monitoring processes for violations of relevant security policies (e.g. acceptable use, security).

Awareness ★	Recognises the need for information systems and services to be operated and monitored securely and can list some of the main policies and practices involved in achieving this Explains the main principles of secure configuration of role specific security components and devices, including firewalls and protective monitoring tools (e.g. SIEM)
Working ★★	Demonstrates experience applying the principles of secure configuration of role-specific security components and devices in a training or academic environment, for example through participation in syndicate exercises, undertaking practical exercises, and/or passing a test or examination Supports the overall aims of a Cyber Security operations-related team, e.g. a monitoring team Applies routine security procedures appropriate to the role, such as patching, managing access rights, malware, protection or vulnerability testing under direction/supervision Develops and tests rules for detecting violations of security operating procedures under supervision
Practitioner ★★★	Develops security operating procedures for use across multiple information systems or maintains compliance with them Applies routine security procedures appropriate to the role, such as patching, managing access rights, malware protection or vulnerability testing with autonomy Develops and tests rules for detecting violations of security operating procedures with autonomy Leads small teams managing Cyber Security operations within an organisation
Expert ★★★★	Leads teams managing Cyber Security operations within an organisation Identifies the need for, and implements, new security operating procedures and practices to meet changing requirements Is a subject matter expert in developing and operationalising techniques for Cyber Security operations, e.g. detecting anomalous activity, automating orchestration and configuration of IT

Las habilidades son para todo el personal gubernamental que trabaja en un rol de seguridad o cualquier persona que desee saber más sobre lo que se requiere para los diferentes roles. También son para algunos miembros del sector público en general que han adoptado el modelo.

Para nuevas revisiones del *framework* se espera contar con una herramienta de elaboración de perfiles de habilidades, accesible en línea en todo el Gobierno, que asigna la capacitación a los niveles de habilidad como una ayuda en la carrera del profesional.

Estas habilidades se deben alinear con la parte de desarrollo y usarse para alimentar las discusiones sobre el desempeño y los logros en la carrera. Esto permite acordar las áreas donde habrá que poner mayor foco.

Análisis *benchmark*

Framework talento en seguridad para el Gobierno

UK

- ***Learning and development.*** Cada *skill* tiene un repositorio de formación indicativo. Esta formación no está avalada por el Gobierno, por lo tanto, se desarrollará un **aprendizaje** completo para apoyar el *framework*.

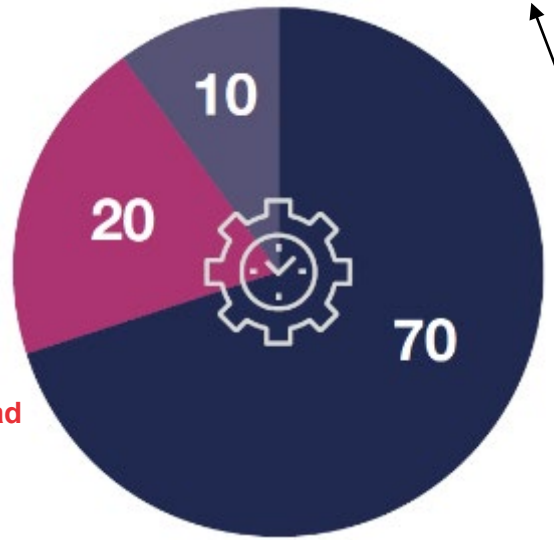
List of skills

Skill	Specialism	Source
Applied Personnel Security	Personnel Security	CPNI
Applied Physical Security	Physical Security	CPNI
Applied research	Cross-specialism	CIISEC Framework I2 skill
Applied security capability	Cyber Security	NCSC Information Risk Assurance skill 5.5
Applied Technical Security	Technical Security	CPNI
Business continuity management	Cross-specialism	Business Continuity Institute
Compliance monitoring and controls testing	Cyber Security	CIISEC Framework D2 skill
Cyber Security operations	Cyber Security	
Design	Cross-specialism	
Forensics	Cyber Security	
Incident management, incident investigation and response	Cyber Security	
Information risk assessment and risk management	Cyber Security	
Intrusion detection and analysis	Cyber Security	
Investigative interviewing	Personnel Security	
Legal and regulatory environment and compliance	Cross-specialism	
Penetration testing	Cyber Security	

Skills

Especialidad

Fuente



70% aprendiendo a través de la experiencia → o*n- the job*

A menudo se considera el más beneficioso, ya que permite poner en práctica conocimientos e integrar el aprendizaje. Se trata de asumir áreas de responsabilidad laboral que son nuevas y aprender a través de estas experiencias.

20% aprendiendo a través de otros → *near the job*

A veces se denomina "aprendizaje social". Se trata de cómo se comparten los conocimientos y experiencias con los demás y también cómo se aprende de esto. A esto se refieren como desarrollo profesional continuo (*Continuous Professional Development,* CPD).

10% aprendiendo a través de la educación estructurada → o*ff –the-job*

Cubre todas las formas de cursos formales y programas de aprendizaje. Estos pueden impartirse en modalidad *e-learning*, presencial en clases o certificaciones.

70/20/10 es un modelo de aprendizaje y desarrollo ampliamente utilizado. La formación se asigna por competencias, las cuales se pueden ver en el repositorio y determina las expectativas mínimas de competencia que se deben reflejar para acceder a la formación.

Análisis *benchmark*

Framework talento en seguridad para el Gobierno

UK

- ***Personal development.*** El desarrollo es un aspecto clave en este *framework* y la idea central es **estructurar periódicamente conversaciones** sobre el desempeño y los logros. Estas son fundamentalmente entre los profesionales y los mánagers, y busca discutir roles deseados y acordar niveles de *skills* hacia los que debería progresar el profesional en un determinado tiempo.

El **ciclo de planificación** para el desarrollo personal contempla **6 elementos clave:**

- **Entender fortalezas y gaps.**
- **Investigar oportunidades de carrera.**
- **Mantener conversaciones sobre la carrera.**
- **Crear un plan de acción.**
- **Ejecutar el plan de acción.**
- **Seguimiento.**

¿Qué cuestiones estratégicas involucran estas conversaciones?

- Questions to think about
- People who can help you
- When you need to think about this
- Tools that can support you
- Key points for line managers

Las actividades de desarrollo se pueden emprender para mejorar una habilidad o área en particular en el rol actual y a medida que avanza a través o hacia diferentes roles.

Análisis *benchmark*

CyBOK – *Cybersecurity Body of Knowledge*

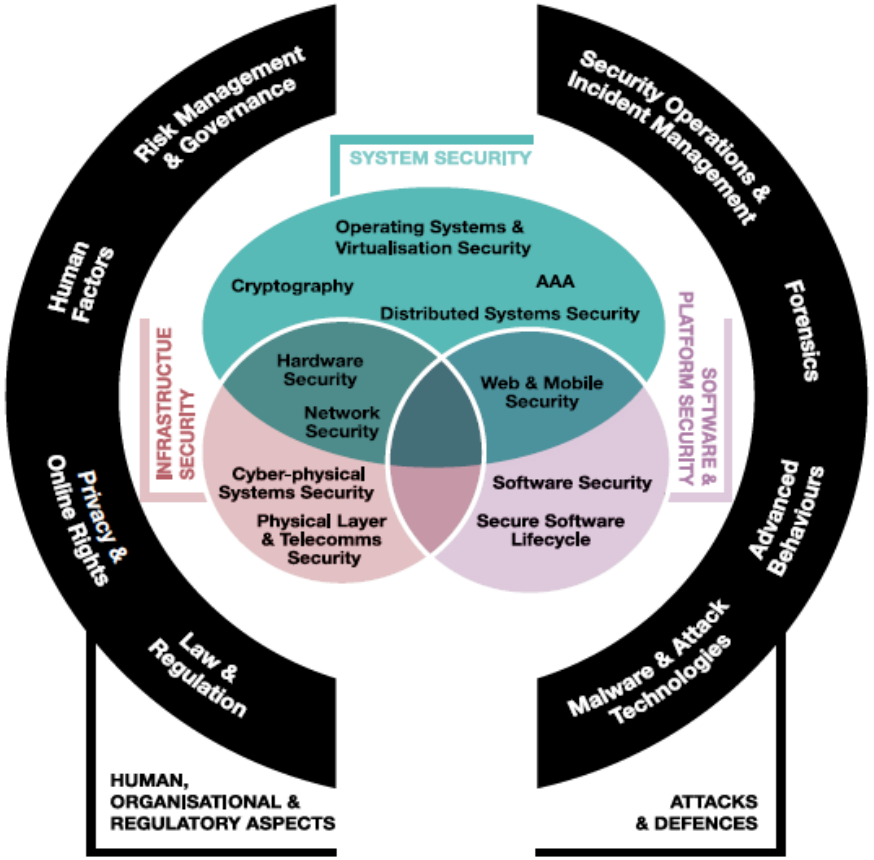
UK

El CyBOK es un recurso único, que proporciona por primera vez un "cuerpo de conocimiento" subyacente que **abarca la amplitud y profundidad de la ciberseguridad.**

El objetivo principal del proyecto es **codificar el conocimiento en ciberseguridad** que sustenta la profesión. Además, el proyecto permitirá el **desarrollo de trayectorias profesionales y planes de estudio** para la educación.

19 áreas de conocimiento

La versión 1.0 de *CyBOK* se publicó el 31 de octubre de 2019 y se lanzó formalmente en enero de 2020. La siguiente fase del proyecto (hasta marzo de 2021) se centrará en la difusión y aplicación de *CyBOK*.



El Centro Nacional de Ciberseguridad (NCSC) utilizará CyBOK como base para describir el contenido del curso de la actuación *NCSC – (ACE-CSE) and Certified Degrees.*

También se busca motivar a otros a usar *CyBOK* para ayudar en el diseño de materiales de cursos de ciberseguridad en educación, capacitación y profesionalización.

El *CyBOK* es un recurso que promueve la narrativa alrededor de la ciberseguridad y, por ende, es una base esencial como estándar de desarrollo del talento.

Análisis *benchmark*

CyBOK – *Cybersecurity Body of Knowledge* – *Human Factors*

UK

El *CyBOK* aborda múltiples áreas de conocimiento, pero hemos querido **profundizar en el aspecto humano** porque es donde la **concienciación, educación y capacitación en ciberseguridad** tienen un rol más determinante.

Las personas somos el eslabón más débil en seguridad. **Después de todo, los humanos están por naturaleza sujetos al error y a hacer cosas que no tenían intención de hacer.** Esta noción hace que la responsabilidad tienda a recaer en el usuario final, pero muchas veces el diseño de los sistemas es el que lleva a ciertas incidencias. Por esto, la necesidad de que existan **manera útiles de ofrecer seguridad** de una manera que la carga no sea en el usuario final.

"Instead of fitting the human to the task, fit the task to the human"

La seguridad debe ser útil:

Efectividad: ¿los usuarios pueden cumplir con sus objetivos?

Eficiencia: ¿qué recursos se gastan para hacerlo?

Satisfacción: ¿cuál es el nivel de conformidad y aceptación de los usuarios?

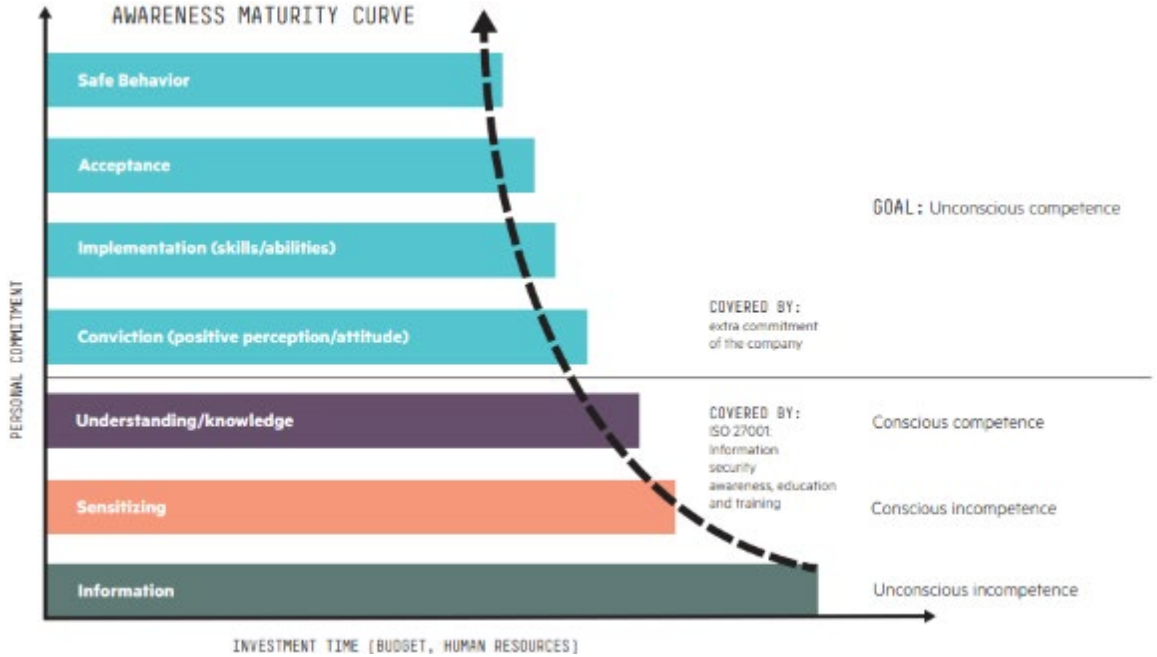
Balance entre productividad y seguridad:

¿Cuánto tiempo se tarda en completar una tarea de seguridad? ¿Cuántos pasos?

¿Las políticas de seguridad interrumpen la productividad del usuario?

¿Se percibe agotamiento frente al cumplimiento?

- **Los cursos teóricos (estándares ISO) no son suficientes para cambiar el comportamiento.**
- **Se debe invertir en habilidades y conocimiento de seguridad.**
- **La cultura organizacional es clave porque provee el entorno para la práctica.**



Security Awareness. El propósito es captar la atención, pero también que exista un **compromiso real con la seguridad** (*engagement*) para que los resultados en la práctica sean visibles.

Security Education. El propósito de **romper modelos mentales** que limitan la educación, como la base para desarrollar nuevas habilidades.

Security Training. Además de proveer habilidades, se debe **ofrecer un entorno donde puedan ponerlas en práctica** y "experimentar".

Alcanzar niveles de conciencia adecuados y un cambio en la cultura de ciberseguridad son la antesala del aprendizaje y del cambio del comportamiento humano.

Principales iniciativas que tienen impacto en los diferentes actores del ecosistema del talento en ciberseguridad

UK

Iniciativa 1. *CyberFirst Initiatives*

Desarrollando la próxima generación de profesionales cibernéticos de UK a través de becas, cursos y competiciones para jóvenes de 11 a 17 años. Cubre una amplia gama de actividades: un plan integral de becas para apoyar financieramente a los estudiantes universitarios y un plan de aprendizaje de grado, un concurso exclusivo para chicas y miles de plazas gratuitas en los cursos *CyberFirst* en universidades y colegios de UK.

Iniciativa 2. *Education and Skills by NCSC*

Asesoramiento, recursos y oportunidades para escuelas y estudiantes interesados en ciberseguridad.
Esta iniciativa refleja el compromiso para garantizar que el sector educativo (bajo reciente aumento en ataques *ransomware*) sea resiliente contra las amenazas, publicando recursos prácticos que mejoran la seguridad y respuesta a incidentes.
La información es relevante para cualquier organización, no solo cuerpos educativos.

Iniciativa 3. *CyBOK*

"Cuerpo de conocimiento" en ciberseguridad

El principal objetivo del proyecto es codificar el conocimiento en ciberseguridad que sustenta la profesión. Además, el proyecto permitirá el desarrollo de trayectorias profesionales y planes de estudio para la educación.

Iniciativa 4. *National Centre for Computing Education*

El Centro Nacional para la Educación en Computación es financiado por el Departamento de Educación de UK y su objetivo es apoyar a los educadores con la enseñanza en ciencias informáticas.
Gestionado por un consorcio entre STEM Learning, la fundación Raspberry Pi y el BCS, The Chartered Institute for IT.
Cuenta con una amplia gama de recursos que cubren elementos de los currículos en diferentes etapas de la educación.

Iniciativa 5. *CISSE UK*

CISSE UK es una colaboración entre el Gobierno, la industria de ciberseguridad y la comunidad académica para promover y establecer una educación sobresaliente en todo el Reino Unido.
El *core* de esta iniciativa, está en eventos para la comunidad.
Busca establecer una cultura de educación en ciberseguridad sobresaliente, innovadora y de vanguardia.

Iniciativa 6. *Chartered Institute of Information Security*

Institución que tiene el estatus Royal Charter y se dedica a elevar el nivel de profesionalismo en ciberseguridad. **CIISEC es un organismo independiente sin fines de lucro gestionado por sus miembros**, garantizando estándares para la capacitación, cualificación y prácticas operativas.
De esta institución se deriva un *framework* de *skills* en ciberseguridad.

Iniciativa 7. *UK Cyber Security Council*

La intención es ayudar a garantizar que aquellos que trabajan en ciberseguridad puedan tener habilidades y experiencias reconocidas fácilmente, de manera clara y consistente, así como ayudar a los empleadores y trabajadores a tener más confianza en la profesionalidad, capacidad e integridad.
El *Council* buscará desarrollar vínculos más fuertes con otras profesiones y disciplinas en todos los sectores clave para considerar las expectativas que deben integrarse en los respectivos códigos de conducta.

Iniciativa 8. *Cyber Security Challenge UK*

Fundada por una serie de organizaciones en los campos de contratación, tecnología y empresas sociales, **respaldada por la Estrategia Digital del Reino Unido desde 2017**. La TTC se administra como un colectivo de la industria, ya que reconoce que solo trabajando juntos y uniendo fuerzas se puede lograr un cambio significativo. El TTC es para organizaciones de todos los tamaños, desde *start-ups* hasta grandes multinacionales, que abarcan todos los sectores de la industria.

De cada una de estas se despliega una diversidad de programas o actuaciones puntuales que se detallan más adelante en el documento.

Análisis *benchmark* – Programas o actuaciones

Mejora del impacto en organizaciones (públicas y privadas)

UK

El trabajo digital del Servicio Nacional de Salud (NHS) es un ejemplo del desarrollo de capacidades de ciberseguridad. Esta iniciativa, además de crear mejores servicios sanitarios de manera ágil y efectiva, refleja una **estructura de TI segura** que permite marcar una **diferencia real en la vida de los ciudadanos**.

Cyber and Data Security → Los equipos diseñan, desarrollan y operan los servicios de TI que apoyan al personal médico y utilizan datos para mejorar la atención y experiencia de los pacientes.

Virtual Perimeter Security

Proyecto de seguridad perimetral que apoya a las organizaciones del NHS a protegerse, otorgando los siguientes beneficios:

- **Visibilidad**
- **Inteligencia**
- **Cumplimiento**
- **Planeación (*value for money*)**

Special Training for Senior Information Risk Owners (SIROs)

Curso gratis de capacitación en ciberseguridad para los SIRO. Certificado por el GCHQ que ayuda a mejorar el conocimiento sobre los riesgos en ciberseguridad. Además de esto, aporta:

- **Mejorar el cuidado de los pacientes y los resultados de la organización.**
- **Desarrollo de conocimiento y responsabilidades alrededor del riesgo.**
- **Ayuda a estos perfiles a desarrollar una transformación cultural para mejorar la postura de ciberseguridad, información sobre la aplicación de mejores prácticas y una planificación eficaz de ciberseguridad.**

Simulated phishing training

Esta táctica es una de las más comunes por el poco esfuerzo que requiere por parte de los cibercriminales, quienes generalmente se aprovechan de la falta de *awareness*:

- **Esta capacitación busca incrementar el *awareness* de todo el personal sanitario y de la seguridad social.**
- **Ofrece un panorama de cómo están actuando los empleados frente a estas amenazas, de manera que se pueda hacer un seguimiento e implantar cambios.**

On-site assessments

Evaluaciones presenciales gratuitas que aportan:

- **Identificación vulnerabilidades y comprensión de las áreas de alto riesgo.**
- **Plan de recomendaciones que ayuda a priorizar qué acciones se deben tomar para mejorar los niveles de ciberseguridad.**
- **Ayuda a que la organización alcance la acreditación *Cyber Essentials Plus*, que es obligatoria a partir de 2021.**

GCHQ: *Government Communications Headquarters*. *E*s uno de los tres servicios de inteligencia de UK.
Cyber Essentials: esquema respaldado por el Gobierno que ayuda a proteger las organizaciones. Certificación que se lleva a cabo con una verificación técnica práctica.

Análisis *benchmark* – Programas o actuaciones

Impacto en organizaciones (públicas y privadas)

UK

No.	Nombre de la actuación	Organismo	Descripción	Estado	Resultados
1	**Deliverables of *UK Cyber Security Council***	ISACA UK Cyber Security Council Iniciativa propia	Buscan defender la profesión de la ciberseguridad en todo UK, proporcionar una amplia representación para la industria, acelerar la conciencia y promover la excelencia en la profesión. Lo hará mediante la entrega de **liderazgo intelectual**, **herramientas profesionales y recursos educativos al sector** y a aquellos que buscan ingresar al sector. **Presupuesto: 1 - 2,5M£**	Activo	• Lista definida de **certificaciones** y un marco fácil de entender de cómo se vinculan todas y qué capacidades transmiten, basándose en las trayectorias profesionales que ya se han realizado. • Nuevo código de ética para los profesionales de ciberseguridad en todas las especialidades. • Desarrollar y administrar un estatus *Royal Chartered* para que los profesionales aspiren a desarrollar una hoja de ruta sólida. • Este *Council* depende en gran medida del Gobierno, pero tiene la intensión de irse haciendose cada vez más independiente.
2	***Cyber Skills Immediate Impact Fund* (CSIIF)**	Department of Digital, Culture, Media & Sport (DCMS) Iniciativa NA	Está diseñado para proporcionar financiación y apoyo a proveedores de formación y organizaciones benéficas para ejecutar iniciativas que aumenten rápidamente el número y la diversidad de quienes ingresan a la profesión. **La financiación alcanza las £100.000 máximo por iniciativa**.	Última actualización 2019	• El CSIIF se lanzó en febrero de 2018 e identificó siete iniciativas que recibirían apoyo para su puesta en marcha y expansión. • Ejemplos notables de proyectos incluyen un campo de entrenamiento de 10 semanas para mujeres y una iniciativa para la comunidad neurodiversa. *Community Cyber Security Centre Pllot.* • Cada vez han obtenido más apoyo de la industria y esperan que el proyecto sea autosostenible sin la ayuda del Gobierno.

Análisis *benchmark* – Programas o actuaciones

Impacto en organizaciones (públicas y privadas)

UK

No.	Nombre de la actuación	Organismo	Descripción	Estado	Resultados
3	***CyberFirst and Critical National Infrastructure (CNI)*** ***Apprenticeships***	GCHQ NCSC Partnership Allstate, Global Cyber Alliance, IBM, Microsoft, Lloyds y Tesco Iniciativa CyberFirst	Ofrece a las organizaciones la oportunidad de moldear y enseñar habilidades técnicas que tienen aplicación en el mundo real. £20.000 salario prom/año. Enfoque en prácticas de aprendizaje y trabajo (*online* y *onsite*).	Inscripciones para 2021 cerradas	• Mejor fit entre las empresas y los candidatos, debido a que los programas abordan directamente cuestiones de alta relevancia y prioridades reales. • Cientos de estudiantes han sido apoyados para algunos de los programas que duran entre 18 y 24 meses y que se imparten en diferentes niveles.
4	***Open Playbook***	Tech Talent Charter Iniciativa propia	Catálogo de código abierto de recursos y estudios de casos para ayudar a las empresas a aumentar la inclusión y la diversidad en sus equipos tecnológicos. Los capítulos incluyen: • Cultura inclusiva. • Contratando talento diverso. • ¿Qué funciona? Evidencia basada en acciones. • Programas de reentrenar.	Activo	• Con la ayuda de las estrategias prácticas de esta actuación, las empresas han podido impulsar notablemente la inclusión y diversidad en roles de tecnología.

Análisis *benchmark* – Programas o actuaciones

Impacto en organizaciones (públicas y privadas)

UK

No.	Nombre de la actuación	Organismo	Descripción	Estado	Resultados
5	***Digital Skills Partnership (DSP)***	UK Department for Digital, Culture, Media & Sport *Partnership* Empresas Iniciativa propia	**DSP** reúne a organizaciones del sector público y privado. El objetivo es ambicioso: mejorar la capacidad digital en todo el espectro de habilidades, desde las habilidades esenciales hasta las habilidades que se necesitan en una economía cada vez más digital, así como las habilidades avanzadas requeridas para roles especializados.	Activo	• A través del apoyo a *partnerships* locales, reúnen *partners* de diferentes sectores para diseñar, desarrollar y coordinar la entrega de programas innovadores que abordan *skills* digitales, exclusión digital, mejores prácticas y concienciación. • Fortalecer la empresa digital, ayudando a pequeñas empresas y organizaciones benéficas a mejorar las competencias de sus empleados para que puedan aprovechar los beneficios de productividad que implica la tecnología.
6	***NCSC Advice and Guidance***	GCHQ NCSC Iniciativa propia	Amplia lista de temas relacionados con la ciberseguridad, que incluye: • Gestión de activos. • Gestión de Identidades. • *Cloud*, inteligencia artificial. • *Cyber Essentials* (esquema de certificación respaldado por el Gobierno). En total son **46 temas diferentes**, cada uno con recursos útiles.	Activo	• Mejorar la seguridad de las empresas, incluidas SMB, de forma rápida, fácil y asequible o incluso gratis, para que se protejan de las formas de ataque más conocidas. • Desarrollar un conjunto de herramientas para ayudar a las organizaciones a comprender mejor sus riesgos y prepararse para gestionar las amenazas. • Entrega de guías diseñadas para optimizar la protección, como *10 steps to cybersecurity,* que describe otras medidas clave para las pymes de tecnología y organizaciones públicas y privadas más robustas.

Impacto en organizaciones (públicas y privadas)

UK

Key Takeaways

El *Cyber Security Council* considera que el liderazgo intelectual es el camino a la excelencia de la profesión. Para ello, los recursos educativos como las certificaciones que vinculen capacidades son clave en el desarrollo de las hojas de ruta de los profesionales.

La formación o *apprenticeship,* que se ejecuta en colaboración público-privada da, la oportunidad de moldear la enseñanza para que haya un mejor ajuste entre oferta y demanda de talento. Un ejemplo de esto es el esfuerzo de CyberFirst y Critical National Infrastructure *(CNI)* con el sector privado.

Ayudarle a las pymes a entender los riesgos a los que están expuestas es una prioridad. Prueba de ello son las guías que pone a disposición el NCSC, donde abordan más de 40 temas, con el objetivo de proteger este tejido productivo.

El Cyber Skills Immediate Impact Fund *(CSIIF)* es un organismo esencial para la financiación de iniciativas de formación con presupuestos de hasta £100.000 por iniciativa. El apoyo a los proveedores de formación es clave.

UK otorga un espacio para que la comunidad participe activamente en la revisión de estas actuaciones, abriendo un espacio para entender qué más pueden hacer desde el Gobierno y la industria de manera conjunta e identificar oportunidades que maximicen el valor.

Gap de la Fuerza laboral en ciberseguridad

UK

Para analizar el *gap* de la fuerza laboral en UK se ha consultado el estudio del (ISC)2 denominado *Cybersecurity Workforce Study 2020*.

- UK plantea que, dada la escasez de definiciones en la industria y la velocidad de la evolución en ciberseguridad, **definir con precisión el tamaño del gap es un gran desafío**, más aún si se consideran las variables multidisciplinarias en las especialidades (roles) de la ciberseguridad por sector.

En consecuencia, han tratado de comprender mejor la naturaleza y los matices de la oferta y la demanda para darse una imagen más completa de dónde se percibe el gap.

- La problemática del *gap* va más allá de una escasez de profesionales; hay una brecha importante también en las capacidades de ciberseguridad.

La capacidad se trata del nivel y la combinación de experiencia y habilidades necesarias.

Sector	No. de Organizaciones	Gap en Habilidades Técnicas Básicas		Gap en Habilidades Técnicas de Alto Nivel		Subcontratación de Capacidades en Cyber
Público	12,400	18%	2,200	27%	3,300	65%
Privado	1.32 Millones	54%	710,000	31%	407,000	30%

Fuente: (ISC)2 *Cybersecurity Workforce Study*, 2020; *Initial National Cyber Security Skills Strategy*, 2018.

Análisis *benchmark* – Programas o actuaciones

Impacto en profesionales de ciberseguridad

UK

Uno de los **elementos desfavorables** para los profesionales en ciberseguridad en UK es que **el rol se gestiona con mayor frecuencia de forma informal en las organizaciones:** la gran mayoría de las personas que tienen alguna responsabilidad en ciberseguridad dentro de su organización no tienen calificaciones formales y tampoco están trabajando para lograrlas. Esto ha llevado a una **narrativa fragmentada sobre las habilidades de ciberseguridad y una falta de coherencia entre las diferentes especialidades**, lo que a su vez hace que el camino hacia las carreras profesionales sea difícil de navegar, motivando las siguientes actuaciones.

No.	Nombre de la actuación	Organismo	Descripción	Estado	Resultados
1	***Development by CIISec***	CIISec Iniciativa NA	Busca promover el desarrollo profesional a traves de: • *Certificaciones.* • *Apprenticeships.* • *Training.* • *Associate Development Programme.* • *Marterclass Programme.*	Activo	• **Otorgar la certificación avalada por el NCSC, denominada *Certified Cyber Professional (CCP)* . Mayor nivel de profesionalismo.** • *Networking* entre líderes de la industria. • Conectar miembros con organizaciones. • Que los profesionales accedan a cursos que cumplan con los estándares de la industria (ISO, GDPR, etc.).
2	***CSX® Cybersecurity Nexus Training and Credentialing***	ISACA Iniciativa NA	Programas de certificación basados en el desempeño: • *Cybersecurity Nexus Courses* : +15 cursos • *Cyber Nexus Hands-On Labs:* +70 laboratorios prácticos • *Credentials* : *Cybersecurity Fundamentals* *Cybersecurity Audit* *CSX Technical Foundations* *Cybersecurity Practitioner* *Career Pathways*	Activo Algunos cursos no están disponibles	• Desarrollo de habilidades prácticas construidas a partir de experiencias *online* , *on-demand* y eventos en vivo que simulan amenazas del mundo real. • Fortalecer la preparación ante un ataque a través de laboratorios que implican aprendizaje y autoevaluación. • Credenciales como prueba de las competencias que catapultan el desarrollo profesional. • **La capacitación ofrecida está alineada con los roles del *framework* NICE.**

Análisis *benchmark* – Programas o actuaciones

Impacto en profesionales de ciberseguridad

UK

No.	Nombre de la actuación	Organismo	Descripción	Estado	Resultados
3	***European Cyber Security Competition (ECSC) UK***	European Union Cyber Security Challenge UK Iniciativa Cyber Security Challenge UK	El *European Cyber Security Challenge* es una iniciativa de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) y tiene como objetivo mejorar el talento en ciberseguridad en toda Europa y conectar a los grandes potenciales con organizaciones líderes en la industria. Cada país tiene una edición.	Activo Ediciones por año	• Posicionar la ciberseguridad como una disciplina al servicio de la humanidad, que promueve una sociedad impulsada por los valores, la libertad de pensamiento, la dignidad y el pensamiento crítico. • Promueve la colaboración entre países participantes, miembros de la industria y concursantes. • Promueve el desarrollo de futuros expertos en la industria. • Ha logrado que jóvenes talentos hagan uso de la base de datos de ENISA (European Agency for Cyber Security) y tomen decisiones informadas sobre la variedad de posibilidades ofrecidas por la educación superior en EU en ciberseguridad.
4	***NCSC Resources for Cyber Security Professionals***	GCHQ NCSC Iniciativa propia	• Múltiples guías para navegar, así como reportes y consejos. • Certificaciones. • Ejercicios de simulación a manera de prueba para medir resiliencia y capacidad de respuesta. ***Excercise in a Box.*** • Comunidad *online* para compartir inteligencia sobre ciberamenazas. • Apoyo para trabajar en alguno de los 13 sectores de infraestructura crítica (CNI).	Activo	• Información centralizada en el NCSC ayuda a los profesionales a conocer los estándares y enfoques bajo los cuales se trabaja en las instituciones de UK. • Las certificaciones promueven la capacitación de alto nivel en un amplio y complejo rango de temas dentro del *CyBoK*. • Incremento en dos vertientes: a*wareness & application.* • Poner a disposición reportes de vulnerabilidades permite entender no solo cómo funcionan, sino cómo prevenirlos. • Los ejercicios de simulación ofrecen informe personalizado, que ayuda a identificar próximos pasos y otros insights relevantes para cada caso.

Análisis *benchmark* – Programas o actuaciones

Impacto en profesionales de ciberseguridad

UK

GSP

***Government Security Profession* (GSP)** es un programa gubernamental que **reúne a los profesionales de seguridad** que trabajan en el Gobierno para ayudarlos a **adquirir habilidades y conocimientos**.

En UK se tiene la **visión** de crear una profesión de seguridad gubernamental dinámica líder en el mundo, que involucre, apoye e inspire a los profesionales existentes y continúe construyendo una comunidad alrededor de la ciberseguridad, diversa, motivada y próspera.

Objetivos

El objetivo principal es la incorporación de profesionales en ciberseguridad de nivel básico al Gobierno central y **abordar la brecha de profesionales en altos niveles ejecutivos** (*High Executive Officer, HEO*) y la oficina ejecutiva senior (*Senior Executive Officer, SEO*), que con frecuencia **se van al sector privado después de haberse capacitado**.

Otros objetivos que persigue son: (i) atraer y reclutar el mejor talento al GSP; (ii) retener una fuerza laboral receptiva, altamente capacitada y motivada; (iii) desarrollar una oferta de **aprendizaje clara con acreditación** externa e intercambio con la industria; (iv) apoyar y alinear trayectorias profesionales claras en la profesión y el Gobierno en general, y (v) garantizar futuras **canalizaciones de talento**, incluidos los programas de grado y posgrado en ciberseguridad.

Oportunidades de carrera profesional

- El GSP ofrece la oportunidad de trazar una carrera en seguridad gubernamental, trabajando no solamente en el Gobierno, para desarrollar habilidades y experiencia.
- Reúne a todos los profesionales de la seguridad que trabajan en el Gobierno para ayudarlos a adquirir las habilidades y los conocimientos que necesitan para desempeñar sus funciones y crear un lugar de trabajo atractivo.

Framework GSP

- Este *framework* apoya el desarrollo de los profesionales en los diferentes roles relacionados con la seguridad de UK, entre ellos, la ciberseguridad.
- **Explica los caminos hacia la profesión y cómo ampliar el conjunto de habilidades en los diferentes roles a desempeñar.**

Impacto en profesionales de ciberseguridad

UK

Key Takeaways

Uno de los programas de mayor impacto en los profesionales de la Administración Pública es el *Government Security Profession (GSP)*. Reúne a los profesionales para ayudarlos a adquirir habilidades y conocimientos, construyendo una comunidad amplia y diversa, que a su vez abordar la problemática de la brecha de profesionales. Este organismo es el encargado de gestionar el *The Government Security Profession Career Framework.*

La certificación *NCSC Certified Professional (CCP)* se ha revisado en junio de 2021 y el organismo que se encarga es el Chartered Institute of Information Security *(CIISec).* Los profesionales son evaluados de una manera rigurosa en diferentes especialidades de la ciberseguridad, teniendo que evidenciar habilidades técnicas y reflejar que han resuelto necesidades reales de empresas de manera ética y profesional dejando claro sus deberes y actividades, así como evidenciar que sabe comunicar de manera efectiva la temática de la gestión de riesgos.

Los recursos que pone el NCSC a disposición de los profesionales es el mecanismo mediante el cual abordan las certificaciones, capacitaciones a alto nivel en concordancia con el *CyBOK*, así como temas de concienciación y conocimiento de estándares y preparación ante incidentes a través de ejercicios de simulación. La cantidad de recursos y aplicación de los mismos es bastante amplia en este sentido.

Análisis *benchmark* – Programas o actuaciones

Impacto en estudiantes

UK

En el espacio de *Further Education* (*FE*), entendido como cualquier estudio posterior a la educación secundaria que no sea parte de la educación superior (universitaria), había más de 47.000 estudiantes en campos relacionados con las TIC y 670 en ciberseguridad. Para (2017/2018) se estima que había 230 estudiantes en el nivel 4 para ser tecnólogos en ciberseguridad.

Una de las problemáticas que presenta la industria es reclutar estudiantes con habilidades en STEM, teniendo que competir así con otras disciplinas que buscan jóvenes con este tipo de destreza, para profundizar en su educación.

Estudiantes	2016 - 2017		
Nivel educación	**Relacionados con TIC**	**En ciberseguridad**	
Further education (FE)	+ 47.000	1.42%	670

No.	Nombre de la Actuación	Organismo	Descripción	Estado	Resultados
1	***Cyber Discovery Programme*** Extracurricular	GCHQ NCSC Delivered by SANS Institute Iniciativa CyberFirst	Programa diseñado para introducir a jóvenes **talentos entre 13-18 años a la ciberseguridad**. **Enfoque por fases, online y gratis.** La finalidad es aumentar el talento disponible para detener actividades criminales que ponen en riesgo la vida y las instituciones de UK. **Presupuesto: £20M.**	Inscripciones cerradas actualmente	Lanzado en 2017, ha logrado una comunidad de 70.000 personas. • En primera fase participaron 23.000, 12.500 pasaron a fases más avanzadas, más de 800 alcanzaron el nivel "Élite" y 170 fueron invitados al b*ootcamp* en el verano. • 60% de los estudiantes que participaron, considerarían ahora una carrera en ciberseguridad. • 75% de los estudiantes que participaron en el año 1 consideran que volverían para el año 2. • Formar a los estudiantes de la mano de profesionales altamente calificados. • Aumentar las capacidades del NCSC con el mejor talento disponible.
2	***Bursary and Degree Apprenticeship***	GCHQ NCSC Partnership Allstate, Global Cyber Alliance, IBM, Microsoft, Lloyds y Tesco Iniciativa CyberFirst	**Becas universitarias** con programas de hasta dos años. £4.000 por año universitario. Flexibilidad como eje central. **Aprendizaje** involucra un trabajo con remuneración al mismo tiempo que se obtiene un grado gratis. £20.000 salario prom/año. Enfoque en prácticas de aprendizaje y trabajo (*online* y *onsite*).	Inscripciones para 2021 cerradas	• Aporte significativo en los planes de carrera de los estudiantes, logrando posicionarlos posteriormente al grado en roles dentro de entidades del Gobierno. • Ha logrado financiar más de 500 becas en 2018, con el objetivo de llegar a 1.000 para 2021. • Fomentar experiencia en ciberseguridad y relaciones entre los estudiantes con entidades del Gobierno y la industria en general, a través de programas de verano en la Academia CyberFirst. • Formacion de profesionales evitando los créditos estudiantiles.

Análisis *benchmark* – Programas o actuaciones

Impacto en estudiantes

UK

La educación continua (*FE*) y la educación superior (*HE*) ofrecen oportunidades para aplicar de manera práctica los componentes básicos que se traen de niveles más elementales para desarrollar habilidades que serán aplicables en un entorno laboral. Por esto, es crucial que las bases de formación en los ciclos más elementales o básicos sean realmente sólidas. La gestión del talento abordada de una manera coherente permite convertir el talento en trabajos reales de ciberseguridad.

No.	Nombre de la actuación	Organismo	Descripción	Estado	Resultados
3	***CyberFirst Trailblazers and Adventurers* (cursos gratis) 12-14 años**	GCHQ NCSC Iniciativa CyberFirst	***Trailblazers*** es un curso de medio día para iniciar a cada estudiante en el camino a considerar qué GCSE tomar y cómo las ciencias de la computación juegan un rol fundamental. ***Adverturers*** resalta la variedad de roles de trabajo que existen y que involucran la tecnología.	Activo	Los estudiantes aprenden, entre otras cosas: • Personalización de *websites* y cómo contribuir de manera *online*. • Habilidades en análisis forense digital y las bondades de la inteligencia basada en *open-source* u *open-data*. • Sinergias entre la creatividad y la tecnología y cómo se aplican estos elementos en las organizaciones, específicamente en marketing. • Apoyo a la escogencia de GCSE, dando visibilidad al potencial y beneficios de estudiar las ciencias de la computación. • Mejorar la interpretación y el uso del *big data*, *3D printing* y criptografía.
4	***CyberFirst Defenders, Futures and Advanced* (cursos gratis) 14-17 años**	GCHQ NCSC Iniciativa CyberFirst	Introduce cómo construir y proteger pequeñas redes y dispositivos personales. El proposito que que los estudiantes se familiaricen y tengan una visión clara al considerar una carrera profesional en ciberseguridad. Para niveles avanzados se enfoca en implementacion de conocimiento.	Activo	• Ayudar a aumentar el nivel de conciencia acerca de la ciberseguridad. • Poner en práctica diferentes ramas de la ciberseguridad, como el impacto de amenazas y la huella digital, o algunas más avanzadas, como riesgos de aplicaciones y *software* y cómo prevenirlos. • Estudiar el comportamieno de los cibercriminales. • Desarrollo de habilidades avanzadas en jóvenes, como lo es *digital forensics*, *encryption technologies*, *source intelligence techniques* y *penetration testing*.

GCSE: Certificado General de Educación Secundaria.

Análisis *benchmark* – Programas o actuaciones

Impacto en estudiantes

UK

No.	Nombre de la actuación	Organismo	Descripción	Estado	Resultados
5	***National Cyber Security Academy* (NCSA)**	Welsh and UK Government University of South Wales Iniciativa Con *partners* de la industria	***Partnership*** entre la universidad y la industria para formar personal con habilidades que le haga frente a los desafìos del siglo XXI. En esencia el enfoque es empleabilidad a través del desarrollo de talento.	Activo	• Reducir el gap del talento en ciberseguridad, tanto en UK como en Gales. • Ha lanzado un piloto de £500.000 entre Gobierno, academia y grandes compañías como Airbus y Alert Logic. • Es un gran impulso para la región (Newport, Wales) en términos de desarrollo del conocimiento. • Vincular a la industria en el circuito de capacitación, ha incrementado la efectividad del programa y la empleabilidad.
6	***T Level Courses***	UK Department for Education Institute for Apprenticeships and Technical Education Iniciativa propia	**Cursos** que le siguen a los GCSE (calificación en UK equivalente a bachillerato). Estos cursos de 2 años se desarrollan en **colaboración con empleadores** para que el contenido satisfaga las necesidades de la industria y prepare a los estudiantes para el trabajo. **Respaldo de £500 millones al año.**	Activo	Lanzados en septiembre de 2020 los primeros 3 *T level* . Se espera: • Ofrecer a los estudiantes experiencias "*on-the-job*". • Esto respalda el objetivo de la estrategia de garantizar una fuerza laboral competente en todos los sectores, ya que incluye formación en diverdas áreas (finanzas, agricultura, legal, etc.). • Para septiembre de 2021 se espera implantar otros 7 cursos *T Level* . • En el lapso de dos años se espera impartir 1.800 horas de estos cursos, lo cual es un incremento notable en cuanto a cursos de educación técnica.

Impacto en estudiantes

UK

Key Takeaways

El programa *Cyber Discovery Programme* de la iniciativa *CyberFirst* es un claro ejemplo de la apuesta en UK por introducir jóvenes talentos a la industria. Lanzado en 2017, con un presupuesto de £20M y llevado a cabo por fases en las que participan más de 23.000 candidatos, ha logrado no solo identificar talento, sino generar vocación entre una comunidad que llega hasta los 70.000 integrantes.

UK es consciente de que la formación en STEM es un habilitador clave para los roles en ciberseguridad, especialmente para puestos júnior. Sin embargo, los reclutadores han destacado que tienen dificultad en encontrar esos perfiles y a menudo luchan por conseguir un buen *fit* entre el candidato y las necesidades de las empresas.

En general, las iniciativas de *CyberFirst* con impacto en edades tempranas buscan implantar habilidades críticas y dar visibilidad al potencial y beneficios de emprender una carrera profesional en las ciencias de la computación. Esto nuevamente es un esfuerzo por lograr en los estudiantes una visión clara, al mismo tiempo que se construye cantera.

Algunas de las actuaciones respaldan el objetivo 3 de la estrategia de garantizar una fuerza laboral competente en todos los sectores de la economía. Por ejemplo, los cursos *T-Level* se desarrollan en colaboración con empleadores, ofreciendo experiencias *on-the-job* que preparan a los estudiantes para el trabajo, de manera que satisfagan al mismo tiempo las necesidades de la industria.

Análisis *benchmark* – Programas o actuaciones

Impacto en escuelas y universidades

UK

La educación formal proporciona los componentes básicos que equiparán a los jóvenes para seguir carreras en ciberseguridad. En este sentido, el acceso a una enseñanza en informática de alta calidad sentará las bases que se pueden desarrollar y aplicar de manera práctica en la educación superior, lo que permitirá finalmente asumir roles más técnicos que tienen una alta demanda. Sin embargo, la educación formal no es el único vehículo para capturar y aprovechar el talento de los jóvenes, las actividades extracurriculares son una forma clave de identificar talentos y alimentar y desarrollar intereses a una edad temprana, lo que ayuda a desarrollar habilidades y a marcar trayectorias profesionales futuras.

No.	Nombre de la actuación	Organismo	Descripción	Estado	Resultados
1	***CyberFirst Schools / Colleges Scheme***	GCHQ NCSC Partnership Schools in Northern Ireland and Wales Iniciativa CyberFirst	**Programa piloto que desarrolla un *hub* de escuelas en ciberseguridad (CSH).** Lo componen escuelas comprometidas con brindar un enfoque estructurado para la excelencia en la educación en ciberseguridad. Hay diferentes tipos de reconocimiento: *gold*, *silver* y *bronze* **(certificaciones).**	Activo	• Promover la colaboración entre el NCSC, escuelas locales, empresas y organizaciones que comparten el objetivo de animar a jovenes a involucrarse en la informática y la aplicacion de la ciberseguridad en la vida cotidiana. • La colaboración mencionada otorga oportunidades para las escuelas en terminos de compartir recursos y experiencia con las compañías y universidades. • Inicialmente el alcance era en Gloucestershire y ahora ha trascendido a Gales. • Un mayor número de escuelas reconocidas y promovidas por el NCSC por su excelencia en la temática de la ciberseguridad.
2	***Cyber Security for Schools Resources***	GCHQ NCSC Partnership NEN Education Network Iniciativa Education and Skills by NCSC	**Se ha creado una web dedicada a recursos que ayudan a:** • Gobernanza de consejo y líderes sénior. • Personal. • Equipos de TI/Compras/Proveedores. • Otros recursos útiles**.**	Activo	• Mantener en alerta a las instituciones con alta depedencia de las TIC. • Ayudar a entender los riesgos asociados a la ciberseguridad, sensibilizando y mejorando la preparación en caso de incidentes. • *Tips* prácticos para el personal acerca de la ciberseguridad (30.000 *sets* enviados a escuelas). • Entrega de guías diseñadas para optimizar la protección, como *10 steps to cybersecurity* o *Common Cyber Attacks Infographic*.

Análisis *benchmark* – Programas o actuaciones

Impacto en escuelas y universidades

UK

No.	Nombre de la actuación	Organismo	Descripción	Estado	Resultados
3	***NCSC - Academic Centres of Excelence in Cyber Security Education and Certified Degrees***	GCHQ NCSC Iniciativa Education and Skills by NCSC Higher Education	**ACE-CSE** aborda requisitos de conocimiento, habilidades y capacidades para la inverstigación y educación. Con un alto número de universidades y programas en ciberseguridad, se dificulta que los estudiantes y empleadores evalúen la calidad y el grado en el que el programa se ajusta a su carrera profesional. **Programas certificados**.	Activo con: 23 *másteres* 3 *másteres* Integrados 3 *bachelors*	• El *assessment* por parte del NCSC incluye 11 tipos diferentes de grados, donde se incluye *Master, Bachelor* e *Integrated Master* . • Las universidades pueden atraer estudiantes de alto nivel de todas partes del mundo. • Empleadores pueden reclutar miembros calificados y desarrollar habilidades en ciberseguridad en los empleados existentes. • Estudiantes que ingresan a la industria pueden tomar decisiones mejor informadas al buscar una calificación altamente evaluada. • Animar a más universidades a la enseñanza en ciberseguridad. • Desarrollar una comunidad influente de educadores que dé forma y apoyo a la educación en ciberseguridad, en interacción con el ecosistema: empresas, Gobierno, estudiantes y educadores.
4	***Cyber Security Education Workshop 2021 - Call for Abstracts*** Yet to come	CISSE Partnership Open University's School of Computing Iniciativa propia de CISSE	**Se enfoca escencialmente en educadores, pero es de inter'es igualmente en otros grupos de la industria.** El objetivo de este taller es explorar los desafíos y oportunidades actuales, se hará hincapié en la educación superior a través del aprendizaje a distancia o remoto.	Activo	Los resultados que se podrían esperar de este evento son: • Innovación en el desarrollo e implementación de planes de estudio. • Conectar la ciberseguridad con la empleabilidad. • Certificaciones y acreditaciones de la industria. • Motivar y apoyar la diversidad en el aprendizaje y la participacion de minorías. • Como superar los desafios y mantener alta la motivación en el esenario del COVID-19.

Análisis *benchmark* – Programas o actuaciones

Impacto en escuelas y universidades

UK

No.	Nombre de la actuación	Organismo	Descripción	Estado	Resultados
5	**Teach computing**	National Centre for Computing Education and Department of Education UK Iniciativa propia de NCCE	**Provee apoyo esencial a profesores** de informática de primaria y secundaria. Se entregan certificaciones reconocidas como prueba del compromiso de desarrollar una práctica alrededor de la informática. Ofrece cursos de desarrollo profesional. **Respaldado con £84M.**	Activo	• Procurar un mejor encjae entre la enseñanza en fases tempranas y el mundo laboral de las profesiones informáticas. • Educación informática de alta calidad que se basa en construir unas sólidas bases en diferentes etapas. • *Continuing Professional Develoment (CPD) Program.* De 40 horas para profesores de secundaria. Se espera llegar a 8.000 profesores. • Creación de los *Network Computing Hubs* , hay 40 en UK, liderados por escuelas con excelencia en la enseñanza de la informática. Es en esencia una red de apoyo valiosa para el ecosistema.

- El Departamento de Educación está realizando una inversión significativa para continuar mejorando la experiencia de todos los profesores a fin de garantizar que todos los alumnos tengan las habilidades digitales que necesitan para el futuro y que los **profesores, estén capacitados para ofrecer excelencia**.

- Respaldado con una financiación de £84M anunciada en noviembre de 2017, el Departamento de Educación ha lanzado el programa integral para mejorar la enseñanza de la informática e impulsar la participación en ciencias de la computación, particularmente entre las niñas.

Impacto en escuelas y universidades

UK

Key Takeaways

UK reconoce que para capturar con éxito el talento futuro debe asegurarse de que los futuros profesionales estén informados sobre los diferentes tipos de roles y las trayectorias que deben seguir para llegar allí, desde abordar determinadas materias en la escuela y en la educación superior, hasta ir adquiriendo experiencia relevante fuera del aula.

UK ha puesto en marcha esquemas para crear *hubs* de escuelas en ciberseguridad con las administraciones descentralizadas, como Gales o Irlanda del Norte. Esto proporciona un enfoque estructurado para la excelencia desde las diferentes, escuelas además de promover la colaboración entre las administraciones en busca de oportunidades.

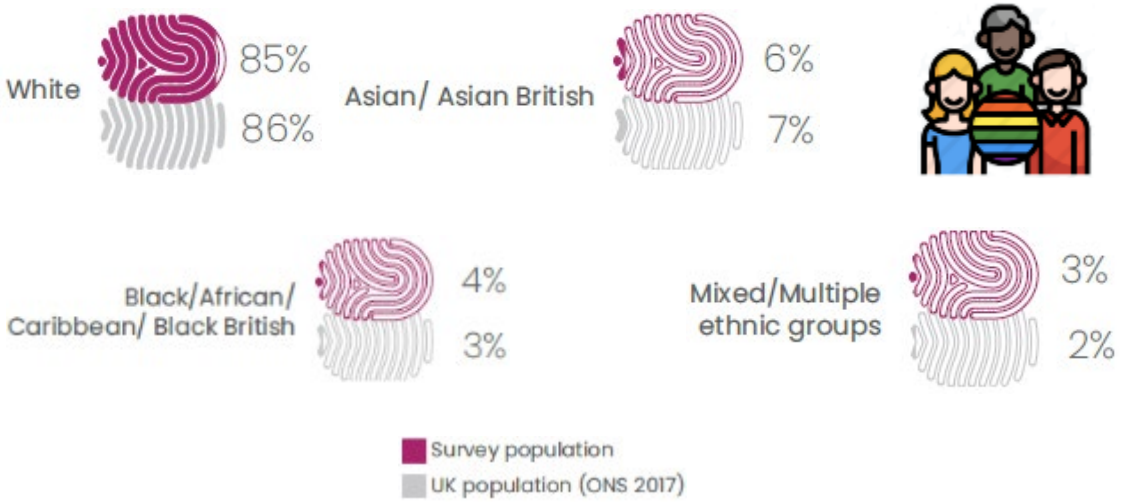
Hay actuaciones en etapa de planificación por materializarse en el corto plazo. Por ejemplo, el *Cyber Security Education Workshop 2021 - Call for Abstracts* es una actuación de extrema relevancia enfocada a los profesores. Se espera que esto sea una oportunidad única para innovar en el desarrollo e implementación de planes de estudio de ciberseguridad.

Diversidad en ciberseguridad

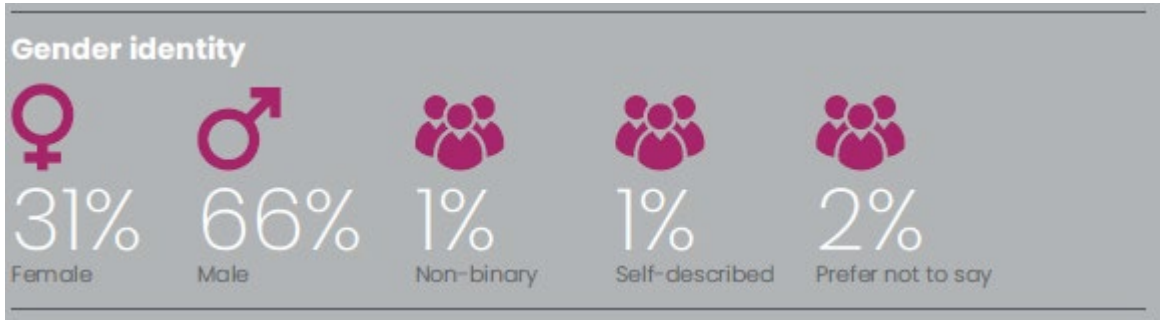
UK

El estudio que hemos tomado como base para tener un contexto de la diversidad e inclusión en ciberseguridad en UK es llevado a cabo por KPMG UK, apoyado por el NCSC, donde participan profesionales de la seguridad (+1200) e incluye compañías de diferentes sectores y tamaños (2020).

Este informe es el primero en su clase, por lo cual no es posible ver tendencias, pero sí establece una línea de base para la diversidad en términos de identidad de género, orientación sexual, etnia y antecedentes socioeconómicos, y examina la experiencia de inclusión y discriminación de los profesionales.

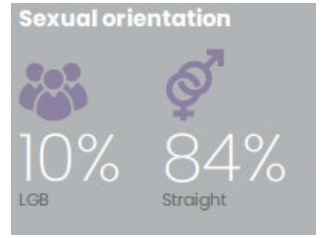


La representación femenina en la industria es del **31%**. Eso es más alto que lo indicado por estudios similares de la industria que sitúan la participación femenina en el **15%** (DCMS).



La baja diversidad y representación étnica es innegable. Es vital que la industria despliegue iniciativas de D&I que promuevan el desarrollo profesional de las minorías y que estos grupos no perciban que su progreso es limitado porque no se ajuste con la cultura de las organizaciones.

La comunidad LGTBI parece estar mejor representada en la industria que el promedio en UK, con un **10%** de los encuestados que se identifican en este grupo en comparación con el **2,2%** de la población.



Ahora bien, si la diversidad es acerca de números, la inclusión se trata de sentimientos. Sin inclusión, la industria de la ciberseguridad no se beneficiará al mejorar los niveles de diversidad.

Fuente: *KPMG & National Cyber Security Centre; Tech Talent Charter.*

Inclusión en ciberseguridad

UK

El **41%** de los profesionales negros sienten que han experimentado discriminación por su origen étnico durante el año pasado, más de seis veces el nivel de nuestra muestra de la encuesta en su conjunto.

A falta de soluciones más concretas a falencias de discriminación, no es de extrañar que **poco más del 9% de todos los encuestados estén considerando cambiar de empleador o dejar la industria por completo**.

En general, el 72% de los encuestados dicen que pueden ser ellos mismos en el lugar de trabajo. Eso es alentador, pero enmascara el hecho de que no todos se sienten tan bienvenidos. **De hecho, uno de cada cinco profesionales de la seguridad cibernética (21%) siente que no puede ser él mismo en la industria.**

En una encuesta realizada a los miembros firmantes (+500) de la iniciativa Tech Talent Charter en UK, **el 82% afirma que el género es una prioridad top y el 58% sostiene que la etnicidad es igualmente una prioridad.**

El talento, independientemente de las características de quien lo posee, es muy requerido por la industria de la ciberseguridad, y el hecho de que ese talento se vea afectado por temas de inclusión y no pueda prosperar es una situación altamente indeseable para todo el ecosistema.

La industria debe aprovechar su experiencia en *big data* y otras tecnologías para establecer las mejores prácticas y medir la diversidad e inclusión en las organizaciones.

Fuente: *KPMG & National Cyber Security Centre; Tech Talent Charter.*

Análisis *benchmark* – Programas o actuaciones

Impacto en diversidad e inclusión

UK

El *gap* entre oferta y demanda en ciberseguridad, es un problema tanto inmediato a largo plazo. UK se encuentra en el proceso de **atraer talentos diversos a la profesión** al apoyar, oportunidades para motivar a la fuerza laboral actual a capacitarse (*upskilling and reskilling)* como profesionales de ciberseguridad, y así inspirar a futuros profesionales. Un componente clave de esto es proporcionar una mayor coherencia y coordinación a la gama de iniciativas que se ofrecen.

No.	Nombre de la actuación	Organismo	Descripción	Estado	Resultados
1	***CyberFirst Girls*** Extracurricular	GCHQ NCSC *Partnership*: empresas y colegios Iniciativa CyberFirst	Programa diseñado para **chicas de entre 12-13 años, con el fin de resaltar algunas de las habilidades y aptitudes clave** necesarias para una carrera exitosa en ciberseguridad. Se basa en la competencia en un ambiente desafiante, donde se compite en equipos de 4 y participan escuelas de UK, Irlanda del Norte y Escocia.	Activo Inscripciones cerradas para 2021	En 2020 casi 12.000 mujeres jóvenes entraron en la ronda *online*. • Con apoyo del Gobierno y empresas, en 2020 se realizaron semifinales en 18 ubicaciones en UK, donde participaron 156 escuelas o colegios, para escoger a las 10 finalistas. • Promover el talento de ciberseguridad desde la base de la diversidad. • Incentivar y despertar el interés en las chicas para abordar la temática de la ciberseguridad con mayor confianza.
2	***Women in Cyber Security***	CISSE Partnership LT Harper (Agencia de reclutamiento en ciberseguridad) Iniciativa propia de CISSE	El objetivo de este taller es reunir mujeres profesionales en el campo de ciberseguridad para que compartan su experiencia en la industria.	Activo	• Ofrecer un punto de interacción para futuras estudiantes de ciberseguridad. • Promover un *pipeline* de comunicación y colaboración entre profesionales, estudiantes y educadores. Esto a su vez genera que desde etapas tempranas se diseñen programas acorde con las necesidades reales de las empresas.

Análisis *benchmark* – Programas o actuaciones

Impacto en diversidad y exclusión

UK

No.	Nombre de la actuación	Organismo	Descripción	Estado	Resultados
3	***Diversity & Inclusion*** **Women**	LT Harper (Agencia de reclutamiento en ciberseguridad) Iniciativa **Sector privado**	La compañía tiene un enfoque para aportar a la diversidad en ciberseguridad. **Actualmente el 26% de las contrataciones en ciberseguridad son mujeres.** El objetivo es construir una red de mujeres en ciberseguridad y otorgarles acceso a recursos que apoyen el desarrollo de sus carreras profesionales.	Activo	• Motivar el compromiso organizacional con la diversidad de género en la industria de la ciberseguridad. • Las mujeres pueden hacer uso de una plataforma gratuita de búsqueda de mentores en el mundo de la ciberseguridad. • Promocionar un desarrollo óptimo en los planes de carrera de mujeres en ciberseguridad.
4	***Cyber Skills Immediate Impact Fund*** **(CSIIF)**	Department of Digital, Culture, Media & Sport Iniciativa NA	Este fondo apunta a incrementar rápidamente la diversidad y el número de personas que trabajan en ciberseguridad. Apoya el propósito final de la estrategia nacional de ciberseguridad de desarrollar una oferta sostenible de talento en UK. **La financiación alcanza las £100.000 máximo por iniciativa**.	Última actualización 2019	• El CSIIF ya proporciona financiación a una serie de programas de formación dirigidos a grupos subrepresentados en la industria. Ejemplos notables de proyectos incluyen un campo de entrenamiento de 10 semanas para mujeres y una iniciativa para la comunidad neurodiversa. • Se ha logrado llegar a una gama más amplia de candidatos ofreciendo oportunidades de aprendizaje flexibles para adaptarse a diversos estilos de vida, como, por ejemplo iniciativas con mujeres que regresan a la vida laboral despues de ser madres. • Para el verano de 2018 se estableció el programa y rápidamente 24 candidatos neurodiversos estuvieron listos para iniciar una carrera en ciberseguridad.

Impacto en diversidad e inclusión

UK

Key Takeaways

Se ha llegado a pensar que una de las posibles medidas para incrementar la presencia femenina en la industria es despertando el interés desde temprana edad. En esta línea UK ha diseñado el programa *CyberFirst Girls*, en el que en 2020 casi 12.000 mujeres jóvenes se han inscrito. Este esfuerzo no solo reúne el sector público y privado de UK, sino que involucra la participación de Irlanda del Norte y Escocia.

A través del fondo *Cyber Skills Immediate Impact Fund (CSIIF)*, UK ha logrado incrementar la diversidad y ofrecer oportunidades de aprendizaje flexibles que se adapten a diversos estilos de vida garantiza menos fricción a la hora de incorporar otros colectivos. Este talento no se debe abordar como un esfuerzo adicional, sino como una oportunidad de potencializar un talento de alto valor desde el entendimiento de la diversidad.

Diversidad en ciberseguridad – Iniciativa *NeuroCyber*

UK

En UK hay cerca de 700.000 personas en el espectro del autismo y se cree que este grupo es un potencial desatendido importante, donde más del 75% de los cognitivamente disponibles tienen aptitudes e intereses para que sean profesionales sobresalientes en ciberseguridad.

"It's easier to think outside the box when you already live there"

NeuroCyber

El propósito de *NeuroCyber* es aumentar la neurodiversidad en el sector cibernético a través de prácticas inclusivas

1 **Sensibilización**

2 **Networking**

3 **Mejorar los entornos Inclusivos**

Las organizaciones desconocen el potencial de la fuerza laboral diversa como una ventaja competitiva.

¿Qué actuaciones tienen?

Eventos

- Conferencistas.
- Eventos para conectar a candidatos con organizaciones.

Hub de información

- Espacio idóneo para aclarar las dudas que tienen con respecto a la neurodiversidad.
- Recursos de gran utilidad para empresas y candidatos en diversos canales.

Tips de Inclusión

- Identificar y compartir *tips* basados en hechos para el sector de ciberseguridad.
- Promover un lenguaje común para la industria que mejore la inclusión.

Algunos miembros: Microsoft, HM Government, EY, National Autistic Society, Tech UK y Fujitsu, entre otros.

Fuente: *NeuroCyber*.

Inversión

UK

En UK se espera lograr los resultados planteados en los objetivos de la estrategia de ciberseguridad 2016-2021, buscando invertir de manera más activa, al seguir apoyando tanto la oferta como la demanda para elevar los estándares de ciberseguridad del Reino Unido.

- La estrategia de ciberseguridad señala que se utilizará la autoridad y la influencia del Gobierno británico para **invertir en programas que respondan a la escasez de habilidades en ciberseguridad**, desde las escuelas y universidades hasta toda la fuerza laboral.
- Uno de los imperativos estratégicos de esta estrategia, **en los cuales se basa su política de inversión, es**: “UK necesita una industria de ciberseguridad dinámica y una base de habilidades de apoyo que pueda seguir el ritmo y adelantarse a la amenaza cambiante”.
- De cara a lograr reducir su exposición a daños cibernéticos, UK considera imprescindible **equilibrar los riesgos con suficiente inversión en las personas, tecnología y gobernanza**.

El presupuesto total asignado durante el periodo de ejecución 2016-2021 es de £1.900 millones.

Otras actuaciones y/o programas

UK

ADA National College for Digital Skills

ADA se especializa en capacitación de alto nivel para *skills* digitales → Estudiantes (16 años) y futuros profesionales.

A través de *apprenticeships* y la validación de sus componentes de aprendizaje por *Open University*, el objetivo es que todos los estudiantes culminen con un grado profesional. Ofrecen Innovación digital, *data analytics* y entre otros. Su metodología está diseñada para adaptarse a empleos a tiempo completo y utiliza un enfoque de aprendizaje mixto, que combina el estudio basado en el trabajo y asistencia a ADA (80-20).

National Occupational Standards (NOS)

Esfuerzo conjunto con los Gobierno de Escocia y Gales → Organizaciones y profesionales.

Los NOS son declaraciones de los estándares de desempeño que las personas deben alcanzar al desempeñar funciones en el lugar de trabajo, junto con especificaciones de los conocimientos y la comprensión subyacentes. Este programa facilita que las organizaciones encuentren el estándar que más se ajusta a sus necesidades según la especialidad y sector al que pertenecen. Esto busca incorporar ciberseguridad para cambiar la cultura empresarial.

Institute of Coding (IoC)

Ha reunido a *partners* de la industria, Gobierno y educación superior para crear más de 150 cursos → Estudiantes.

El IoC mejora las capacidades digitales de alto nivel, impartiendo cerca de 24 cursos en ciberseguridad, a través de un amplio consorcio de universidades, organizaciones profesionales y empleadores, que tienden a mejorar el flujo del talento en el mercado. Se ha involucrado a más de 800.000 estudiantes hasta la fecha.

Conclusiones

VARIABLE	UK	DETALLE
***Framework* talento en seguridad para el Gobierno de UK**		Este recurso aparenta ser muy estratégico para quienes tienen el interés en emprender un proyecto de desarrollo profesional en seguridad. El contenido es robusto en cuanto a roles, habilidades y desarrollo personal y profesional. Sin embargo no hay evidencia clara de que tenga sinergias con el sector privado.
***Cybersecurity Body of Knowledge* (CyBOK)**		Es probablemente el marco de referencia más robusto en ciberseguridad en UK. A pesar de no tener actuaciones enfocadas al talento en sí, logra codificar el conocimiento que sustenta el sector y plasmarlo en 19 áreas diferentes.
Impacto en organizaciones (públicas y privadas)		El avance que ha alcanzado UK se ve más reflejado naturalmente en las instituciones del gobierno. Es notable que el progreso de la industria dependerá en gran medida de cómo logren trasladar ese *expertise* al sector privado.
Impacto en profesionales en ciberseguridad		UK sugiere constantemente que sus capacidades deben ser de clase mundial y en esta línea desarrollan el *framework* para el desarrollo profesional. Adicionalmente, para UK las certificaciones son fundamentales, como un aval de la calidad que se espera del desempeño de los profesionales.
Impacto en estudiantes		Las actuaciones están alineadas con el objetivo de la estrategia de garantizar una fuerza laboral competente para todos los sectores. Se trazan objetivos en diferentes horizontes de tiempo impactando varias etapas de la formación.
Impacto en escuelas y universidades		Las iniciativas más visibles se enfocan en la excelencia a través de la colaboración y consolidación de *partnerships*. Por otra parte, algunas de sus actuaciones se centran en poder innovar los planes de estudio.
Inclusión (mujeres y minorías)		Es notorio el compromiso con la diversidad a través de algunas actuaciones, logrando que en algunos casos las minorías estén mejor representadas en la industria que en la población en general.
Inversión		La cantidad de recursos para atacar la problemática parece estar disponible, por falta de información no ha sido posible determinar cómo realizará la asignación real de los recursos.

 No iniciada
 Incipiente
 En proceso
 Desarrollada
 Muy desarrollada

Conclusiones y recomendaciones

- *La estrategia de ciberseguridad de UK es ambiciosa, tiene posiciones tanto como defensivas como ofensivas en materia de seguridad y, en relación con el talento, el objetivo primordial es desarrollar un pipeline autosostenible que proporcione las capacidades para satisfacer las necesidades del sector público y privado.*
- *UK está en el proceso de desarrollar e implementar una estrategia de talento autónoma, que construya sobre el trabajo realizado e integre la ciberseguridad tanto en el sistema educativo como en todos los sectores de la economía.*
- *La esencia de la estrategia para la gestión del talento en UK es garantizar la combinación y el nivel adecuados de capacidades en ciberseguridad en toda la economía, reflejando el compromiso y comprensión del contexto sobre el talento en ciberseguridad.*
- *El framework estudiado para UK ayuda a los profesionales en su desarrollo profesional a partir de la definición de unos roles y sus respectivas habilidades a desarrollar para garantizar un adecuado desempeño. El foco está en los empleados del Gobierno y las áreas principales de este son: career pathways, skills & development.*
- *El proyecto CyBOK busca alinear la ciberseguridad con el resto de las disciplinas y actividades mediante el conocimiento de expertos en múltiples áreas de conocimiento. Específicamente para la parte de gestión de talento no determina acciones puntuales, pero sirve como base para describir contenido de ciberseguridad, útil para el diseño de planes de estudio y, además resalta la importancia de la concienciación, educación y capacitación para lograr un impacto en el comportamiento humano frente a la seguridad.*
- *El organismo insignia para la ciberseguridad en UK es el National Cyber Security Centre, el cual brinda apoyo a los entes más críticos de UK en materia de ciberseguridad. Es posiblemente el organismo que mejor entiende la ciberseguridad, destila este conocimiento en acciones prácticas a disposición de su ecosistema y utiliza la experiencia académica y de la industria para fomentar las capacidades en ciberseguridad.*

Conclusiones y recomendaciones

- *La mayor ambición que tiene UK es ser el líder mundial en ciberseguridad y reconoce que esto solo es posible teniendo acceso a un pipeline sostenible con el mejor talento de ciberseguridad.*
- *UK se está enfocando principalmente en mejorar las habilidades de la fuerza laboral del sector público en todos los niveles jerárquicos para mantener los sistemas y datos seguros.*
- *UK reconoce la dificultad de cuantificar con precisión el verdadero gap de la fuerza laboral en ciberseguridad. Sin embargo, expresan que cada parte del sector público debe tener un plan para abordar esta brecha de capacidades. En consecuencia, ha tratado de comprender mejor la naturaleza y los matices de la oferta y la demanda para darse una imagen más completa de dónde se percibe el gap, y así emprender acciones con un fuerte enfoque en el aprendizaje, reciclaje y la retención del talento.*
- *La ciberseguridad se está convirtiendo en un elemento importante en los planes de estudio en todos los niveles educativos. Sin embargo, el conocimiento fundamental sobre el que se está desarrollando el campo de la seguridad cibernética está fragmentado y, como resultado, puede ser difícil tanto para estudiantes como para educadores trazar caminos coherentes de progresión a través de la asignatura.*
- *Uno de los lineamientos que se pueden seguir para determinar el impacto real de las iniciativas enfocadas a un cambio de cultura son las métricas. Por ejemplo, nº de empleados que completan capacitación sobre awareness en ciberseguridad.*
- *La formación en STEM como habilitador de roles en ciberseguridad es clave y es algo que está faltando. Se necesitan más acciones tendientes a mejorar esa oferta para que los reclutadores no tengan esa dificultad a la hora de encontrar los candidatos que mejor se ajustan a las posiciones.*
- *El compromiso de UK con la excelencia se ve reflejado, entre otros, en el programa Academic Centres of Excelence in Cyber Security Education and Certified Degrees (ACE-CSE). Esta actuación aborda conocimientos, habilidades y capacidades para la investigación y educación. Reúne un alto numero de universidades con diversos másteres y grados y facilita información valiosa para que los estudiantes tomen decisiones más informadas.*

ISRAEL

ISRAEL

¿Qué orden seguiremos?

- Postura de ciberseguridad de Israel.
- Estructura y organismos que participan y tienen competencias relacionadas con la ciberseguridad.
- Análisis *benchmark*.
- Conclusiones y recomendaciones.

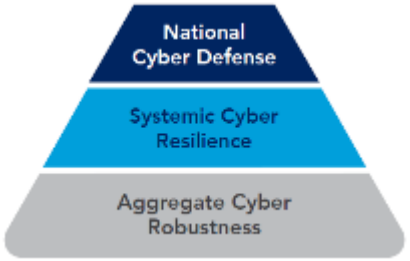
Postura actual de ciberseguridad y ciberdefensa nacional

ISRAEL

Israel ha logrado posicionarse como uno de los jugadores más importantes del mundo en el ámbito de la ciberseguridad y ciberdefensa.

La manera en la que ha llegado a este punto ha sido esencialmente con un **ecosistema proactivo de inteligencia e innovación, financiado correctamente**. Este esfuerzo y apuesta por la seguridad le ha llevado a reforzar su alianza estratégica con EE.UU. y a involucrarse más en la definición de políticas internacionales para el ciberespacio.

Israel ha adoptado un **enfoque integral de política de ciberseguridad** con un enfoque específico en el desarrollo de:

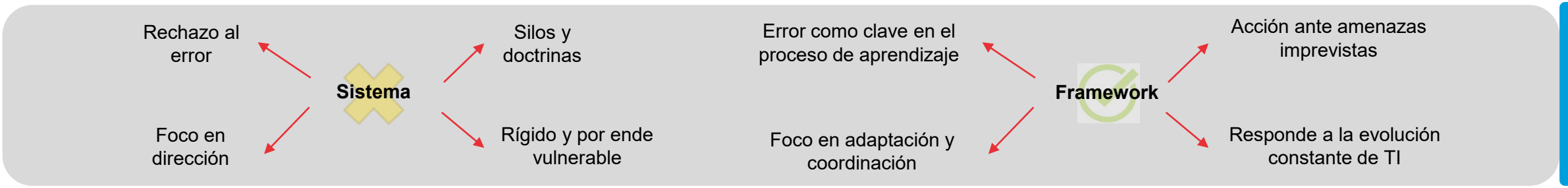


¿Cual es el principal organismo que gestiona la ciberseguridad en Israel?

Cyber Israel
National Cyber Directorate

La ciberseguridad en Israel se reconoce como algo dinámico o en **constante cambio**, y el enfoque que tiene hacia la materia es una **lección de adaptación**. En este sentido, Israel logra un cambio de dirección:

- Israel rechaza la división entre defensa y ataque, ya que los considera como una necesidad continua.
- Enfoque holístico y flexible.
- Ser reconocido como uno de los líderes de la industria tiene un coste y un riesgo latente de ataques. Israel ha logrado mitigar esto eficientemente.
- Una visión acerca de la importancia futura del ciberespacio.

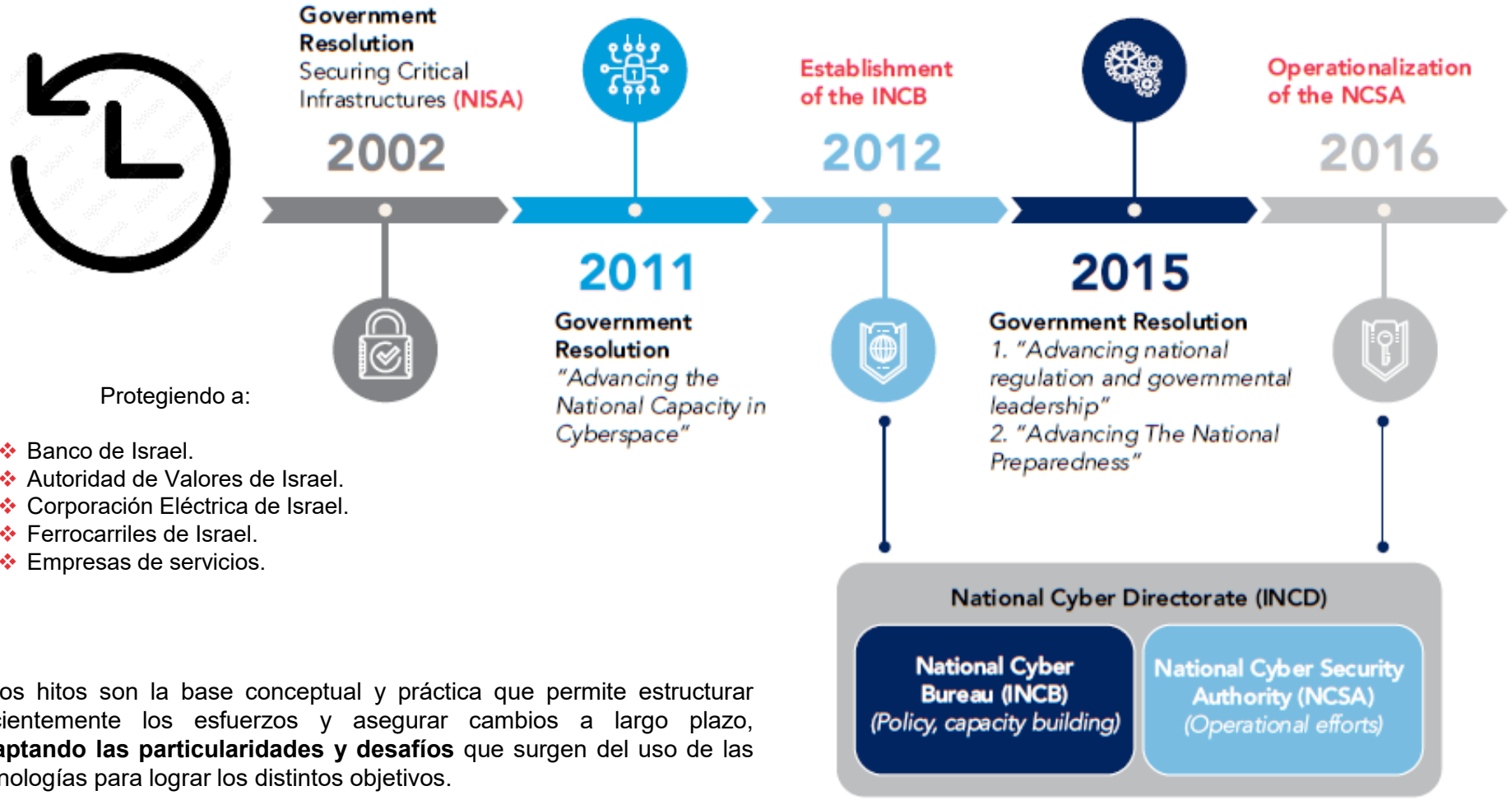


El desarrollo de esta postura solamente ha sido posible con la estrecha **coordinación entre los actores públicos y privados nacionales e internacionales.**

Desarrollo de los esfuerzos de ciberseguridad en Israel

ISRAEL

Israel ha tenido la **visión** de ser una nación líder en el **aprovechamiento del ciberespacio, como motor de crecimiento económico, bienestar social y seguridad.**



Protegiendo a:

- Banco de Israel.
- Autoridad de Valores de Israel.
- Corporación Eléctrica de Israel.
- Ferrocarriles de Israel.
- Empresas de servicios.

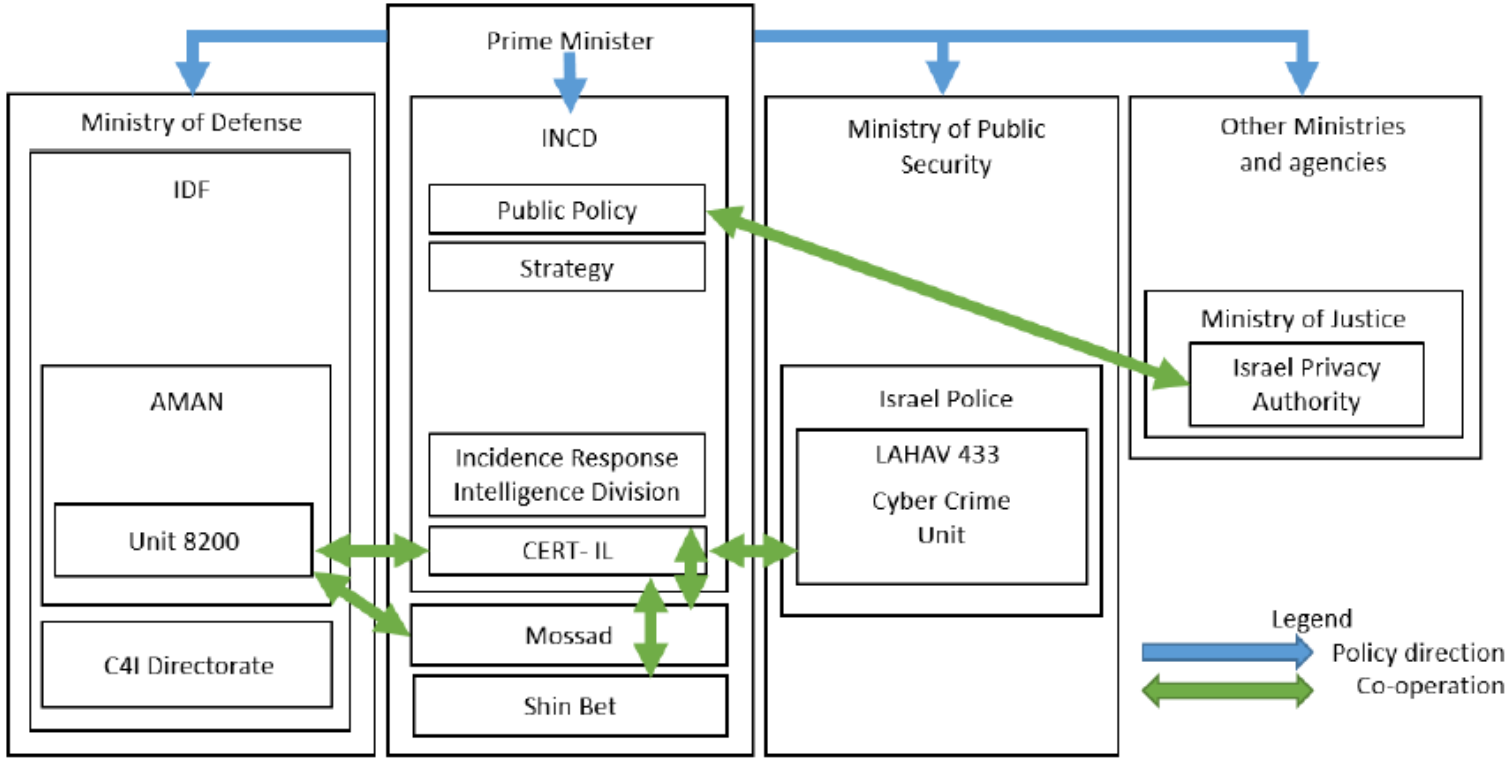
- Antes de 2017 Israel nunca había formulado una estrategia de ciberseguridad nacional oficial e integral.
- Una estrategia para Israel es en esencia un **medio para hacer realidad una visión** cibernética, manteniendo el ciberespacio seguro y enfrentando las diversas amenazas.
- Para Israel, uno de los objetivos centrales es **garantizar el papel continuo en el escenario internacional**.
- La *Dirección Cibernética Nacional de Israel* o *Israel National Cyber Directorate*, publicada en 2020, es considerada la primera publicación que **conecta los principios de la seguridad nacional, con los intereses actuales de las empresas y la ciudadanía**.

Estos hitos son la base conceptual y práctica que permite estructurar eficientemente los esfuerzos y asegurar cambios a largo plazo, **adaptando las particularidades y desafíos** que surgen del uso de las tecnologías para lograr los distintos objetivos.

Estructura para la gestión de la ciberseguridad

ISRAEL

El diagrama refleja la **estructura de las organizaciones que tienen competencias en ciberseguridad** y la manera en la que se coordinan y cooperan las agencias más importantes del Gobierno con otras dependencias críticas en la formulación de políticas y cooperación.



- El diagrama describe la mayor autoridad en Israel y puede, cuando es necesario, imponer medidas y obligar a las empresas a seguir determinadas directrices en materia de ciberseguridad.
- El Israel National Cyber Directorate es la autoridad máxima en cuestión de ciberseguridad y depende directamente de la oficina del primer ministro.
- Las funciones esenciales de este organismo son: la planificación de políticas para que el país sea cada vez más robusto en ciberseguridad, facilitar la cooperación internacional, formular un marco legal de las actividades a realizar tanto en el territorio nacional como internacionalmente, gestionar integralmente las campañas y mejorar la resiliencia. Hay colaboración con otras agencias de inteligencias como, Amán o Mossad.

Fuente: *Israel National Cyber Directorate* (INCD).

Organismos con competencias en talento de ciberseguridad

ISRAEL

Cyber Israel
National Cyber Directorate

Funciona como un órgano asesor del primer ministro, el Gobierno y sus comités, que recomienda la política nacional en el campo cibernético y promueve su implementación, de acuerdo con la ley y las resoluciones gubernamentales.

Oficina del Primer Ministro de Israel

Israel Defense Forces (IDF)

El Estado Mayor o el Cuartel General de Israel es el mando supremo.
Están integrados por las fuerzas terrestres, aéreas, navales, teleprocesamiento, tecnológico y logístico e inteligencia militar.
Es la única ala militar de las fuerzas de seguridad israelíes y no tiene jurisdicción civil dentro de Israel.

National Cyber security Authority

Entidad de seguridad israelí responsable de proteger el ciberespacio civil israelí durante 2016-2018. La NCSA brindó servicios de manejo de incidentes y orientación para todas las entidades civiles, así como todas las infraestructuras críticas.

National Cyber security Bureau

Designado para ayudar al primer ministro en la elaboración de una Política Cibernética Nacional y fomentar la aplicación de sus aspectos de seguridad nacional. Específicamente se asignó para desarrollar una estrategia nacional.

Aman

La Dirección de Inteligencia Militar es el organismo central de inteligencia militar de las Fuerzas de Defensa de Israel.

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

El CEC fue fundado por la Fundación Rashi, una de las organizaciones filantrópicas más grandes e influyentes de Israel, y el Ministerio de Defensa, con la visión de impulsar el cambio social en Israel a través de la educación tecnológica.

C4i

La dirección C4i es la unidad tecnológica de élite de las Fuerzas de Defensa de Israel (IDF). La principal actividad es proporcionar a los comandantes en el campo la tecnología todo lo que necesitan para manejar una situación de combate de la mejor manera posible. Los principales objetivos de la dirección son iniciar, desarrollar, explotar y fortalecer el sistema de integración tecnológica de las IDF.

HackerU

Con más de una década de experiencia como el principal instituto de capacitación en tecnología digital de Israel, HackerU es un proveedor de renombre mundial de educación tecnológica, servicios de ciberseguridad y transferencia de conocimiento de alto calibre.

UNIT 8200

Unidad del Cuerpo de Inteligencia israelí de las Fuerzas de Defensa, responsable de recopilar inteligencia de señales (SIGINT) y descifrar el código.
Además, es responsable de tareas ofensivas.
Podría ser el equivalente al NSA en EE.UU.

Creación del National Cyber Directorate

ISRAEL

Un buen ejemplo de la **voluntad y capacidad de cambio de dirección** que tiene Israel se refleja en cómo estableció en 2015 el National Cibersecurity Authority dentro de la oficina del primer ministro, con el objetivo de proteger el ciberespacio civil israelí, y cómo tan solo dos años después reconoció que esto **no respondía a las necesidades** de seguridad del país, y el primer ministro Benjamin Netanyahu estableció el National Cyber Directorate.

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Unificación del National Cibersecurity Authority con el National Cyber Bureau

Cyber Israel
National Cyber Directorate

Subordinada a la oficina del Primer Ministro

Esta unificación permitió la **gestión estratégica de políticas de seguridad,** junto con el **despliegue de capacidades operativas,** bajo un solo organismo:
La Dirección Cibernética Nacional de Israel.

En este contexto, a esta dirección se le confían todos los aspectos de la defensa cibernética de Israel, desde la **formulación de políticas** hasta la **creación de poder tecnológico**.

Propósito: defender el ciberespacio nacional de Israel de las amenazas cibernéticas y **promover y establecer las capacidades de ciberseguridad**.

Visión: un ciberespacio seguro y gratuito en Israel que recalca el crecimiento económico y mejora la postura estratégica general del país.

Objetivos

Defensa → Liderar los esfuerzos de defensa del ciberespacio nacional mediante **la prevención, detección, identificación y respuesta** a los ciberataques.

Resiliencia → Preparar y permitir que el sector privado israelí y el público en general se protejan de las amenazas mediante la **adopción de tecnologías seguras, la publicación de las mejores prácticas, la capacitación del personal y la concienciación**.

Liderazgo en innovación → Establecer y reforzar la base de la ciencia y la tecnología mediante el **desarrollo de capital humano de alta calidad**, el apoyo a la investigación académica avanzada, la participación en una profunda I+D tecnológica y el fomento de la industria, al tiempo que combina lo anterior en un ecosistema vibrante.

Postura internacional → Promover al Estado de Israel como líder mundial en ciberseguridad, fortaleciendo así su defensa, su resiliencia económica y su posición internacional, a través de la colaboración internacional, el **desarrollo de capacidades** y la participación de procesos multilaterales.

Estrategia y política → Diseñar y formular una estrategia y política de ciberseguridad creando un punto focal de **conocimiento y autoridad profesional** en la política cibernética.

Cyber Defense Doctrine – Guide to Organizational Cyber Defense

ISRAEL

El propósito de la doctrina de defensa es presentar al tejido productivo un **método profesional ordenado para gestionar los riesgos cibernéticos en la organización.** Usando este método, la organización reconocerá los riesgos relevantes, formulará una respuesta defensiva e implementará un plan de reducción de riesgos en consecuencia.

¿Qué es?

La doctrina de defensa organizacional es un elemento constitutivo de la *Estrategia Nacional de Seguridad Cibernética*, que consta de varios niveles de defensa para la economía israelí y su continuidad funcional.

¿Cuál es el enfoque?

La doctrina ve a la organización como un todo y permite **elevar el nivel de resiliencia** organizacional a través de la asimilación continua de procesos, métodos y productos de defensa.

Esta doctrina **identifica y clasifica a las organizaciones** dependiendo del grado de riesgo al que están expuestas en caso de un ataque.

Categoría A

Organizaciones con **potencial de riesgo o daño medio-bajo** como resultado de un incidente cibernético (hasta USD 1,5M).

Categoría B

Organizaciones con **potencial de riesgo o daño alto** como resultado de un incidente cibernético.

Posteriormente, esta doctrina **realiza un proceso de evaluación y gestión de riesgos**.

Se define primero **cuáles son los principales objetivos** de defensa (generalmente procesos de negocio o activos digitales), **qué nivel de defensa se requiere** y **cuáles son las brechas** para luego proceder a **construir un plan de trabajo**. En este sentido, la doctrina presenta diferentes métodos de evaluación.

Como resultado, el producto final después de trabajar bajo esta doctrina **permite que la organización comprenda el mapa de riesgos y los controles necesarios** para reducir esos riesgos, incluidas las prioridades para implementar el plan de trabajo.

Las actividades de ciberdefensa se llevan a cabo debido al **deseo de la organización de gestionar los riesgos** a los que está expuesta.

Fuente*: INCD*.

Cyber Security Awareness Training – for organizations and employees

ISRAEL

La plataforma usada para compartir recursos de carácter formativo con la finalidad de **crear conciencia o *awareness* entre la población civil y las organizaciones** en Israel es gestionada por la *Dirección Cibernética Nacional de Israel* (INCD).

Propósito de la formación

- Reconocer y comprender las ciberamenazas organizacionales y personales.
- Aprender herramientas y recomendaciones básicas para ayudar a reducir las amenazas cibernéticas, la actividad misma del ciberespacio personal y organizacional.
- Que las empresas y la ciudadanía conozcan el factor profesional con el que se puede contactar y/o informar en caso de emergencia.

Descripción de la formación

- Responsabilidad del empleado en la organización.
- Formas (proceso o fases) de un ciberataque.
- Recomendaciones de defensa.

Resultados

- Una población más consciente de los riesgos y daños para proteger mejor la información y los activos.
- Empleados conscientes de la conducta humana como un factor de riesgo.
- Conocimiento acerca de las herramientas que se ponen a disposición (tecnológicas) y sobre su uso responsable.

Israel es partidario de que capacitar a los empleados sobre cómo reconocer y responder a las amenazas cibernéticas puede mejorar drásticamente la resiliencia cibernética de las organizaciones.

Fuente*: INCD*.

Análisis *benchmark*

HackerU (I/III)

ISRAEL

Esta iniciativa busca empoderar la fuerza laboral digital global y cuenta con más de una década de experiencia como el **principal instituto de capacitación en tecnología digital de Israel**. Es un proveedor de renombre mundial de educación tecnológica, servicios de ciberseguridad y **transferencia de conocimiento de alta calidad**.

HackerU

Our Mission

La misión principal de HackerU es **transformar diversos grupos** de estudiantes de diversos orígenes socioeconómicos y construir las fuerzas de trabajo cibernéticas y digitales del mundo, a través de un **ecosistema único encabezado por innovación tecnológica, servicios líderes en la industria y capacitaciones impulsadas por el mercado**.

Foco en diversidad

On The Global Level

Disminuir el *gap* de fuerza laboral global capacitando a la próxima generación de expertos digitales y cibernéticos para construir ecosistemas tecnológicos sostenibles en todo el mundo.

On The Local Level

Sostener las redes de negocios locales equipando a las empresas con tecnólogos digitales calificados y candidatos en ciberseguridad desarrollados dentro de la comunidad local.

On The Individual Level

Brindar oportunidades y movilidad a millones de personas en todo el mundo, mientras se reduce la creciente escasez de candidatos de la fuerza laboral con habilidades digitales.

Situado en el centro del desarrollo tecnológico israelí, HackerU es una de las únicas organizaciones que **prestan servicios tanto al sector de alta tecnología como al sector educativo**, simultáneamente.

Fuente: *INCD.*

Análisis *benchmark*

HackerU (II/III) – Desarrollo profesional

ISRAEL

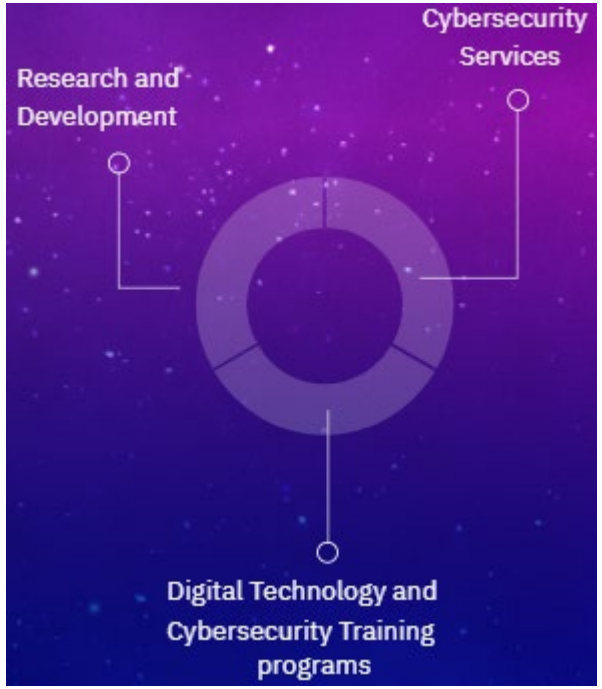
Los profesionales en ciberseguridad **usan las mismas técnicas y herramientas avanzadas que usan los actores de amenazas** reales para exponer las brechas de seguridad en la infraestructura de red y protegerla antes de que los ataques puedan causar daños.

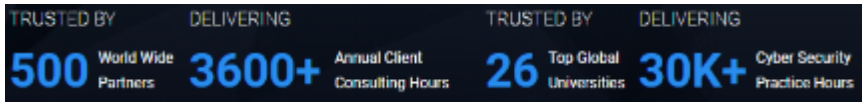
From Local

1. **Desarrollo de carrera**, incluyendo asesoría y eventos de *networking*, conectando estudiantes con oportunidades de trabajo.
2. **Redes para los negocios**, construyendo desde cero, implantando profesionales al ámbito local y satisfaciendo lo demanda de la industria.
3. **Profesorado local**, reclutando desde la industria local y conectando otros expertos para ofrecer formación y planes de estudio más elaborados.
4. **Programas orientados al mercado**, desarrollados por expertos que trabajan en la industria para alinear con el mundo digital actual.

To Global

1. **R+D**, estudiando tecnologías emergentes y estrategias digitales para proveer los planes de estudio más relevantes.
2. **Material de los cursos**, actualizando constantemente los programas con las herramientas y tecnologías más punteras.
3. **División de inversión** en tecnología punta, trayendo economías de escala a través de todas las iniciativas de transferencia de conocimiento.
4. **Soluciones HackerU**, servicios de ciberseguridad y marketing digital a cientos de empresas y administraciones públicas.





- **Seguridad defensiva** → La mejor seguridad es la seguridad proactiva y preventiva:
  - **CISO *as a service*** (estrategia).
  - **Evaluación de riesgos.**
  - **Cumplimiento y Gobierno.**
  - **Respuesta a incidentes.**
  - **Revisión de código.**

- **Seguridad ofensiva:**
  - ***Penetration Testing.***
  - ***Red Team Simulations.***
  - **Campañas de *phishing*.**
  - **Evaluación de redes.**

HackerU es considerado el socio de referencia tanto para organizaciones públicas y privadas, así como para instituciones académicas, pues sus **programas son diseñados especialmente por expertos** de la industria para que la los profesionales estén mejor preparados de cara a ingresar a la fuerza laboral.

HackerU (III/III) – Programas de Grado

ISRAEL

Cada graduado de HackerU comienza su nueva carrera con las **herramientas y los conocimientos esenciales necesarios para sobresalir como profesional** en la era digital. Miles de expertos de la industria dan su primer paso en estos programas, y su éxito es un testimonio del compromiso de brindar los mejores programas de capacitación en el mundo.

01 Hands-On Simulation Labs

Los programas de HackerU cuentan con laboratorios de simulación prácticos que preparan completamente a los estudiantes para escenarios del mundo real. Este entorno de aprendizaje inmersivo permite a los graduados de HackerU estar verdaderamente preparados para un empleo al momento de terminar los estudios.

02 Expert Instructors

Todos los programas de HackerU están diseñados y entregados por profesionales líderes en tecnología con antecedentes probados en sus respectivos campos. Como líder mundial en tecnología digital y educación en ciberseguridad, HackerU se compromete a compartir su conocimiento para establecer profesionales preparados para el trabajo.

- .Net Programming
- Ethical Hacking — Data & Cyber Security
- Programming QA
- Linux Server Management
- Gaming & VR
- Full Stack Development
- UX Design
- iPhone & Android App Development
- Digital Marketing — Social Media, Advertising & SEO
- Maya 3D Animation — with ZBrush Specialization
- Network System Administration
- DBA Master
- Automation Development QA
- Red Team Specialist
- Blue Team Specialist

03 Unique Recruitment Process

Ofrecen a las instituciones académicas un programa de orientación único que maximiza la inscripción y retención de estudiantes. A muchos futuros estudiantes les preocupa que un cambio de carrera no cumpla con sus objetivos a largo plazo. HackerU minimiza esta incertidumbre con una fase de prueba, donde los estudiantes escogen un campo de tecnología y tienen un tiempo de prueba antes de comprometerse con el programa completo.

04 Global Certifications

Enfocados en las necesidades locales y globales, los programas de HackerU brindan a los estudiantes la capacitación necesaria para aprobar los exámenes de certificación más esenciales de la industria. El plan de estudios está diseñado para que los estudiantes estén completamente preparados para realizar trabajos inmediatamente después de la graduación.

05 Career Assistance

Con más de 12.000 graduados en todo el mundo, HackerU se esfuerza por reducir la brecha global de la fuerza laboral trabajando con miles de empresas y satisfaciendo directamente sus necesidades. Además, optimizan el proceso de contratación con *partners* de reclutamiento en todo el mundo.

Análisis *benchmark*

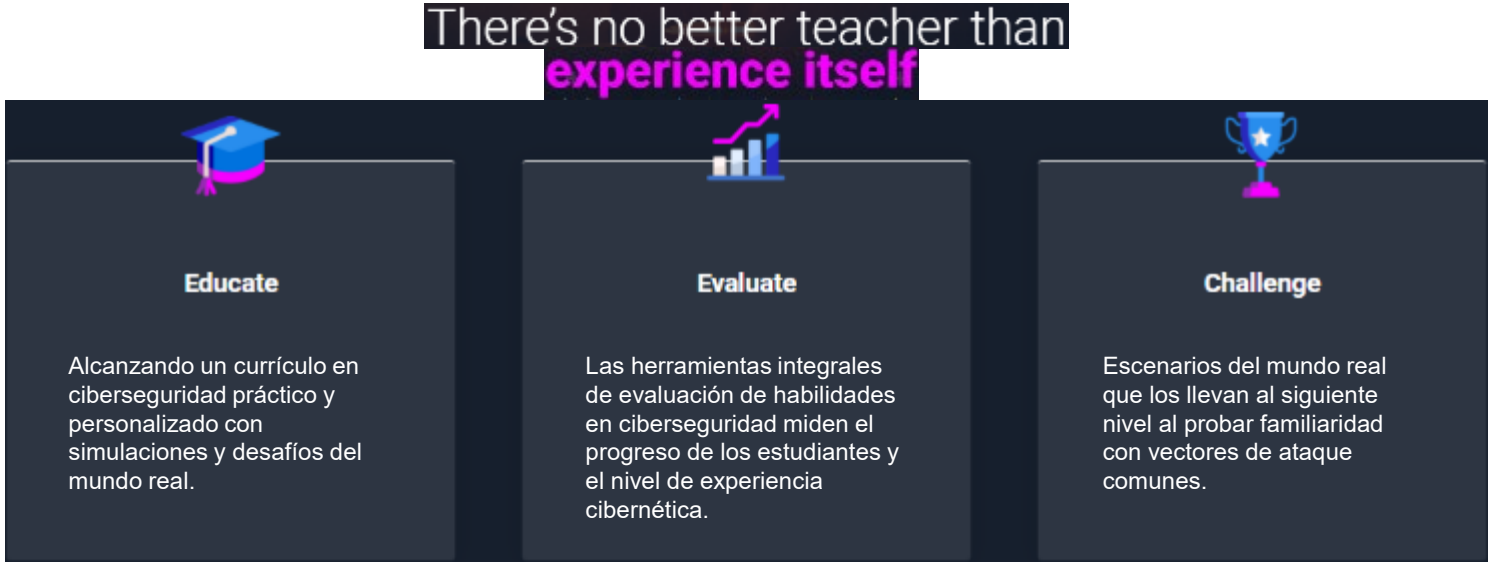
Cywar

ISRAEL

Este portal de aprendizaje práctico de clase mundial, concebido y desarrollado por líderes mundiales en ciberseguridad, tiene como finalidad capacitar a una nueva generación de profesionales cibernéticos.

¿Por qué esta iniciativa?

Cywar es una plataforma *top of the line* educativa de ciberseguridad, que permite a los estudiantes y profesores aprovechar todos los beneficios del aprendizaje asincrónico. 100% accesible desde la nube, en cualquier momento y en cualquier lugar desde cualquier dispositivo, los equipos internos y los aspirantes a profesionales de la ciberseguridad confían en los programas personalizables, las simulaciones del mundo real y los ejercicios de capacitación de *Cywar* para desarrollar y dominar sus habilidades cibernéticas.



En un **escenario práctico**, adecuado para estudiantes de todos los niveles, desde principiantes hasta expertos, con el objetivo de perfeccionar sus habilidades, *Cywar's Practice Arena* centraliza una colección diversa de contenido práctico desde los elementos básicos de ciberseguridad hasta los escenarios más avanzados y complejos del mundo real.

Cywar's Challenges ofrece a los aspirantes de cualquier nivel una experiencia de aprendizaje ludificada y actividades prácticas. Incluye una biblioteca continuamente actualizada de escenarios del mundo real, así como una variedad de pruebas y máquinas virtuales a las que se puede acceder desde cualquier lugar y dispositivo.

Esta iniciativa cuenta con las herramientas necesarias para que los futuros expertos en ciberseguridad puedan aplicar y **obtener acreditaciones**.

Aprendizaje asincrónico: en esencia, el aprendizaje en línea asincrónico permite a los estudiantes ver el material educativo cada semana en el momento que ellos elijan.

Análisis *benchmark*

Cyber Education Center

ISRAEL

El CEC fue fundado por la Fundación Rashi y el Ministerio de Defensa, y lo que espera este centro es **impulsar un cambio social a través de la educación en tecnología**.

- En Israel se piensa que cultivar la excelencia, junto con el avance de la educación y capacitación cibernética y tecnológica, son fundamentales para **lograr un cambio social real** y un medio para demostrar que se pueden **brindar igualdad de oportunidades** a los niños y niñas de la generación futura de Israel.
- Además de ofrecer una variedad de programas y proyectos a nivel nacional, **invierte considerables recursos y esfuerzos en el desarrollo de programas educativos no formales, dirigidos a estudiantes en la periferia geográfica y social de Israel.**

Driving change in the social periphery

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

2,000 Graduates

3,000 Apprentices and trainees

80 Study centers nationwide

300 Volunteers

30 High-tech companies are partners

330 Staff

Leading gender equality

- El CEC se ha propuesto liderar el cambio hacia la igualdad de género y, con ese fin, creó la comunidad CyberGirlz. Esta comunidad ofrece a las niñas una amplia variedad de actividades en el campo de la tecnología, así como **programas educativos diseñados especialmente para ellas**. A través de este esfuerzo, el Cyber Education Center espera garantizar que las mujeres desempeñen un papel fundamental en el mundo tecnológico del mañana.

La experiencia del CEC muestra que, cuanto a más temprana edad los niños y niñas comiencen a aprender tecnología y computación, mejor. Con este fin, se ha diseñado una serie de programas de educación tecnológica adicionales, dirigidos a los más pequeños.

Análisis *benchmark*

Cyber Education Center

ISRAEL

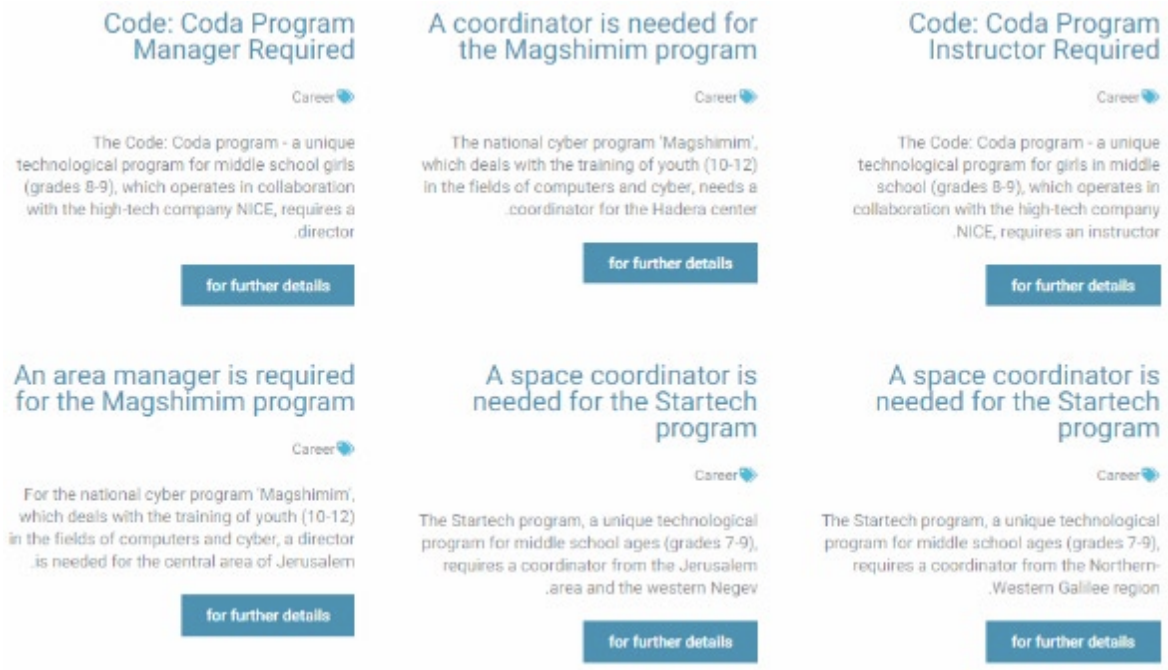
Para los profesionales Israel ofrece una **plataforma con puestos de trabajo que tienen un valor social**. En ese sentido, el CEC trabaja para reducir la disparidad social a través de la excelencia.

Valores *que promuevan igualdad.*
Calidad *que se refleje en el trabajo.*
Compromiso *con la profesión y la industria.*

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

Esta misma plataforma, además de apoyar que los profesionales se puedan postular a diferentes posiciones, sirve para ayudar en el **proceso de reclutar educadores o profesores** para los mismos cursos que imparte el CEC.

Esto refleja un **ecosistema integrado** y robusto que sirve a diversos grupos de interés.



Además de esto, los profesionales tienen a su disposición recursos *online,* como libros digitales y cursos en línea, que suman a su formación en ciberseguridad. Aportar estas y otras herramientas, según Israel, incrementa significativamente la probabilidad de vincularlos al servicio del país.

Análisis *benchmark*

Programa Magshimim

ISRAEL

Israel valora su capital humano y ha invertido mucho en **sus ambiciones, habilidades y experiencia para empoderarlos tecnológicamente**. La ciberseguridad tiene tanta prominencia en Israel que **la educación en la materia comienza en la escuela secundaria**. Esto lo convierte en un **país pionero que enseña ciberseguridad** como una opción. Además de eso, muchas universidades en Israel ofrecen una **especialización de pregrado en seguridad en Internet**, y es el primer país en la historia en ofrecer un **PhD en ciberseguridad**.

- Los **estudiantes de décimo grado están aprendiendo habilidades de ciberseguridad** y muchos de ellos pueden ser reclutados posteriormente por agencias de defensa o inteligencia nacional, como la Unit 8200.
- **El programa extracurricular Magshimim** (lanzado en 2011), para estudiantes de secundaria sobresalientes de zonas desfavorecidas del país, enseña programación, código, cifrado y cómo defender una red contra el *hacking*.
- Este programa **integra temáticas que despiertan el interés de los jóvenes**, como pueden ser personajes animados, y lo combina con ejercicios de simulación para el desarrollo de habilidades.

- Una de las diferencias más significativas en Israel es que **la mayoría de los graduados de la escuela secundaria son llamados al ejército**, lo que ofrece a Israel un gran grupo de talentos para unirse a los esfuerzos oficiales del país.
- Israel está particularmente enfocado en **reclutar, a más talento femenino a temprana edad** para que se una a programas como *Magshimim*. De hecho, uno de los directores regionales del programa va a las escuelas a reclutar chicas para el programa.

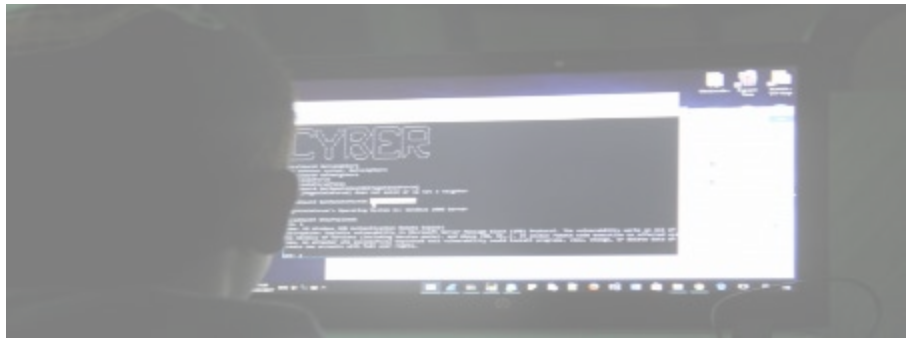
"Mi mejor frase es decirles que hay una oportunidad aquí para estudiar algo que no muchos adolescentes en todo el mundo tienen la oportunidad de tener. Una oportunidad que si ni siquiera intentas aprovechar, podrías perderte de algo que puede cambiar tu vida".
Ofir Ben Yair, director regional del *Programa Magshimim*.

Magshimim Program

+530 *students completed the program.*

+4.800 *students in the next 5 years.*

Los estudiantes han diseñado aplicaciones para permitir que los profesores controlen de forma remota los ordenadores de sus estudiantes, con el fin de administrar una clase en línea.



Magshimim es un programa con foco en grupos poco representados, que el primer ministro lo declaró como el programa oficial de capacitación cibernética de Israel.

Análisis *benchmark*

Iniciativa Shift

ISRAEL

Iniciada como parte de los esfuerzos para promover la igualdad de género en tecnología, **la comunidad *Shift* empodera a las adolescentes** al compartir experiencias, y el aprendizaje entre pares y conocer modelos a seguir.

PURPOSE

El sector de TI de Israel, aunque goza de reconocimiento mundial, sigue siendo en gran medida un "club de hombres" en el que las mujeres son una pequeña minoría. La comunidad Shift fue iniciada por el Centro de Educación Cibernética de Rashi, como parte de los esfuerzos para promover la igualdad de género. Su programación se basa en el entendimiento de que para lograr un impacto significativo debemos introducir a las chicas en el mundo de la ciberseguridad lo antes posible.

Sh!ft

La comunidad fue concebida como una red social para compartir experiencias y aprendizaje entre pares. Sus miembros disfrutan de una variedad de actividades en línea y del mundo real, entre ellas: *hackatones*, visitas a empresas de TI, reuniones con mujeres exitosas en el campo, maratones de estudio antes de los exámenes en ciencias de la computación y un foro en línea que ofrece servicios de apoyo profesional.

GOAL

El objetivo de *Shift* es alentar a las adolescentes a especializarse en ciencias de la computación y otras asignaturas tecnológicas en la escuela secundaria, así como apoyar a quienes elijan hacerlo, fomentando su confianza y motivación para seguir carreras tecnológicas a medida que crecen, desde las unidades del ciberespacio de las Fuerzas de Defensa de Israel, a través de estudios académicos, hasta la misma industria de ciberseguridad.

Partners

Government | philanthropy

Operating body

Cyber Education Center

Otras actuaciones y/o programas

ISRAEL

Fulfillment Initiative

Un programa de excelencia para estudiantes de décimo y undécimo grado (un programa de tres años), que tiene como objetivo aumentar el número de admitidos desde la periferia geográfica y social a las unidades tecnológicas de élite en las Fuerzas de Defensa (Cuerpo de Inteligencia, TIC y Ciberseguridad , etc.). Como parte del programa, los participantes aprenden contenido tecnológico profesional de alto nivel, enfocándose en programación, comunicaciones y redes, sistemas operativos y más. Durante el tercer año, **los alumnos desarrollan un programa de proyecto final, bajo la guía de un mentor de la industria**.

StarTech

Un programa tecnológico único para estudiantes de la escuela media (grados 7-9), que opera en decenas de centros de estudio en la periferia geográfica y social. Los participantes del programa reciben herramientas prácticas en la programación de juegos de computadora y aplicaciones móviles, a través del aprendizaje utilizando el método PBL (*Project-Based Learning*). Junto con el contenido profesional, **el programa enfatiza el desarrollo personal**: investigación y desarrollo, un sentido de competencia y autoaprendizaje, junto con el trabajo en equipo y otras **habilidades blandas** que son vitales en el siglo XXI.

Mamriot (despegar en español)

Programa de excelencia educativa en cibernética y computación, cuyo objetivo es **brindar a las chicas de secundaria (10-12) una base de conocimientos profesional** y de calidad en estos campos; Darles la oportunidad de diferenciarse en posiciones tecnológicas significativas en las *Israeli Defense Forces (IDF)* y luego permitirles integrarse en la industria de tecnología y cibernética en el estado.

On Top

Es un plan de estudios que brinda una **línea pedagógica innovadora, matemática y programática** para estudiantes de octavo a noveno grado de un segundo círculo de excelencia. Los estudiantes fortalecen las habilidades matemáticas al resolver problemas de la vida de los clientes de nuevas maneras, y utilizando la programación como herramienta. **El programa proporciona a los maestros de secundaria una paquete completa de contenido** y acompañamiento durante todo el año.

En esencia, el objetivo de estas iniciativas es hacer que los niños se den cuenta de que la práctica hace la perfección y de que el aprendizaje es un proceso de práctica orientada a objetivos, que es la base para desarrollar capacidades y lograr un progreso significativo. Para desarrollar su potencial y alcanzar la excelencia los niños necesitan la oportunidad de practicar desde una edad temprana y el campo de la tecnología brinda esa oportunidad.

Otras actuaciones y/o programas

ISRAEL

Parque de alta tecnología Be'er-Sheva

El parque de alta tecnología Be'er-Sheva, inaugurado en septiembre de 2013, es el resultado de una iniciativa conjunta del municipio de Be'er-Sheva y la Universidad Ben-Gurion del Negev (+8.000 estudiantes de ingeniería). Está ubicado cerca de la Universidad Ben-Gurion del Neguev y del Centro Médico Soroka y adyacente a la estación de tren del norte de la ciudad. La División de TI de las Fuerzas de Defensa de Israel (IDF), que incluye unidades de tecnología de élite, también se despliega allí.

La planificación estratégica del área ha permitido un modelo de ecosistema único que conecta físicamente a las empresas que residen en el parque con la universidad, el hospital y la central de TI de las IDF, lo que lleva a una visible colaboración entre varios sectores y organismos.

Actualmente hay tres edificios que cubren alrededor de 50.000 metros cuadrados, y están ocupados por algunas de las principales empresas internacionales del sector tecnológico (unas 70 empresas y *start-ups* total), incluidas DELL, IBM, Oracle, WIX, Mellanox, Deutsche Telecom, Incubit, Allscripts, AudioCodes y más, que han centrado allí sus centros de investigación y desarrollo globales. Estas empresas emplean actualmente a más de 2500 ingenieros y profesionales de TI, y se espera que para la siguiente fase el parque tenga una superficie de 200.000 metros y emplee a unas 10.000 personas.

El ecosistema único y la sinergia entre la academia, la industria, el ejército, el Gobierno y una autoridad municipal que apoya esfuerzos han ayudado a impulsar iniciativas que están ayudando a dar forma al mañana. El parque Be'er-Sheva constituye un hito histórico y traerá cambios socioeconómicos y educativos que transformarán la ciudad de Be'er-Sheva y la región, de una ciudad metropolitana en un centro internacional de innovación, que está desarrollando pensadores creativos, lo que lleva a avances en todos los ámbitos.

Este parque es considerado una fuente primordial de experiencia y talento en ciberseguridad.

Análisis *benchmark*

Partners

ISRAEL

La red de *partners* de Israel a nivel internacional es robusta, al asociarse con instituciones académicas de todo el mundo y capacita a los estudiantes para que tengan éxito en la economía digital con un conjunto de programas de capacitación hechos prácticamente a medida.

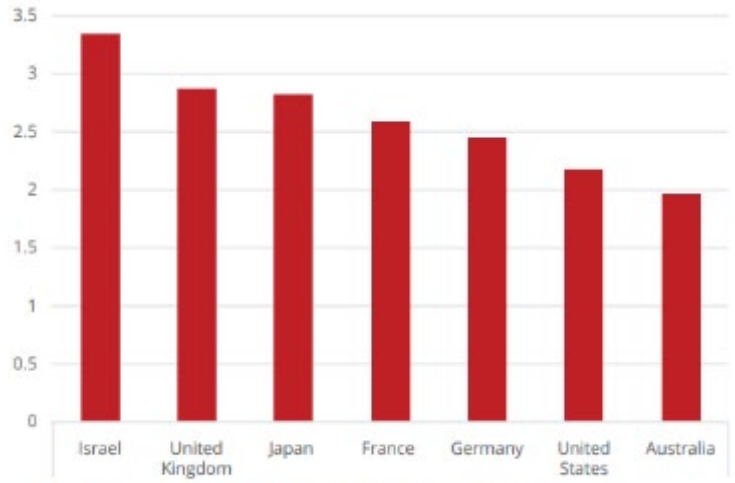
Inversión y cifras del mercado de ciberseguridad en Israel

ISRAEL

A pesar de que la economía de Israel enfrenta varias dificultades, ocupando el puesto 31 en términos de PIB per cápita a nivel mundial, **hay importantes inversiones en capacidades de ciberseguridad**. → La industria de la ciberseguridad en Israel está cercana a los **82 billones de dólares.**

- Israel **gasta del 6 al 8% de su PIB en defensa**, y también encabeza el mundo en términos de gasto interno bruto en I+D en relación con el PIB, gastando más del 4,5% de su PIB (OCDE). Este énfasis en la investigación y el desarrollo, así como el papel estimulante de las unidades técnicas de las IDF (por ejemplo, la Unidad 8200), proporcionan un entorno fértil para que las *start-ups* prosperen y haya un sector de alta tecnología.
- Además de esto, el primer ministro ha afirmado que **la ciberseguridad es un excelente negocio para la nación**. Se han desarrollado estrechas relaciones con países como Singapur, ayudándolos a establecer *start-ups* de ciberseguridad (300), exportando soluciones de TI por valor de 6.500 millones de dólares.

Prima salarial para profesionales en ciberseguridad



Cybersecurity salary premium (annual average salary from survey compared to OECD average annual wages).

- Según un informe publicado por Mcafee en 2020, Israel es el país que refleja una **mayor prima salarial en el mundo** (respecto a la media salarial anual en las profesiones de TI) para profesionales que se dedican a la ciberseguridad, como lo señala la figura.
- Se calcula que Israel ha llegado a representar (2016) el 20% de la inversión global en ciberseguridad, como lo afirmó en una conferencia en Tel Aviv el primer ministro Benjamin Netanyahu (2009-2021).
- El numero de compañías activas en Israel que tienen como actividad principal la ciberseguridad es mayor a 400 para el año 2019.

De los 394 billones de dólares que registra el PIB de Israel para 2019, bajo la premisa inicial de gasto en defensa del 6 al 8%, el presupuesto alcanzaría los 27.500 millones de dólares.
La proporción para ciberseguridad no se conoce con precisión, pero solo para el INCD el presupuesto a 2019 se ha duplicado con respecto a 2017, alcanzando los 64 millones de dólares.

Fuente: *Hacking the Skills Shortage Report*, Mcafee 2020.

Conclusiones

VARIABLE	ISR	DETALLE
Estrategia y estructura de ciberseguridad		El ecosistema único de Israel consiste fundamentalmente en un *framework* en constante evolución en el que colabora el Gobierno (incluidas agencias de defensa), las empresas y las universidades, y el Gobierno desempeña principalmente un papel de orientación y asesoramiento con una alta inversión de recursos económicos.
Israel Cyber National Directorate		Con el apoyo de las fuerzas militares este centro consolida capacidades estratégica y operativas que permiten una adecuada generación de políticas de ciberseguridad, así como gestionar la respuesta operativa a incidentes. El componente de participación internacional de este organismo es vital en el contexto internacional de seguridad.
Impacto en organizaciones (públicas y privadas)		Tanto a través de resoluciones como de iniciativas puntuales como la *Cyber Defense Doctrine*, se han desarrollado mejores prácticas en las organizaciones para gestionar incidentes, compartir inteligencia con *partners* esenciales y promover conciencia de seguridad.
Impacto en profesionales en ciberseguridad		Desde el INCD se han establecido resoluciones específicas para garantizar que tanto las organizaciones públicas como privadas cuenten con un nivel alto de ciberseguridad, a través de profesionales acreditados con un nivel específico de profesionalismo, confiabilidad y ética. La regulación del sector es clave para el profesionalismo.
Impacto en estudiantes		Israel genera cantera con iniciativas de formación desde temprana edad (secundaria) y tiene notables programas en esta dirección como lo es el caso del *Magshimim*. Además de esto, el servicio militar obligatorio les da una proyección a futuro para desempeñarse en cualquiera de las agencias de inteligencia de Israel.
Impacto en universidades		Israel está entre los países líderes en I+D académico en temas de ciberseguridad a nivel mundial y se encuentra según la OCDE, el 15º en innovación. La colaboración para investigación en materia TIC entre la academia y el sector industrial cuenta con el completo apoyo del primer ministro, quien además viene del sector tecnológico con gran *expertise*. Los programas de estudio, además, son un referente internacional e incluso fue la primera nación en tener un PhD en ciberseguridad.
Inclusión (mujeres y minorías)		A través de iniciativas como *Shift*, *Magshimim* o el mismo CEC, Israel refleja gran compromiso no solo con la diversidad de género, sino con la diversidad e inclusión. Su enfoque de incluir talento de las periferias es notablemente distintiva.
Inversión		Consistentemente Israel es reconocido por su nivel de compromiso mediante inversiones, alcanzando un gasto de casi el 8% de su PIB en seguridad. Abiertamente expone que en gran medida la inversión decidida ha sido la clave para obtener resultados.

No iniciada Incipiente En proceso Desarrollada Muy desarrollada

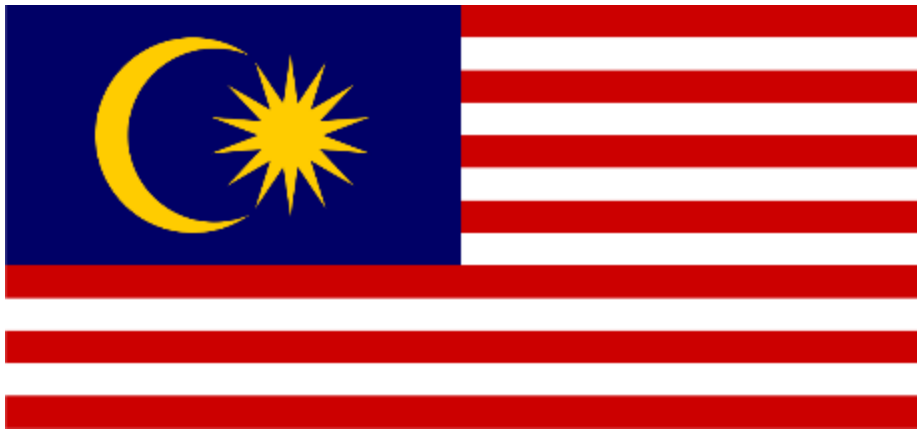
Conclusiones y recomendaciones

- *La posición que tiene Israel frente a la seguridad del ciberespacio es integral. No creen en los sistemas sino por el contrario en los "Frameworks" que abordan la materia como algo dinámico y que requiere de ajuste y adaptación constante para responder a la rápida evolución de TI y de esta manera tomar acción ante las amenazas.*
- *La industria de ciberseguridad de Israel está entorno a los $82 billones de dólares (exportan productos de cyber por valor de $6.500 millones) y de la forma en la que protegen la industria y su infraestructura crítica es teniendo a disposición el mejor talento cibernético. De hecho, el Primer Ministro ha afirmado que la ciberseguridad es un negocio excelente que crece de manera sostenida, al no haber soluciones definitivas ni permanentes. Adicionalmente, es uno de los países que más invierte en seguridad como porcentaje de su PIB (6% al 8%).*
- *La unificación de dos organismos que no satisfacían las necesidades de seguridad de los ciudadanos dio paso a la creación de la Dirección Cibernética Nacional de Israel, o en ingles, Israel National Cyber Directorate (INCD). Esta unificación permitió la gestión estratégica de políticas de seguridad junto con el despliegue de capacidades operativas bajo un solo organismo. El INCD es el organismo insignia en materia de ciberseguridad.*
- *Conscientes de la rapidez con la que evoluciona la tecnología, el ecosistema de Israel consiste fundamentalmente en un framework en constante evolución en el que colabora el gobierno (incluido el ejército), las empresas y las universidades, y el gobierno desempeña principalmente un papel de orientación y asesoramiento.*
- *Uno de los ejes centrales del INCD que permite el cumplimiento de los objetivos para los que fue creado, es establecer y promover las capacidades en ciberseguridad.*
- *La razón principal por la cual Israel es un país líder en el mundo de la ciberseguridad es porque sus empresas y el gobierno invierten masivamente en su capital humano.*
- *La resiliencia y la robustez de ciberseguridad son algo distintivo en Israel. Esto lo logran a través de implementar actuaciones como la Cyber Defense Doctrine, que no es nada distinto a asimilar procesos, métodos y productos de ciberdefensa a lo largo de toda la economía israelí.*

Conclusiones y recomendaciones

- *Israel cuenta con fuertes instituciones de apoyo como HackerU, que a través de la transferencia de conocimiento de calidad empodera la fuerza laboral para haya diversidad y calidad que responda a las necesidades actuales del mercado.*
- *La educación en ciberseguridad comienza en la escuela secundaria en Israel. Varias universidades israelíes ofrecen una especialización de pregrado en ciberseguridad e Israel fue el primer país en el que se pudo obtener un doctorado en ciberseguridad (como disciplina independiente, no como asignatura de informática). En la actualidad, existen seis centros de investigación universitarios dedicados a la ciberseguridad.*
- *El gobierno de Israel y sus diferentes organismos en materia de defensa y tecnología ostentan y permiten experiencia en ciberseguridad. El rol que juega el gobierno dentro del sector tecnológico es clave: facilitando parques tecnológicos (Be'er-Sheva) como impulso a la innovación donde se combina de manera única la parte teórica y práctica de la ciberseguridad con los intereses públicos y privados.*
- *Lo que vertebra los programas de educación y capacitación en ciberseguridad en Israel es el enfoque "hands-on" y profesores expertos que hacen parte de la industria. Esto no solo garantiza la calidad de la enseñanza sino un ajuste con las necesidades reales del mercado al generar profesionales que pueden aportar valor al corto tiempo de terminar los estudios.*
- *Israel es partidario de que capacitar a los empleados sobre cómo reconocer y responder (awareness) a las amenazas cibernéticas puede mejorar drásticamente la resiliencia cibernética de las organizaciones.*
- *Israel es un país que tiene claro la importancia de invertir para el mañana. En ese sentido, invierten considerables recursos y esfuerzos en el desarrollo de programas educativos no formales dirigidos a estudiantes en la periferia geográfica y social de Israel.*
- *Hay un foco notable en la diversidad tanto de genero como de otros colectivos. Israel pone en marcha iniciativas como el Magshimim que busca implantar la educación desde temprana edad (secundaria) para el desarrollo prospero de capacidades y competencias en ciberseguridad. Su metodología lúdica y contenidos personalizados son diferenciales y altamente valorados por los estudiantes.*

Malasia



Malasia

¿Qué orden seguiremos?

- Estrategia de ciberseguridad de Malasia.
- Organismos que participan y tienen competencias relacionadas con la ciberseguridad.
- Análisis *benchmark.*
- Conclusiones y recomendaciones.

Estrategia de ciberseguridad 2020-2024

Malasia

Dentro del contexto de adopción de las tecnologías de la información que naturalmente ha tenido que abordar Malasia, han optado por una estrategia de ciberseguridad que se basa en fortalecer localmente los "*capabilities*" necesarios para desplegar su misión y alcanzar su visión.

a penetración de internet en Malasia para el año 2018 alcanzó el 87.4%, lo que se traduce en 28.7 millones de usuarios. Esto supone la necesidad de fortalecer el ecosistema digital y la infraestructura crítica (CNNI) en servicio de la nación, considerando el incremento de ataques cibernéticos que ha pasado de generar perdidas en 2018 de €80.4 millones mediante 10.742 casos, hasta llegar en 2019 a €100.6 millones con 11.845 casos reportados oficialmente a la Policía Real de Malasia.

11 *Sectores que forman parte de la CNII.*

¿Cual es el principal organismo que gestiona la ciberseguridad en Malasia?

NACSA
AGENSI KESELAMATAN SIBER NEGARA
NATIONAL CYBER SECURITY AGENCY

CNII: *Critical National Information Infrastructure.*

Estrategia de ciberseguridad 2020-2024

Pilares e imperativos estratégicos

Malasia

- Desarrollar un plan integral para construir herramientas y tecnología adecuadas a través de un enfoque integrado

- Mejorar el enfoque de implementación del programa de concientización sobre ciberseguridad a través de la implementación del Plan Maestro Nacional de Concienciación sobre Ciberseguridad

- Desarrollar un plan nacional de desarrollo de capacidades de ciberseguridad.

- Iniciativas de desarrollo de talento a través de nuevos talentos, mejora y actualización de habilidades.

- Desarrollar la materia de ciberseguridad como uno de los planes de estudio de los niveles primario, secundario y terciario, en colaboración con el Ministerio de Educación.

- Se establecerán programas especializados para producir más talento local.

- Más cursos y especializaciones orientados a la industria y, por lo tanto, aumentar el número de estudiantes graduados universitarios preparados en campos de estudio relacionados con la ciberseguridad.

Los factores de éxito de esta estrategia son; gente (gestión del talento), procesos (gestión de políticas y procedimientos) y tecnología (habilitadores).

Organismos con competencias en talento de ciberseguridad

National Cyber Security Agency

Se estableció como una respuesta a la naturaleza dinámica, el aumento de la sofisticación, la naturaleza global y el aumento del impacto socioeconómico de las amenazas cibernéticas. Sirve como la agencia líder que integra las capacidades de ciberseguridad existentes.

National Cyber Coordination and Command Centre

Es un centro desarrollado para fines de gestión de crisis cibernéticas que incluye el monitoreo de amenazas en sistemas críticos del país. También tiene como objetivo garantizar la preparación, respuesta y mitigación de incidentes de ciberseguridad a nivel estratégico y táctico. Su rol varía dependiendo si el país se encuentra en tiempos de paz o no.

National Security Council

En esencia, el NSC es responsable de coordinar las políticas relacionadas con la seguridad nacional y la dirección de los asuntos de seguridad.

La comisión de comunicaciones y multimedia busca establecer una industria de comunicaciones y multimedia que sea competitiva, eficiente y cada vez más autorregulada, generando crecimiento para satisfacer las necesidades económicas y sociales de Malasia. Cuenta con una unidad que actúa como equipo de respuesta a incidentes para el sector de comunicaciones.

La Corporación de Economía Digital de Malasia, es la agencia líder para impulsar la economía digital en Malasia, encabezará los esfuerzos para aumentar el número de profesionales calificados locales, que incluirán iniciativas de desarrollo de talento a través de nuevos talentos, *up-skilling* y *re-skilling*.

GITN recibe el encargo del gobierno de convertir la visión de un gobierno electrónico en realidad. GITN es el proveedor de red oficial para el gobierno electrónico y tienen una amplia gama de infraestructura, hardware y software destinados a ayudar a mejorar e integrar las organizaciones en el gobierno electrónico.

Estrategia de ciberseguridad 2020-2024

Malasia

Para analizar el talento de ciberseguridad de Malasia, debemos comenzar analizando la agencia dedicada a la gestión de todo lo relacionado con la ciberseguridad.

La *Agencia Nacional de Ciberseguridad* (NACSA) se estableció oficialmente en febrero de 2017 como la agencia líder nacional en asuntos de ciberseguridad, con el objetivo de asegurar y fortalecer la resiliencia de Malasia para enfrentar las amenazas de ataques cibernéticos, coordinando y consolidando a los mejores expertos y recursos del país.

La NACSA también está comprometida con el desarrollo e implementación de políticas y estrategias de ciberseguridad a nivel nacional, protegiendo las infraestructuras crítica (CNII), adoptando medidas estratégicas para contrarrestar las amenazas cibernéticas, encabezando programas de sensibilización, culturización y creación de capacidades, formulando un enfoque estratégico para combatir las amenazas, asesorando en la gestión organizacional del riesgo cibernético, desarrollando y optimizando recursos compartidos entre agencias, y fomentando redes regionales y globales constructivas entre entidades con intereses compartidos en ciberseguridad.

Servicios

INDIVIDUALS

10 Medidas de ciberseguridad:

La agencia promueve una ciudadanía mejor informada como un paso esencial hacia la culturización en materia de ciberseguridad. Dentro de esta leve iniciativa buscan informar acerca de cómo protegerse de los ataques cibernéticos, abordando aspectos como las estafas, *phishing*, *ransomware*, y demás.

BUSINESS

Guías y mejores prácticas:

El objetivo es dotar de conocimiento a las empresas para que protejan su negocio y a sus clientes.
Se observa información sobre los controles de seguridad y las acreditaciones con base internacional que se pueden adoptar para aumentar la resiliencia de las organizaciones, y así proteger sus activos.

GOVERNMENT

Guías, boletines administrativos y certificaciones:

La agencia busca desarrollar una cultura de ciberseguridad en la administración pública. Desde aprender a manejar las nuevas tecnologías, hasta gestionar adecuadamente los riesgos y proteger las organizaciones en base a métodos y herramientas estandarizadas.

La agencia declara que estos esfuerzos generan resultados sólo a través de una coordinación estratégica en alianza con el sector privado y otros organismos públicos.

Capacidades, concienciación y educación

Malasia

Uno de los pilares de la agenda de Malasia para la gestión de la ciberseguridad es el desarrollo de capacidades, *awareness* y educación. Para esto, el Gobierno desarrollará e implementará un plan nacional de capacidades de ciberseguridad integral que determinará las áreas de experiencia y conjuntos de habilidades que deberán mejorarse continuamente a nivel nacional, sectorial y organizacional.

Objetivos

- Desarrollar un Plan Nacional de Desarrollo de capacidades en ciberseguridad
- Desarrollar un plan integral para construir herramientas y tecnología adecuadas a través de un enfoque integrado.

Estrategia

- Mejorar el enfoque de implementación del programa de concientización de ciberseguridad a través de la implementación del plan maestro nacional de concientización.

Objetivos

- Desarrollar la materia de ciberseguridad como uno de los planes de estudio de los niveles primario, secundario y terciario, en colaboración con el Ministerio de Educación.

El Plan se implementará mediante la construcción de una colaboración intersectorial coherente en el intercambio de información estratégica y las iniciativas de conciencia de seguridad, profundizando en la comprensión de las amenazas avanzadas, desarrollando una cultura que comprenda los riesgos de seguridad en el contexto de la resiliencia empresarial y ampliando la capacidad para desarrollar un entorno más seguro y resiliente.

Las organizaciones tanto públicas como privadas son coleccionistas de capacidades. Entre más capacidades tienen, más cosas pueden hacer. La clave está en desarrollarlas o adquirirlas.

Desarrollo de capacidades en los profesionales

Malasia

Malasia ha estado desarrollando e implementando capacidades a través de la colaboración de varios ministerios, agencias y organizaciones de la CNII. Uno de los vértices de este esfuerzo está en aumentar el número de profesionales calificados locales a través de programas de capacitación y certificación para satisfacer la demanda tanto en el sector público como en el privado. Malasia reconoce que en el país faltan certificaciones profesionales reconocidas y de buena calidad para el desarrollo de habilidades especializadas en ciberseguridad.

Malaysia Digital Economy Corporation

MDEC se estableció en 1996 para liderar el crecimiento de la economía digital. Es la piedra angular para el despliegue de iniciativas tendientes al desarrollo de una población con capacidades digitales. El foco lo ponen en acelerar el crecimiento de su economía digital, asegurándose de que sea inclusivo y gratificante para todos, enfocados en los impulsores clave: empoderar a los malasios con habilidades digitales, habilitar empresas impulsadas digitalmente e impulsar las inversiones del sector digital

La Corporación de Economía Digital de Malasia es la agencia líder para impulsar la economía digital en Malasia. Encabezará los esfuerzos para aumentar el número de profesionales calificados locales, que incluirán iniciativas de desarrollo de talento a través de nuevos talentos, *up-skilling* y *re-skilling*.

Análisis *benchmark*

Plataforma de empleo *MyDigitalWorkforce*

Malasia

Esta plataforma tiene como objetivo combinar las oportunidades profesionales en el mundo digital con los talentos potenciales. Ya sea un recién graduado, un talento experto o alguien que se encuentre transitando el camino hacia la vida laboral, esta plataforma ofrece una amplia gama de oportunidades de trabajo que se han consolidado con otras plataformas de reclutamiento asociadas.

Integración con otras plataformas de empleo

WOBB es una plataforma de búsqueda de empleo de Malasia fundada en 2014 por Derek Toh, ex director asociado de la firma de contratación Robert Walters, Malasia.

HAYS Recruiting experts worldwide

WOBB

Partner

Tanto Hays Malaysia como WOBB desarrollan esquemas de contratación con Malaysia Digital Economy Corporation para agilizar la contratación de talentos para la economía digital. Hays Malaysia apoya el esfuerzo de MDEC para garantizar que el talento adecuado se adapte a las carreras digitales al proporcionar atractivos paquetes de contratación a posibles empleadores. Esto ayudará a las empresas que necesiten talentos digitales al mejorar la eficiencia del proceso de "*matching*" de trabajo y talento.

Esta iniciativa no solamente reconoce la importancia de integrar diversos reclutadores en el proceso de posicionar a los talentos y profesionales al mercado laboral, sino que es consciente a su vez de las necesidades y limitaciones de las compañías.

Análisis *benchmark*

National cyber crisis exercise (X-Maya)

Malasia

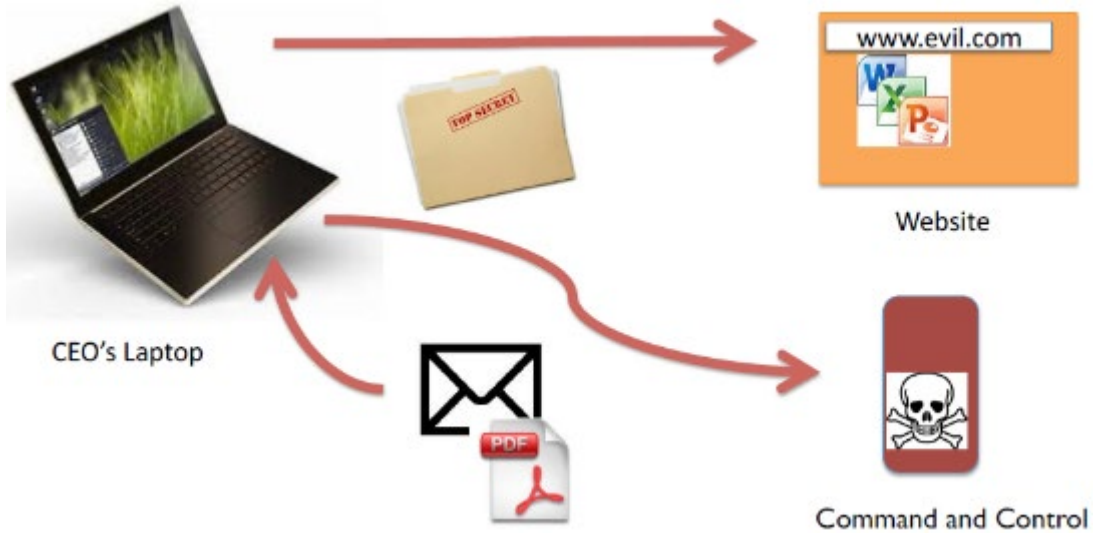
La iniciativa denominada Ejercicio Nacional de Crisis Cibernética (también conocida como X-Maya) fue diseñada para probar la efectividad de los procedimientos que se han desarrollado bajo el *Plan Nacional de Manejo de Crisis Cibernéticas* (NCCMP) y para evaluar la preparación de las agencias de infraestructura nacional críticas contra los ataques cibernéticos. Hasta la fecha, se han organizado seis (6) ejercicios nacionales de ciber crisis con la participación de más de 100 agencias públicas y privadas de las 10 *Critical National Information Infrastructure* (CNII).

Propósito de los ejercicios

- Lograr que las agencias se familiaricen con los procedimientos nacionales de gestión de crisis de ciberseguridad.
- Ejercitar la viabilidad, identificar las brechas y mejorar aún más el Procedimiento Nacional de Respuesta, Comunicación y Coordinación de Ciberseguridad
- Mejorar la preparación general de la ciberseguridad de las agencias que hacen parte de la infraestructura crítica.
- Fomentar el intercambio de información entre agencias.

Descripción de la Formación

- *Desktop exercise*
- *Hands-on / 'Blackbox'*
- *Progress Tracking*
- *Automation*
- *Infrastructure hosting - Cloud*



Malasia considera que poner a prueba las capacidades es uno de los pilares para que las organizaciones logran cambios significativos

Estos eventos cuentan con la participación de agencias tanto gubernamentales como privadas de la CNII (Infraestructura Crítica Nacional de Información) cuyos activos, sistemas y funciones son vitales para la nación y su incapacidad o destrucción tendría un impacto devastador en Malasia.

NCCMP: *National Cyber Crisis Management Plan*.

Análisis *benchmark*

El "*readiness*" como variable fundamental

Malasia

El Gobierno de Malasia aprovechará sus capacidades para desarrollar y aplicar medidas activas de ciberdefensa para mejorar los niveles de preparación de la ciberseguridad en las redes nacionales y gubernamentales. Se desarrollarán cursos, contenido y programas de ciberseguridad para los programas de formación gubernamentales y para grupos destinatarios específicos que se identificarán en función de sus funciones y responsabilidades. Todas las plataformas de formación existentes se utilizarán para establecer centros de formación principales que puedan atender a estos grupos objetivo y satisfacer adecuadamente sus necesidades y requisitos en cuanto a capacidades y esfuerzos de desarrollo de capacidades.

La apuesta por programas de formación en función de las responsabilidades de cada persona es una manera de alcanzar un mejor ajuste o "*fit*" entre lo que se busca aprender y el entorno en el que se desempeña el trabajador.

National Cyber security Awareness Master Plan

Malasia

Malasia también ha estado creando activamente programas de concienciación y creación de capacidades. Si bien la rapidez de las TIC aporta beneficios y ventajas a los ciudadanos, también conlleva riesgos para la economía, la armonía social y la seguridad de la nación. Para gestionar estos riesgos, el *awareness* público es fundamental. Las agencias han estado llevando a cabo varios programas de sensibilización para educar a los malasios. Como medio para coordinar estos programas, NACSA está desarrollando el plan maestro nacional de concienciación sobre ciberseguridad.

¿Cuál es el objetivo de este plan?

Aumentar el nivel de conciencia sobre la ciberseguridad entre los ciudadanos de Malasia a través de programas e iniciativas concertados y efectivos.

Se identifican 4 grupos objetivo principales

- Niños
- Jóvenes
- Adultos / padres
- Organizaciones

El Gobierno desarrollará e implementará el Plan Maestro Nacional de Concienciación sobre Ciberseguridad. En el marco del Plan, se establecerá la estructura de Gobernanza Nacional de Concienciación sobre ciberseguridad, que tiene como objetivo desarrollar un programa integrado y concertado de concienciación sobre el tema. El objetivo principal del programa integrado es reducir el número de incidentes cibernéticos mediante la ejecución de programas de concienciación y pedir acciones que estén más organizadas, coordinadas y capaces de llegar a un público objetivo más amplio entre los malasios.

Es *awareness* es considerado como uno de los primeros pasos que desencadenan el cambio cultural y de largo plazo.

Análisis *benchmark*

Catalizando I + D de clase mundial

Malasia

Este pilar tiene como objetivo catalizar la I+D+i a través de la construcción y el fortalecimiento del ecosistema de innovación en ciberseguridad. Es importante destacar que estas iniciativas contarán con el respaldo adicional del establecimiento de un centro de excelencia compartido. Se establecerán programas especializados para producir más talento local y contribuir a una comunidad de I + D sostenible y vibrante. También se fomentarán las colaboraciones entre universidades, instituciones educativas, industrias y *stakeholders* clave del Gobierno para ayudar a diseñar, crear e introducir más cursos y especializaciones orientados a la industria y, por lo tanto, aumentar el número de estudiantes graduados universitarios en campos de estudio relacionados con la ciberseguridad.

2 *Iniciativas Centrales*

MIMOS Berhad está posicionado para encabezar esta iniciativa, ya que ha sido muy activa y productiva impulsando la I + D en ciberseguridad, junto con socios de la academia, la industria y el Gobierno, durante más de dos décadas.

Las áreas clave de I+D incluyen:

- Tecnología de mejora de la privacidad
- Firma digital
- Identidad digital
- Autenticación de entidad
- Algoritmo de cifrado
- Seguridad física cibernética

¿Qué se espera obtener?

Estimular y fomentar la investigación interdisciplinaria y colaboración.

Estimular la creación de nuevas empresas locales de ciberseguridad a través del establecimiento de un centro de creación / ideación de ciberseguridad.

Promover el uso de productos y servicios de seguridad de las TIC locales y apoyar el crecimiento y la expansión de la industria.

Fortalecer los centros académicos de excelencia en las universidades a través de la colaboración con la academia, los institutos educativos y la industria.

Las tecnologías desarrolladas se han incorporado en varios sistemas para proporcionar una postura de mayor seguridad, por ejemplo, el *datawarehouse* sanitario de Malasia, el *gateway* de servicios en línea del Gobierno, el centro nacional de coordinación y comando cibernético y la identidad digital nacional.

Otras actuaciones y/o programas

Malasia

Como parte de su visión de impulsar la innovación en ciberseguridad en Malasia, han introducido una serie de iniciativas para ayudar a unir a grandes empresas a trabajar con *start-ups* y expertos de la industria para desarrollar nuevas tecnologías:

- Establecer programas de tutoría para compartir conocimientos de dominio, experiencia técnica y empresarial.
- Establecer una plataforma para que los proveedores de soluciones locales muestren sus soluciones, seguido de una prueba piloto de adopción de los desafíos (visibilidad).

Skill-Up Programme

A partir de 2018 a través de la colaboración con *Protection Group International* (PGI) del Reino Unido y la *Universidad de Tecnología e Innovación de Asia Pacífico* (APU), el programa hizo que los participantes se sometieran a un curso de 5 días que cubriera varios aspectos de ciberseguridad y asistieran a cursos certificados por el GCHQ del Reino Unido para aquellos que completaran con éxito el curso. En 2020, a los profesionales en ciberseguridad se les ofrece la oportunidad de mejorar sus habilidades en dominios como Cloud Security. De esta manera, MDEC podrá ayudar a retener el talento en la fuerza laboral de ciberseguridad, lo que es un paso importante hacia el desarrollo de talento sostenible en Malasia.

NxFORCE Programme

Dirigido a estudiantes de educación superior, el programa tiene como objetivo cerrar la brecha de talento en ciberseguridad que enfrenta la industria. Realizado en asociación con ISACA y el *Institute of Higher Education*, los estudiantes tienen acceso a una certificación reconocida a nivel mundial, un laboratorio práctico, una sesión para compartir con jugadores de la industria y una tutoría profesional y una pasantía / beca laboral. El programa comenzó en 2017 y, hasta la fecha, ha capacitado a un total de 640 estudiantes de educación superior para que estén preparados para desempeñarse en la industria.

CYBER100

Programa de Desafío de Innovación en Ciberseguridad. Esta iniciativa analiza la puesta en marcha y la ampliación innovadoras locales que pueden aportar soluciones a los principales desafíos nacionales de ciberseguridad. Está disponible para empresas constituidas en Malasia, con más del 50% de los accionistas malasios y la empresa debe proponer productos desarrollados localmente para resolver los desafíos. Los premios ascienden a 20.000 euros, y el propósito final es impulsar la innovación.

A través de la asociación con la industria, agencias gubernamentales e institutos de educación superior, se han lanzado varios programas de ciberseguridad que cubren el crecimiento de la industria, la innovación y el desarrollo del talento.

Potencial de la industria de la ciberseguridad en Malasia

Malasia

Malasia es uno de los países mejor calificados en materia de ciberseguridad del continente asiático. Estos son algunos de sus datos primordiales.

10.500

Demanda de talento en ciberseguridad para el año 2020.

Top 10%

De las oportunidades laborales en Malasia están relacionadas con la ciberseguridad.

21%

Es el porcentaje de mujeres en la industria de ciberseguridad.

539 M de euros

Valor estimado del mercado general de servicios de seguridad para 2021.

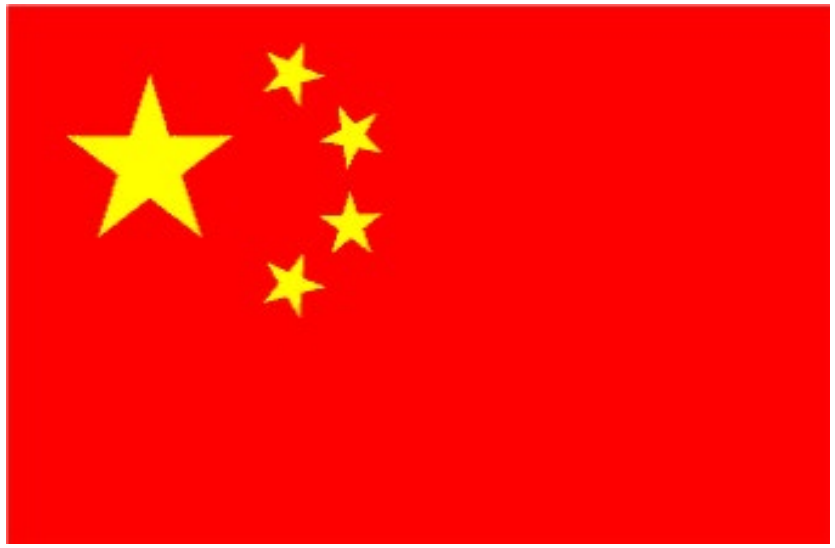
Fuente: *Malaysia Digital Economy Corp.* (MDEC)

Conclusiones y recomendaciones

Malasia

- *La estrategia de ciberseguridad de Malasia tiene como uno de sus pilares crear conciencia entre el público en general. Esto explica por qué le apuestan a introducir la educación en ciberseguridad incluso en la educación primaria. La concienciación y educación tiene como objetivo mitigar los riesgos a los que se exponen los ciudadanos y alcanzar cierto nivel de conocimiento para prevenir incidentes.*
- *Su puede afirmar que los retos predominantes en el panorama de la ciberseguridad de Malasia se pueden atribuir a la concienciación y la educación. Las soluciones tecnológicas en sí no pueden hacer mucho: son los propios actores del ecosistema los que necesitan tener un conocimiento básico de los elementos esenciales de la ciberseguridad y la regulación relacionada para que al menos puedan evitar los incidentes más comunes.*
- *A pesar de que se desconocen las cifras por la dificultad de cuantificarlas con precisión, Malasia es consciente de se enfrenta a una escasez en su fuerza laboral de ciberseguridad y brechas de talento en muchos sectores. En el mundo de hoy constantemente conectado y sin fronteras, tal insuficiencia puede ser desastrosa para las organizaciones. La escasez de profesionales deja a las organizaciones vulnerables y expuestas a peligros incalculables del ciberespacio.*
- *Una de las actuaciones en Malasia que consistentemente se refleja en la estrategia de ciberseguridad apunta a lograr un mayor número de graduados universitarios en campos relacionados con la ciberseguridad.*
- *En Malasia se reconoce la necesidad primaria de contar con certificaciones de calidad, las cuales no tienen actualmente, para el desarrollo de habilidades y capacidades especializadas en ciberseguridad.*
- *Tienen un enfoque interesante de cara a las plataformas de empleo impulsadas por MDEC, donde no solamente reconocen la importancia de integrar diversos reclutadores, sino que son conscientes a su vez de las necesidades y limitaciones de las compañías.*
- *Malasia busca fortalecer el ecosistema empresarial a través de iniciativas que permiten la colaboración entre grandes empresas y startups. Esto no solo permite compartir conocimiento sino que las nuevas empresas puedan dar a conocer su offering.*
- *Para hacerle frente al gap de talento y la problemática de fuga de talento, Malasia le apuesta a iniciativas relacionadas con el upskilling y certificaciones reconocidas, siempre bajo la figura de partnership con importantes organismos como ISACA*

China



China

¿Qué orden seguiremos?

- Estrategia de ciberseguridad de China.
- Análisis *benchmark*.
- Conclusiones y recomendaciones.

Estrategia de ciberseguridad

La *República Popular China* (PRC) viene siendo la potencia en ascenso del panorama internacional. Considerando su gran superficie y recursos naturales, estructura poblacional alta y eficiente, economía en desarrollo inclinada al uso de tecnología, poder de veto que posee el Consejo de Seguridad de las Naciones Unidas, capacidad militar y el aumento de la capacidad cibernética. La República Popular China ha estado planificando su estrategia de ciberseguridad con el propósito de permitir el crecimiento económico, desarrollar su capacidad militar, adquirir tecnologías emergentes dentro de las operaciones de espionaje cibernético y permitir la continuidad de sus sistemas. Estos son algunos de los hitos relevantes:

- El Ministerio de Tecnología de China anunció en Julio de 2021 un plan de acción de tres años para desarrollar la industria de ciberseguridad del país, que estima tendrá un valor de más de 32.300 millones de euros para 2023
- La nueva estrategia del Ministerio de Industria y Tecnología de la Información se está dando a conocer a medida que Pekín refuerza su control sobre el sector tecnológico del país, en medio de crecientes preocupaciones por la seguridad de los datos
- El entorno regulatorio es clave en China. Si bien es cierto en materia de avance tecnológico en la industria ciber se encuentran por detrás que EE.UU, el mecanismo regulatorio está mejorando gradualmente.

Integración e innovación de tecnologías emergentes

Foco Estratégico

- Se fortalecerán la investigación y **aplicación de tecnologías de seguridad de los datos** para optimizar la gestión de la privacidad y confianza.
- Se promoverá en todo el tejido productivo la **inversión en ciberseguridad**, gestionar presupuestos y promover el despliegue y la aplicación de productos y servicios de ciberseguridad. Se espera que la inversión en industrias críticas como el de las telecomunicaciones sea **mínimo del 10% de la inversión total en tecnología**.
- El industria de la ciberseguridad en China deberá estar en un nivel acorde para complementar la intensidad de la supervisión regulatoria.
- Con el fin de regular y proteger los datos, se han implantado medidas en la que las compañías que tengan más de 1 millón de usuarios, deberán someterse a una revisión regulatoria antes de realizar una oferta de acciones publica, o en ingles, IPO. Esto es una **medida para controlar los riesgos potenciales en relación con la seguridad nacional** debido a la gran cantidad de movimiento de datos transfronterizos.

China considera la gestión de datos como la piedra angular para las empresas y la economía, así mismo consideran que es el actual campo de batalla en la carrera tecnológica con EE.UU.

Estrategia de ciberseguridad

Cuando se considera el hecho de que 721 millones de los 3.400 millones de usuarios de Internet en el mundo se encuentran en la República Popular China, la importancia y el efecto en la industria de la ciberseguridad a escala global es indiscutible. El país cuenta con el personal más extenso de especialistas en ciberseguridad sobre el número de usuarios, y la magnitud de su comunidad en internet es tan grande, que la gestión de auditoría y control requiere de una infraestructura y estrategia robusta

En esencia, China ha venido trabajando desde hace décadas para diseñar su estrategia de ciberseguridad, principalmente con el objetivo de defensa y luego con el objetivo de ataque, especialmente dentro del alcance de las operaciones de ciberespionaje, en relación con la protección de su seguridad y estabilidad domésticas. En este contexto, se puede argumentar que la república popular China tiene objetivos principalmente económicos, políticos y militares en la estrategia de ciberseguridad

Estos objetivos se pueden enumerar de la siguiente manera:

Objetivos específicos:

- Adquirir tecnologías punteras que tengan una influencia significativa en el contexto de las operaciones de ciberespionaje para garantizar el crecimiento económico y la estabilidad.
- Controlar Internet para mantener la gobernanza del partido comunista de China (PCCh) en el país y así controlar los movimientos opositores locales, los focos separatistas y los posibles intentos de levantamiento social.
- Desarrollar medidas contra planes hostiles de guerra de la información basados en tecnologías de red y resistir las operaciones destinadas a intervenir en los asuntos internos del país.
- Establecer una importante estructura antiterrorista / espionaje contra las actividades de ciberespionaje planeadas contra el PCCh por los servicios de inteligencia extranjeros.
- Apoyar la capacidad militar dentro de las oportunidades posibles a través de tecnologías de punta en el campo del ciberespacio y, al mismo tiempo, construir planes contra infraestructuras críticas de potencias militares hostiles
- Organizar estrategias de guerra de información y actividades de ciberataques basadas en tecnologías de red contra las áreas y Gobiernos objetivo.

China no hace explicito la importancia y necesidad del desarrollo y promoción del talento para alcanzar los objetivos de su estrategia, sin embargo, se puede inferir que para la gestión de las tecnologías que esperan adquirir o desarrollar (innovación), es imprescindible el talento en ciberseguridad

Análisis *benchmark*

Curso de capacitación administrativa de aplicación de la ley de la Administración Nacional del ciberespacio – Edición # 13

Con el fin de fortalecer la construcción de equipos de aplicación de la ley y mejorar el nivel de las capacidades de los negocios, en Julio de 2021, la Administración Nacional del ciberespacio de China celebró el 13 ° curso de capacitación en aplicación de la ley de la Administración Nacional del ciberespacio en la ciudad de Wuxi, provincia de Jiangsu.

Mejora de capacidades

Esta capacitación se centró en el estudio y la implementación de los pensamientos de Xi Jinping sobre el estado de derecho y sobre el poder de la red, siguiendo de cerca la situación y las tareas de administrar la red de acuerdo con la ley

Objetivos:

(i) Promover de manera integral el trabajo del estado de derecho en internet a un nuevo nivel.

(ii) Lanzar cursos como: 'La construcción del sistema legal de redes de mi país' e 'Interpretación del trabajo policial en red'. Estos abarcan el estudio teórico, la interpretación jurídica, la práctica policial y otros enlaces.

¿Cuál es el propósito?

El propósito, es profundizar en el aprendizaje y la comprensión de las importantes exposiciones del Secretario General Xi Jinping sobre el estado de derecho en internet, para mejorar aún más la comprensión, la posición política, el entendimiento de los procesos de aplicación de la ley y unificar el pensamiento

Alcance

Cerca de 120 aprendices de varias provincias, regiones autónomas, municipios directamente dependientes del Gobierno central y la administración del ciberespacio del Cuerpo de producción y construcción de Xinjiang participaron en la capacitación.

Construyendo escuelas para los próximos 10 años

A pesar de las controversiales definiciones que tiene el presidente de China acerca de ser una superpotencia en materia de ciberseguridad, Xi Jinping parece estar avanzando en la consecución de este objetivo

El principal regulador de internet de China, la administración del ciberespacio de China, y el Ministerio de Educación de China anunciaron que China planea construir de cuatro a seis escuelas de ciberseguridad de clase mundial en diez años. Esto sería entre 2017 y 2027.

Además, las universidades que se ofrezcan a hacer parte de esta iniciativa recibirían todo el apoyo del gobierno chino, en cuanto a recursos financieros y otros recursos.

Objetivos

- Establecer programas interdisciplinarios que involucren ingeniería, derecho, gerencia y otras categorías para capacitar al personal de ciberseguridad.
- Establecer laboratorios de primer nivel con empresas y unidades de investigación científica y realizar las tareas de investigación que encomiende el Estado.
- Coordinar que profesores especializados trabajen en empresas relacionadas con la industria unidades de investigación científica y departamentos gubernamentales, a fin de fortalecer la cooperación entre la escuela y la empresa.
- Contratar personal experimentado, incluidos expertos en gestión de ciberseguridad y talentos especializados, como profesores a tiempo parcial.
- Evaluar los talentos de ciberseguridad con habilidades prácticas en lugar de calificaciones académicas o títulos.
- Emprender proyectos de investigación emitidos por la Administración del ciberespacio o el Ministerio de Educación.

Análisis *benchmark*

Concurso nacional de habilidades y conocimientos de plataforma de sitios web

Llevada a cabo en Beijing en la sede creativa universitaria de la televisión educativa de China, esta prueba fue organizada por la Administración central del ciberespacio de China, la administración integral de redes, la oficina de supervisión de la aplicación de la ley de la Administración central del ciberespacio, la Fundación para el desarrollo de internet de China, y coorganizada por la televisión de educación de China.

Descripción del concurso

- El propósito de esta competencia es promover el aprendizaje mediante la competencia, promover el uso práctico mediante el aprendizaje, implementar seriamente el espíritu de importantes discursos del secretario general Jinping. De hecho, el espíritu del XIX Congreso Nacional del Partido Comunista de China, reunió a cientos de millones de internautas para promover conjuntamente la construcción de un poder de red y trabajar juntos para construir un mejor hogar en línea.

- El tema de este concurso es "Por una mejor red doméstica". Se divide en tres etapas: ensayos, semifinales y finales. También hay rondas nacionales.

- Participan 15 sitios web de noticias, entre ellos: People's Daily online, Xinhuanet, China Net, International Online, China Daily, entre otros.

También asistieron Wei Zhengxin, secretario general de la Fundación para el desarrollo de internet de China, Qiu Guodong, inspector y subdirector de la Administración central del ciberespacio de China, Xu Heng, subdirector de la Administración central del ciberespacio de China.

Qiu Guodong, inspector y subdirector de la Oficina de coordinación de la Administración central del ciberespacio de China, pronunció un discurso en el evento.

Análisis *benchmark*

Digital China construction and development → Digital China Summit

El plan digital *China Construction and Development* ha sido presentado en la cumbre de China digital. Se ha realizado en los últimos años, en 4 ediciones.

1

La cumbre se ha convertido en una plataforma importante de comunicación e implementación de proyectos digitales con impactos en todo el aparato económico de China

La cumbre se celebra en la ciudad de Fuzhou, capital de la provincia de Fujian, y es un escenario donde se presentan avances tecnológicos, se tratan temas de gobernanza digital, se presentan proyectos de transformación digital e innovación y en general se tratan los temas de economía digital.

Algunos datos de este evento:

(i) Asisten en promedio 300 empresas de diferentes tamaños.

(ii) En la reciente edición de 2021 se han presentado más de 400 proyectos, con una inversión total de 47.200 millones de euros. Se firmaron 29 proyectos.

El plan muestra en cuanto a los indicadores de desarrollo, incluido el número de patentes de invención de tecnología de la información nacionales concedidas, la relación entre usuarios de fibra óptica y usuarios de banda ancha, la tasa de penetración de los hogares de banda ancha fija y la tasa de cobertura de las redes de banda ancha en las aldeas pobres se han completado antes de lo previsto.

Desde la perspectiva de la implementación de tareas clave, la construcción y el desarrollo de China digital ha logrado avances sólidos en 10 tareas principales y 16 proyectos clave. Las capacidades de innovación independientes de las tecnologías centrales se han mejorado significativamente, la infraestructura de la información se ha mejorado de manera integral, el desarrollo y la aplicación de big data se ha acelerado, la economía digital ha florecido y los asuntos gubernamentales digitales se han intensificado. La información beneficia a las personas y se han acelerado los servicios más convenientes. Se han tomado medidas sólidas en el desarrollo de una integración profunda de la ciberseguridad y el desarrollo militar-civil, se han logrado resultados fructíferos en la cooperación internacional en la economía digital, se ha mejorado significativamente la gobernanza integral del ciberespacio y, el sistema de garantía de ciberseguridad se ha consolidado.

Análisis *benchmark*

With a passion for a child and a will to strive

En vísperas del 99 aniversario de la fundación del partido, los departamentos locales de ciberseguridad e informatización integraron plenamente las características del trabajo local, y llevaron a cabo clases temáticas del partido, realizaron actividades culturales y se organizaron para revisar la historia del partido a través de una serie de actividades temáticas vívidas y animadas. Este ejercicio de aprendizaje promueve el pensamiento y la comprensión del partido así como promueve el desarrollo de alta calidad de ciberseguridad e informatización.

Shanxi Cyberspace Administration

En esta iniciativa se busca que los equipos de ciberseguridad realicen visitas a sitios emblemáticos de alto valor cultural. Con esta iniciativa se busca inspirara a la fuerza laboral en base al pensamiento del general Xi Jinping. Algunas de las actividades que realizan para fortalecer el espíritu de los trabajados es ver documentales o largometrajes con mensajes e imágenes históricas que logren expresar el amor por la patria.

Posterior a estas visitas, lo equipos expresan que deben seguir inquebrantablemente el camino guiado por estas enseñanzas y estudiar más a fondo el discurso del general Xi Jinping, ceñirse a la inspiración, asumir la misión y esforzarse para ser prácticos.

Esto supone que los equipos de ciberseguridad que participan en estas actividades van a contribuir a una ciberseguridad responsable, integral y competente que fomenta una mejor sociedad impulsada por la informatización.

Análisis *benchmark*

National cybersecurity center in Wuhan

Este ambicioso proyecto consiste en un campus de 15 millas cuadradas en la ciudad de Wuhan, que servirá como escuela, laboratorio de investigación, incubadora de proyectos y cultivador de innovación y talentos.

NCC

7 *centros de investigación, desarrollo de talento y emprendimiento.*

2 *laboratorios centrados en el gobierno.*

1 *escuela Nacional de Ciberseguridad.*

1.300 *estudiantes graduados a 2022.*

2.500 *graduados por año a partir de 2023.*

6.000 *profesionales recibiendo cursos y certificaciones por mes.*

Medio millón de formados en la próxima década.

BRECHA DE TALENTO

Retos a los que hace frente el NCC

- Escasez de talento en ciberseguridad por parte de sus fuerzas militares. El déficit se estima en 1,4 millones de profesionales y este será uno de los componentes del NCC, ayudar a abordar esa escasez mediante el cultivo de talento.
- Dependencia de tecnología extranjera (facilita el espionaje).
- A nivel militar, los estrategas chinos argumentan que interrumpir las comunicaciones o sistemas específicos es clave para disuadir un ataque militar. Ante esto, reconocen que ninguna herramienta por sí sola les otorga una ventaja pero, una fuerza laboral capaz de realizar innovaciones significativas es fundamental para implementar estrategias ganadoras.

Ventajas

- Tres de los componentes del NCC apoyan directamente la innovación. Además otros dos se enfocan únicamente en la parte de gobierno.
- Los estudiantes y las startups pueden solicitar orientación empresarial y fondos de inversión en la incubadora de NCC.
- El centro realiza eventos que atraen talentos de todo el país, algunos de ellos podrían ser una capacidad o ventaja para el ejército popular de liberación (estilo cantera).

Nota: Los dos laboratorios mencionados son: *Combined Cybersecurity Research Institute* y *Offense-Defense Lad*.

Análisis *benchmark*

ZTE cybersecurity lab

Siguiendo el principio de apertura y transparencia y cumpliendo su compromiso con la seguridad de la industria de las TIC contra las amenazas de ciberseguridad, a través de las iniciativas ZTE, se ha establecido un laboratorio de ciberseguridad en Nanjing. Este sirve como una plataforma que permite a los *stakeholders* de la industria y puntualmente a los reguladores, realizar evaluaciones de seguridad independientes de los productos, servicios y procesos. Asimismo, provee una plataforma para la colaboración y la comunicación.

- El laboratorio ubicado en Nanjing es el laboratorio de ciberseguridad más grande y completo de ZTE. Proporciona el entorno de red integral 4G/5G y la infraestructura de evaluación para admitir múltiples funciones de evaluación de seguridad, incluida la revisión del código fuente, la revisión de documentos, las pruebas de penetración, entre otras.
- El laboratorio también es un lugar propicio para facilitar el desarrollo de capacidades, investigaciones en profundidad y exploraciones en el campo de la ciberseguridad.

Proyectos Evaluados

Como parte principal de la evaluación de seguridad independiente, el laboratorio de Nanjing prueba los proyectos clave en todos los niveles y otros proyectos mediante controles al azar en formas de pruebas de penetración y pruebas de conformidad de seguridad. Los proyectos de evaluación a 2020 están en la categoría de *penetration testing* y *security conformance testing*.

Wireless

Cloud

Server & Storage

Transport Network

Multi-Media

Energy

Despliegue de Soluciones de red y otras soluciones

Foco en Industrias

Compañías chinas como ZTE, con activos por más de 13.500 millones de euros que ponen a disposición sus soluciones a las empresas y ciudadanos es un reflejo de la robustez y magnitud del sector TIC en general.

Conclusiones y recomendaciones

- *La estrategia de ciberseguridad de China gira alrededor de permitir el crecimiento económico, desarrollar su capacidad militar, adquirir tecnologías emergentes dentro de las operaciones de espionaje cibernético y permitir la continuidad de sus sistemas.*
- *China no hace explícito la importancia y necesidad del desarrollo y promoción del talento para alcanzar los objetivos de su estrategia, sin embargo, se puede inferir que para la gestión de las tecnologías que esperan adquirir o desarrollar (innovación), es imprescindible el talento en ciberseguridad.*
- *China es consciente de su dependencia actual en ciertas tecnologías extranjeras, lo cual pone en riesgo su infraestructura militar y crítica. Ante esto, le apuestan firmemente a establecer políticas que fomenten la innovación y la generación de talento en ciberseguridad.*
- *Los laboratorios de ciberseguridad y las diferentes pruebas que allí se realizan tiene como objetivo mejorar la seguridad de la industria de las TIC. La verificación y la comunicación de productos de seguridad es un factor determinante para la evolución de la industria.*
- *China realiza eventos en diferentes provincias que reúne a los actores más importantes del ecosistema digital. Esto es un terreno adecuada para el desarrollo e implementación de políticas y proyectos que tienen impacto en todo el aparato económico de China.*
- *En China el sentido de pertenencia y patriotismo es fundamental. El desarrollo de programas de motivación para el mejor desempeño de los equipos de ciberseguridad se basan en las enseñanzas y discursos de general Xi Jinping. Según esto, el desempeño de los equipos es más integro y responsable.*
- *China tiene una apuesta decidida de consolidar escuelas de ciberseguridad de talla mundial. Pero su enfoque es lo más llamativo, porque reconocen la importancia de vincular tanto a profesores a trabajar en conjunto con empresas de la industria, así como también incentivan la contratación de personal especializado de las empresas para que sean profesores de tiempo parcial. Esta relación entre academia y empresa es la piedra angular para un cambio de estructura en la formación.*
- *China entiende la necesidad de vincular talentos con capacidades prácticas más allá de los títulos formativos. Esto les puede dar una ventaja en cuando al número de personas que aportan valor a la industria.*

Canadá

Canadá

¿Qué orden seguiremos?

- Estrategia de ciberseguridad de Canadá.
- Análisis *benchmark*.
- Conclusiones y recomendaciones.

Estrategia de ciberseguridad

Desde las cadenas de suministro hasta la infraestructura crítica que sustenta la economía y la sociedad, los riesgos en el mundo cibernético se han multiplicado, acelerado y se han vuelto cada vez más maliciosos. Las principales corporaciones, industrias y partners internacionales están comprometidos con el desafío cibernético global. Si bien es importante estar muy consciente de las amenazas de ciberseguridad, la política de Canadá no está impulsada por el miedo y la actitud defensiva. Con esto en mente, la estrategia de ciberseguridad existente se ha llevado a cabo con énfasis en el enorme potencial de liderazgo de Canadá en este campo.

>43 horas conectados a internet al mes por cada canadiense. Esto refleja la dependencia y el alto nivel de conectividad del país.

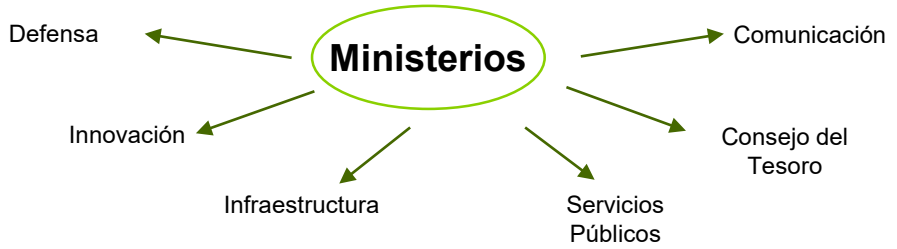
El despliegue de esta estrategia es el mayor esfuerzo económico en ciberseguridad que ha realizado Canadá y refleja un alto compromiso con la industria.

Canadá se encuentra muy interconectado, lo cual supone una adecuada infraestructura y un nivel de servicios al ciudadano de buena calidad. Pero también crea vulnerabilidades. La implementación de las actuaciones contenidas en la estrategia busca mitigar esas vulnerabilidades.

Objetivos centrales de la estrategia

- Financiación para el nuevo centro canadiense de ciberseguridad para respaldar el liderazgo y la colaboración entre diferentes niveles de Gobierno y socios internacionales, proporcionando un recurso claro y confiable para los ciudadanos y empresas canadienses.
- La creación de la Unidad Nacional de coordinación de delitos cibernéticos para ampliar la capacidad de la *Royal Canadian Mounted Police* (RCMP) para investigar el delito cibernético, estableciendo un centro de coordinación para socios nacionales e internacionales.
- Financiación para fomentar la innovación y el crecimiento económico, y el desarrollo del talento en ciberseguridad canadiense.

Stakeholders involucrados en la estrategia



Esta estrategia refleja inversiones en su ejecución desde 2018 por más de 425 millones de euros y busca satisfacer mejor las necesidades de ciberseguridad de los canadienses, permitiéndoles beneficiarse de las oportunidades que ofrece la tecnología digital.

Análisis *benchmark*

GAP de la fuerza laboral en ciberseguridad

Canadá considera que para abordar al gap de habilidades de ciberseguridad en la fuerza laboral es necesario trabajar juntos entre los gobiernos, la academia y el sector privado. Tomar medidas ahora permitirá construir la fuerza laboral del futuro, una que ayudará a respaldar la ciberseguridad canadiense y que contribuirá a la prosperidad futura de Canadá.

- Uno de los objetivos del plan de acción en ciberseguridad 2019-2024, es lograr consolidar un ecosistema de ciberseguridad con la capacidad de adaptación e innovación.

En consecuencia, Canadá invertirá en iniciativas que apoyen el desarrollo de habilidades digitales para abordar la brecha de habilidades cibernéticas, con el objetivo de construir la fuerza laboral para el futuro.

Goal

An Innovative and Adaptive Cyber Ecosystem

Canadá declara en que un ecosistema robusto es la manera más idónea de desarrollar capacidades para el largo plazo.

Actuaciones específicas como el Cybersecurity Talent Alliance están destinadas a reforzar el ecosistema de ciberseguridad en Canadá y conjuntamente abordar el gap de talento en ciberseguridad.

Fuente: *(ISC)2 Cybersecurity Workforce Study*, 2020; *Initial National Cyber Security Skills Strategy*, 2018.

Cyber centre learning Hub

Learning Hub (LH) es una fuente confiable de actividades y programas de aprendizaje innovadores para profesionales de ciberseguridad que trabajan dentro del Gobierno de Canadá. El Hub también brinda servicios, orientación y asesoramiento sobre capacitación y educación en ciberseguridad a la industria, la academia y otros niveles de Gobierno.

Conjuntamente también lleva a cabo actividades de participación y divulgación académica trabajando con universidades, colegios, asociaciones educativas, juntas ministeriales de educación y educadores del sector privado para desarrollar el talento y las capacidades en Canadá.

MULTIPLES CURSOS

Université de Montréal Collaboration

The Learning Hub colaboró recientemente con *Smart Cybersecurity Network*, la red de ciberseguridad inteligente patrocinada por la Université de Montréal, para ayudar a crear su nuevo Curso Masivo Abierto en línea (MOOC) llamado “La cybersécurité en milieu universitaire”. El objetivo de este curso es aumentar la conciencia de la seguridad cibernética dentro de la comunidad académica.

Cyber Security for Educators

Enfocado a profesores de escuela de 4º a 12º grado, este curso proporcionará a los educadores de todo Canadá un conocimiento básico de los conceptos de ciberseguridad, como terminología cibernética, medidas de protección cibernética, seguridad cibernética en el aula y carreras en ciberseguridad. Este curso fue diseñado para ayudar a los educadores a transferir esta nueva información a sus estudiantes. El resultado esperado de esta capacitación será que los maestros de escuela y sus estudiantes implementen prácticas de ciberseguridad más seguras.

Academic Outreach and Engagement

Este equipo trabaja con universidades, colegios, asociaciones educativas, juntas ministeriales de educación y educadores del sector privado para desarrollar el talento y la capacidad de ciberseguridad en Canadá. La misión es garantizar que Canadá sea un líder mundial mediante la mejora de la educación cibernética.

Análisis *benchmark*

Cyber security component of the student work placement program

Liderada por el *Departamento de Empleo y Desarrollo Social de Canadá* (ESDC), esta iniciativa se utilizará para proporcionar recursos a un componente del programa de colocación Laboral para Estudiantes (*Student Work Placement*) para apoyar la creación de hasta 1.000 nuevas oportunidades de aprendizaje integrado en el trabajo (WIL) a lo largo de tres años en ciberseguridad.

El programa SWP actualmente apoya la creación de oportunidades WIL para que los estudiantes canadienses alineen las habilidades de los graduados con las necesidades de contratación de los empleadores en industrias en crecimiento. Los participantes elegibles deben estar inscritos en programas STEM y negocios en instituciones de educación postsecundaria en todo Canadá. Las oportunidades de WIL brindan a los estudiantes valiosas oportunidades de desarrollo de habilidades para facilitar una transición más fluida de la escuela al trabajo después de la graduación, y ayudan a los empleadores a construir una línea de talentos para sus futuras necesidades de contratación.

- El programa *SWP* ofrece a los empleadores subvenciones salariales del 50% por cada nuevo puesto de trabajo estándar que creen (hasta un máximo de 5.000 dólares por puesto).
- La subvención salarial es mayor, 70% (hasta un máximo de 7.000 dólares), para nuevas colocaciones creadas para estudiantes subrepresentados, incluidas mujeres en STEM, pueblos indígenas, personas con discapacidad y recién llegados; así como estudiantes de primer año.

Oferta **FIT** **Demanda**

Trabajar en formas innovadoras de alinear el desarrollo de habilidades educativas con los requisitos de habilidades de los empleadores en sectores clave y emergentes de la economía canadiense es una de las iniciativas de mayor impacto en el avance de la industria.

Cyber security assessment and certification for SMEs

Las pequeñas y medianas empresas (pymes) en Canadá, al igual que en muchos otros países, no tienen las mismas capacidades que las grandes empresas en lo que respecta a ciberseguridad. En este sentido se piensa que la introducción de una certificación voluntaria para ciertas empresas les ayudará a posicionar su ventaja competitiva y promoverá la confianza en la economía digital. El programa de Certificación Cibernética está dirigido a las pymes, que representan aproximadamente el 98% del número total de empresas en Canadá.

Si bien, existe una pequeña cantidad de estándares para la seguridad cibernética. El programa de certificación cibernética, requiere la implementación de controles de seguridad cibernética específicos por parte de participantes certificados por un organismo de certificación acreditado por un tercero para garantizar una aplicación consistente de protecciones de seguridad cibernética para demostrar una seguridad básica proporcionada por empresas. Este programa está diseñado para ser un punto de partida para que las pymes mejoren su postura de ciberseguridad. El propósito último del programa de certificación cibernética, es elevar la postura de seguridad cibernética entre las pymes canadienses, aumentar la confianza del consumidor en la economía digital, promover la estandarización internacional y posicionar mejor a las pymes para competir globalmente. Esta iniciativa público-privada, está dirigida por innovación, *Ciencia y Desarrollo Económico de Canadá* (ISED), en colaboración con el *Establecimiento de Seguridad de las Comunicaciones* (CSE), el *Consejo de Normas de Canadá* (SCC) y organismos de certificación independientes acreditados por el sector privado.

“La innovación digital se ha convertido en el motor del crecimiento económico del siglo XXI. La ciberseguridad no solo es esencial para proteger las fuentes de la innovación digital de Canadá, sino que se ha convertido en una fuente de innovación por derecho propio”

Análisis *benchmark*

Cyber security learning outcomes

Technation es la principal asociación nacional de la industria tecnológica de Canadá y junto con la *Cybersecurity Talent Alliance* (CTA) han publicado *"Cybersecurity Learning Outcomes"*.

Esta publicación se diseñó para garantizar que los candidatos que buscan empleo en un equipo de ciberseguridad organizacional hayan demostrado competencia en los fundamentos de la ciberseguridad y el dominio de trabajo general antes de buscar la especialización.

MISIÓN

La misión es acelerar el desarrollo de habilidades, orientar el desarrollo profesional y la planificación de la fuerza laboral apoyando a las instituciones educativas postsecundarias y a los empleadores, para abordar la creciente escasez de habilidades en ciberseguridad en el mercado laboral canadiense.

Este proyecto está financiado en parte por el programa de iniciativas sectoriales del Gobierno de Canadá.

FOCO ESTRATÉGICO

Desarrollados por un grupo diverso de profesionales de la educación y la industria, la iniciativa está destinada a:

- Ayudar a los educadores en el desarrollo de criterios de capacitación y educación para satisfacer las cambiantes necesidades de la fuerza laboral en ciberseguridad.
- Proporcionar un puente importante entre el *entry level* y el trabajo especializado que normalmente no ha estado disponible en los programas de educación postsecundaria hasta la fecha.
- Apoyar específicamente los requerimientos que tienen los recién egresados con competencias de ciberseguridad para que ingresen al mundo laboral.

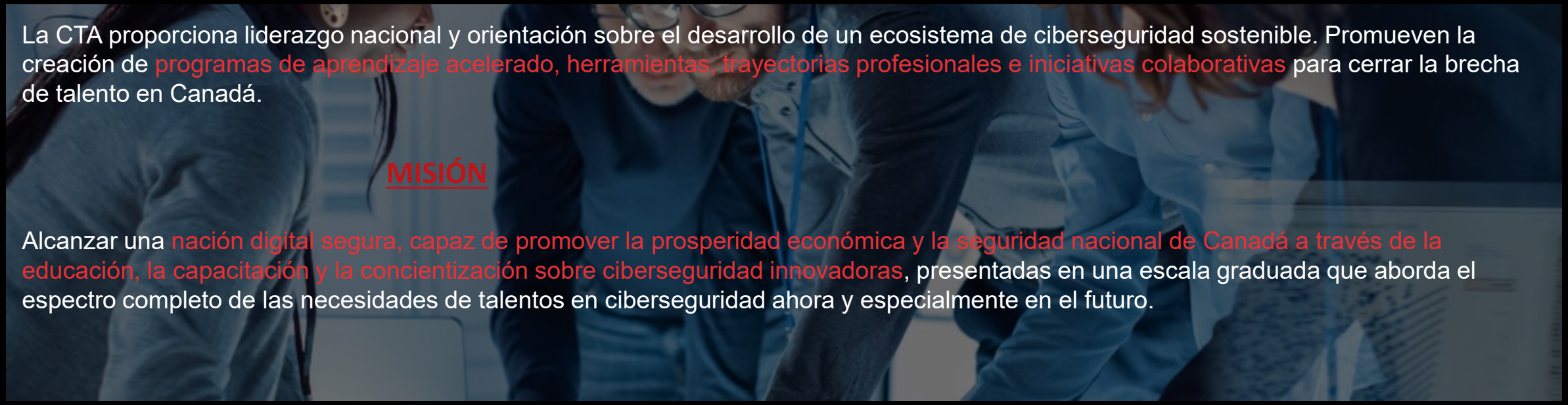
BENEFICIOS CLAVE

- Los educadores tendrán un conjunto definido de "*Learning* Outcomes" para ayudar a brindar estándares comunes en sus programas de educación en ciberseguridad en todo Canadá.
- Los empleadores que reconocen los desafíos de la brecha de habilidades actuales en ciberseguridad, tendrán la confianza de que los futuros empleados comenzarán a trabajar y comenzarán a satisfacer las necesidades de ciberseguridad de su organización.

Los graduados podrán encontrar rápidamente oportunidades de trabajo al estar capacitados con habilidades que los empleadores realmente necesitan. La especialización en ciberseguridad de los estudiantes les permitirá posicionarse en cualquier industria o sector.

Análisis *benchmark*

Cyber security talent alliance



La CTA proporciona liderazgo nacional y orientación sobre el desarrollo de un ecosistema de ciberseguridad sostenible. Promueven la creación de programas de aprendizaje acelerado, herramientas, trayectorias profesionales e iniciativas colaborativas para cerrar la brecha de talento en Canadá.

MISIÓN

Alcanzar una nación digital segura, capaz de promover la prosperidad económica y la seguridad nacional de Canadá a través de la educación, la capacitación y la concientización sobre ciberseguridad innovadoras, presentadas en una escala graduada que aborda el espectro completo de las necesidades de talentos en ciberseguridad ahora y especialmente en el futuro.

Objetivos

- Estimular el desarrollo de estrategias, enfoques y técnicas para aumentar más rápidamente la oferta de trabajadores calificados en ciberseguridad.
- Fomentar una comunidad de aprendizaje diversa a través de esfuerzos creativos que aumenten la presencia de grupos subrepresentadas en la fuerza laboral de ciberseguridad.
- Incrementar el *awareness* de la carrera de ciberseguridad, estimular la exploración y habilitar la preparación con los estudiantes en K-12 (todos los niveles).
- Brindar apoyo a las organizaciones para abordar las demandas del mercado proporcionando herramientas y técnicas que mejoran el reclutamiento, las prácticas de contratación, el desarrollo y la retención de talento.
- Facilitar la investigación y la previsión para identificar y analizar fuentes de datos que respalden la proyección de la demanda y oferta presentes y futuras de trabajadores calificados en ciberseguridad.

Capacidad de aplicación de la ley federal contra el delito cibernético

Goal

Secure and Resilient Systems

Objetivos Unidad NC3

(i) Coordinar las operaciones canadienses contra el ciberdelito y colaborar con socios internacionales.
(ii) Brindar asesoramiento y orientación sobre investigación digital a la policía canadiense.
(iii) Producir inteligencia procesable sobre delitos cibernéticos para la policía canadiense.
(iv) Establecer un mecanismo nacional de denuncia pública para que los canadienses y las empresas denuncien los delitos cibernéticos y el fraude a las fuerzas del orden.

Contexto: La *Real Policía Montada de Canadá* (RCMP) establecerá la *Unidad Nacional de Coordinación de delitos cibernéticos* (Unidad NC3) para coordinar las operaciones de la policía canadiense contra los ciberdelincuentes y establecer un mecanismo nacional para que los canadienses y las empresas denuncien los delitos cibernéticos a la policía.

La RCMP también mejorará su capacidad operativa (investigaciones, inteligencia, servicios de investigación técnica especializada, presencia internacional y experiencia cibernética especializada) para tomar medidas de aplicación federales contra la actividad prioritaria del delito cibernético tanto a nivel nacional como internacional. Más específicamente, la RCMP:

- Mejora la capacidad para atacar las actividades delictivas relacionadas con ciberseguridad.
- Mejora la capacidad especializada de los equipos de investigación federales y aumentar la capacidad para responder y participar en investigaciones conjuntas con los principales socios internacionales de aplicación de la ley de Canadá.
- Detectar, prevenir y responder a amenazas para la seguridad de los canadienses y los intereses canadienses.

Action/Milestone	End Date	Status
Deploy cyber specialists abroad	2020	In Progress
Establish/support cybercrime investigative teams	2021	In Progress
Recruit/train cyber capability specialists	2021	In Progress

Análisis *benchmark*

Kindergarden to grade 6 initiatives

Common Sense Education

Todos los estudiantes necesitan habilidades digitales para participar plenamente en sus comunidades y tomar decisiones inteligentes en línea y en la vida. El galardonado *K-12 Digital Citinzenship Curriculum* aborda las principales preocupaciones de las escuelas:

(i) Prepara a los estudiantes con habilidades críticas del siglo XXI. (ii) Apoya a los educadores con formación y reconocimiento. (iii) Involucra a toda la comunidad a través del alcance familiar. (https://www.commonsense.org/education/digital-citizenship/curriculum).

Cybint

Cybint es una empresa global de educación en ciberseguridad comprometidos con reskilling de la fuerza laboral y mejorar la industria en ciberseguridad con soluciones de educación y capacitación innovadoras. Cybint aborda las dos mayores amenazas de la ciberseguridad: la escasez de talento y la brecha de habilidades. (https://www.cybintsolutions.com/about/).

Scratch Animation

Scratch está diseñado especialmente para personas de 8 a 16 años, pero lo utilizan personas de todas las edades. Con un alcance significativo y presente en una amplia variedad de entornos, incluidos hogares, escuelas, museos, bibliotecas y centros comunitarios, los estudiantes pueden usar Scratch para codificar sus propias historias interactivas, animaciones y juegos. En el proceso, aprenden a pensar de manera creativa, a razonar de manera sistemática y a trabajar en colaboración. Los educadores están integrando Scratch en muchas áreas temáticas y grupos de diferentes edades. (https://scratch.mit.edu/projects/editor/?tutorial=getStarted).

Kids Code Jeunesse

El objetivo de esta iniciativa es brindar a todos los niños canadienses acceso a la educación en habilidades digitales, con un enfoque en las niñas y las comunidades desatendidas. Quieren que los niños de Canadá tengan la oportunidad de aprender el pensamiento computacional a través del código. (https://kidscodejeunesse.org/).

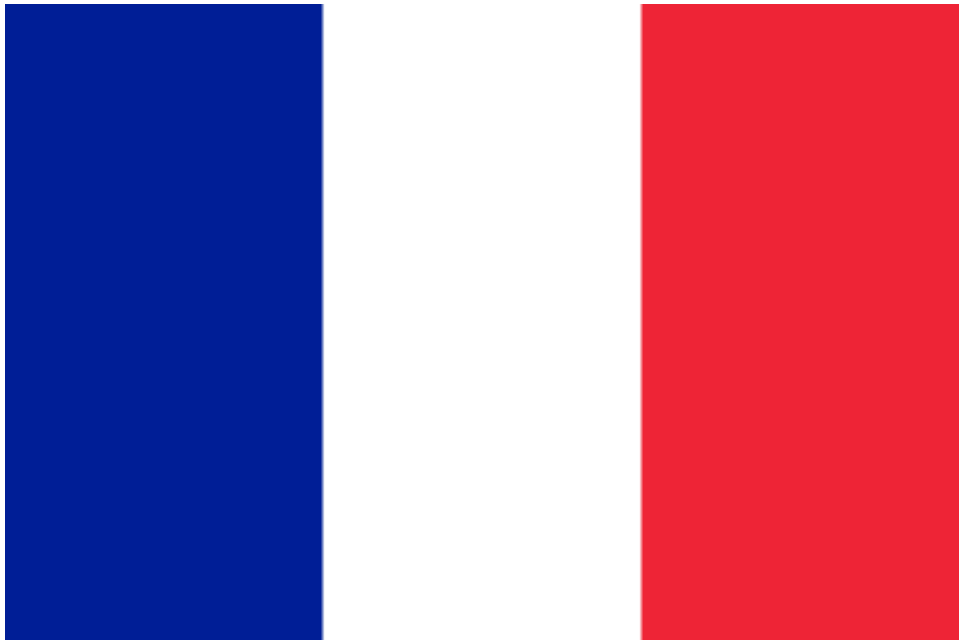
Technovation

Technovation es una organización sin fines de lucro de educación tecnológica global que empodera a las niñas y sus familias para que se conviertan en líderes, creadoras y solucionadoras de problemas. Ofrecen dos programas, Technovation girls y Technovation families, que unen a niños y adultos para resolver grandes problemas en sus comunidades. (https://technovationchallenge.org).

Conclusiones y recomendaciones

- *La estrategia de ciberseguridad de Canadá es altamente inclusiva. Vinculan a diferentes stakeholders clave y reconocen que la inversión es una de las piezas fundamentales.*
- *La inversión de Canadá para el despliegue de su estrategia de ciberseguridad asciende a los 425 millones de euros.*
- *La manera en la que esperan abordar la problemática de la brecha en la fuerza laboral en ciberseguridad, es a través de la consolidación de un ecosistema resiliente que se adapta a las necesidades actuales. Esto nuevamente lo vinculan con una necesidad inminente de invertir recursos económicos.*
- *El Canadian Centre for Cyber Security es la única fuente unificada de asesoramiento, orientación, servicios y apoyo de expertos en ciberseguridad para el gobierno, operaciones de infraestructura crítica, sector privado y público canadiense. Con el Cyber Centre, los canadienses tienen un lugar claro y confiable al que acudir en caso de problemas de ciberseguridad.*
- *El learning hub es una de las iniciativas insignia de Canadá, ya que reúne a los actores más importantes del ecosistema mediante cursos que aportan a la capacitación tanto de estudiantes como de educadores. Es el claro ejemplo de iniciativas con impacto de largo plazo.*
- *Iniciativas que contemplan enfoques innovadores como el Aprendizaje integrado en el trabajo (WIL) a lo largo de tres años en ciberseguridad son una de las mayores apuestas de Canadá porque es la manera en la que esperan que haya un ajuste entre las necesidades de las empresas y el talento disponible en el mercado.*
- *Canadá entiende la necesidad de incluir en sus iniciativas a las pymes. Son el 98% del tejido productivo y por ende esperan a través de certificaciones poder incrementar la competitividad y la confianza en la economía digital.*
- *Algunas iniciativas en Canadá, como la publicación "Learning Outcomes", tiene una parte de mucho valor relacionada con los educadores: estos tendrán la oportunidad de brindar estándares comunes en sus programas de estudio en ciberseguridad.*
- *Importantes iniciativas como la Cyber Security Talent Alliance se centran en puntos de alta importancia para la industria: aumentar la oferta de profesionales, promover la diversidad, incrementar el awareness y apoyar a las empresas en el reclutamiento, desarrollo y retención del talento.*

Francia



Francia

¿Qué orden seguiremos?

- Estrategia de ciberseguridad de Francia.
- Análisis *benchmark*.
- Conclusiones y recomendaciones.

Estrategia de ciberseguridad

La estrategia de ciberseguridad de Francia, o la estrategia nacional francesa para la seguridad del ámbito digital, como la llaman ellos, además de ser la respuesta natural a una transición digital que está viviendo el país, es la apuesta del gobierno francés de favorecer el desarrollo de un ciberespacio innovador que sea lugar de oportunidades para las empresas francesas. Es además una forma de afirmar los valores democráticos y preservar la vida digital y los datos personales de los franceses.

+ *AWARENESS*

5 Objetivos estratégicos

+ *FORMACIÓN*

Intereses fundamentales, defensa y seguridad de los sistemas de información del Estado y de las infraestructuras críticas, crisis informática mayor	Al desarrollar un pensamiento estratégico autónomo, respaldado por un conocimiento técnico de primer rango, Francia creará un dispositivo para defender sus intereses fundamentales en el ciberespacio del futuro. Paralelamente, continuará reforzando la seguridad de sus redes críticas y su capacidad de resistencia en caso de ataque grave mediante el desarrollo de cooperaciones tanto a escala nacional con actores privados como a escala internacional.
Confianza digital, vida privada, datos personales, ciberataques	Para que el ciberespacio sea un espacio de confianza para todo tipo de empresas y para los ciudadanos, se adoptarán medidas de protección y de reacción. La protección implicará una mayor vigilancia de los poderes públicos en el uso de los datos personales y el desarrollo de una oferta de productos de seguridad digital adaptada al público en general. La reacción se articulará en torno a un dispositivo de asistencia a las víctimas de ciberataques que brindará una respuesta técnica y judicial.
Sensibilización, formaciones iniciales, formaciones continuas	La concienciación individual frente a los riesgos ligados a la digitalización de la sociedad sigue siendo insuficiente. Ante este hecho, se reforzará la sensibilización de los estudiantes. Además, con el fin de dar respuesta a la creciente demanda de empresas y administraciones en materia de ciberseguridad, se desarrollará la formación de expertos en este ámbito.
Entorno de las empresas del sector digital, política industrial, exportación e internacionalización	La concienciación individual frente a los riesgos ligados a la digitalización de la sociedad sigue siendo insuficiente. Ante este hecho, se reforzará la sensibilización de los colegiales y estudiantes. Además, con el fin de dar respuesta a la creciente demanda de empresas y administraciones en materia de ciberseguridad, se desarrollará la formación de expertos en este ámbito.
Europa, soberanía digital, estabilidad del ciberespacio	Al desarrollar un pensamiento estratégico autónomo, respaldado por un conocimiento técnico de primer rango, Francia creará un dispositivo para defender sus intereses fundamentales en el ciberespacio del futuro. Paralelamente, continuará reforzando la seguridad de sus redes críticas y su capacidad de resistencia en caso de ataque grave mediante el desarrollo de cooperaciones tanto a escala nacional con actores privados como a escala internacional.

Reclaman que el soporte de todo es la formación y la cooperación internacional, y debe haber un respaldo conjunto de: el Gobierno, las administraciones, las colectividades territoriales, las empresas y más ampliamente, sobre todo los ciudadanos.

Análisis *benchmark*

Potencial de la industria de la ciberseguridad en Francia

El mercado francés de la ciberseguridad está muy avanzado en términos de experiencia y capacidad de los profesionales de la industria local. Además, incidentes recientes han aumentado la conciencia de las amenazas y han reforzado la demanda de productos de ciberseguridad en el país, es decir, hay una demanda creciente especialmente en sectores de TI, incluida la analítica empresarial; dispositivos; cloud; y redes sociales. En general, el coste de la ciberdelincuencia para las empresas francesas supera los 3.300 millones de euros anualmente, y el robo de datos bancarios y patentes representa la mitad del número total de incidentes. Ante una amplia gama de preocupaciones, las autoridades y empresas francesas tienen la intención de hacer frente al ciber terrorismo y la guerra cibernética mediante el diseño de soluciones de *hardware y software* más sofisticadas.

Alta participación del mercado local

5

Empresas hacen el

75% del mercado

(Morpho, Thales, Orange, Cassidian y Atos)

40.000

Puestos de trabajo

Drivers de la industria:

Infraestructura

Cloud Security

6.250M de euros

Para 2020

Tasa de crecimiento anual compuesto a 5 años del

8%

Fuente: Cybersecurity Opportunities in France

El compromiso del país es invertir 1.000 millones de euros en ciberdefensa

Análisis *benchmark*

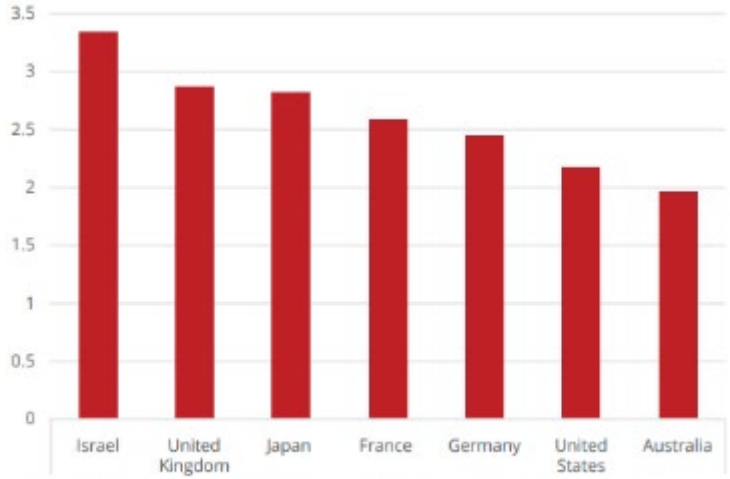
GAP de la fuerza laboral en ciberseguridad

En Francia, al igual que en la mayoría de países se está alcanzando un nivel de escasez de talento crítico. Además de la inminente falta de profesionales en la industria de ciberseguridad, también es evidente que en diferentes sectores de la economía está siendo necesario que se logre una oferta de capacidades en ciberseguridad más visible y accesible. La ciberseguridad es además considerada ahora una prioridad nacional y ante esto contar con profesionales listos para trabajar es una de las prioridades.

¿Cuál es el conjunto de *skills* más escaso?

	France
Intrusion detection	73%
Software development	78%
Attack mitigation	65%
Ability to communicate effectively	68%
Fluency in programming languages	67%
Ability to manage a team	67%
Ability to collaborate with other team members	52%

Prima salarial para profesionales en ciberseguridad



Cybersecurity salary premium (annual average salary from survey compared to OECD average annual wages).

- Las organizaciones en Francia estiman que alrededor del 15% de las posiciones en ciberseguridad no podrán ser cubiertas.

Según un informe publicado por McAfee en 2020, Francia refleja una prima salarial cercana al factor 2,5 (respecto a la media salarial anual en las profesiones de TI) para profesionales que se dedican a la ciberseguridad, como lo señala la figura.

Fuente: (ISC)2 *Cybersecurity Workforce Study*, 2020; *Initial National Cyber Security Skills Strategy*, 2018. *Hacking the skills shortage, McAfee*.

Análisis *benchmark*

La Agencia para la ciberseguridad

Las orientaciones estratégicas adoptadas estos últimos años al más alto nivel del Estado francés han asentado la ciberseguridad como una de las prioridades de la acción del gobierno. Para hacer frente al desafío cada vez mayor que representan los ciberataques y siguiendo las recomendaciones del Libro Blanco sobre Defensa y Seguridad Nacional, se creó en julio de 2009 la *Agencia Nacional de Seguridad de los Sistemas de Información* (ANSSI). Se trata de una agencia interministerial dependiente del Primer Ministro. El estatuto de la ANSSI se reforzó a principios de 2011, puesto que la agencia pasó a ser la autoridad nacional de defensa de los sistemas de información.

Cybersecurity is a fascinating and highly scientific field spanning a range of disciplines and involving a wealth of organisations and actors, from both the public sector and the business world, within France, at the European level, and internationally.

Guillaume Poupard, ANSSI Director

- El papel de la *Agencia Nacional de Ciberseguridad de Francia* (ANSSI) es fomentar una respuesta coordinada, ambiciosa y proactiva a los problemas de ciberseguridad en Francia, impulsar acciones de sensibilización, así como difundir la visión y la experiencia francesa, y los valores europeos, en el extranjero.
- La ANSSI se compromete a garantizar que las administraciones públicas, los servicios públicos y las empresas puedan aprovechar al máximo una digitalización segura y confiable.
- La ANSSI sustituyó a la *Dirección Central de Seguridad de las Redes y la Información* (DCSSI) de la Secretaría General de Defensa Nacional, al tiempo que reforzó sus competencias, personal y recursos.
- Este organismo es considerado un "*warehouse*" de habilidades que imparte su experiencia y ayuda a los departamentos gubernamentales y operadores de vital importancia.
- Tiene la tarea de promover las tecnologías, los sistemas y los conocimientos técnicos franceses. Desempeña un papel en la generación de confianza en la esfera digital.
- El comité estratégico compuesto por altos directivos y funcionarios gubernamentales es el escenario idóneo donde se adelantan propuestas de estrategia del estado e la ciberseguridad en Francia e incluso en Europa.

Los precedentes en materia de ciberseguridad en Francia señalan un alto expertise y buenas prácticas en la gobernanza.

Análisis *benchmark*

Entrenamiento / Formación ANSSI

Ofrece cursos de formación impartidos por expertos de ANSSI para funcionarios y personal militar en forma de cursos cortos y uno de ciclo largo para obtener el título de '*Experto en seguridad de sistemas de información* (ESSI)'.
ANSSI también participa en varios programas para promover el reconocimiento de la formación continua o inicial en el campo de la ciberseguridad.

The ANSSI Cybersecurity Training Center (CFSSI) is involved in the definition and implementation of the French national information systems security training policy.

Guillaume Poupard, ANSSI Director

- SecNum es una capacitación en línea gratuita en temas relacionados con la ciberseguridad.
- La formación y concienciación de los franceses sobre la ciberseguridad es un gran desafío. En respuesta, ANSSI lanza su primer curso en línea, el MOOC SecNumacadémie, que hace que la ciberseguridad sea accesible para todos. El propósito de esta nueva herramienta de formación es concienciar a los usuarios en el lugar de trabajo sobre la ciberseguridad para que se conviertan en actores para mejorar su seguridad y la seguridad de su empresa. Con este MOOC, los usuarios podrán aprender y asimilar conceptos básicos de ciberseguridad que son útiles en el trabajo y en casa.
- SecNumedu ofrece una garantía a estudiantes y empleadores de que la formación en el campo de la ciberseguridad cumple con unos criterios definidos por ANSSI en colaboración con actores y profesionales en la industria (instituciones de educación superior, empleadores ...). Este programa está abierto a cualquier institución de educación superior que cumpla con uno de los siguientes criterios:

    1. Cursos de ingeniería cuyo diploma está reconocido por la comisión francesa des titres d'ingénieurs.
    2. Cursos universitarios que otorgan una licencia o maestría.
    3. El Mastère spécialisé ® reconocido por la Conference des grandes écoles (un Máster + un año de formación).

Esta iniciativas reflejan el compromiso con el acceso y la calidad de la formación en ciberseguridad.

Análisis *benchmark*

Consolidando capacidades

Como respuesta a diversas amenazas y a los desafortunados ataques terroristas de 2015, Francia considera como una de las cuestiones fundamentales en su estrategia de ciberseguridad proteger la infraestructura crítica y es evidente que la consolidación de capacidades técnicas y científicas es una de las orientaciones clave.

OBJETIVO

Francia se dotará de los medios necesarios para defender sus intereses fundamentales en el ciberespacio. Consolidará la seguridad digital de sus infraestructuras críticas y la seguridad de sus operaciones esenciales para la economía.

ORIENTACIONES

> Estar en posesión de las capacidades científicas, técnicas e industriales necesarias para la protección de la información de soberanía, para la ciberseguridad y para el desarrollo de una economía digital de confianza.

Además de esto, Francia tiene la intención de crear un grupo de trabajo de expertos para fomentar la confianza digital. Este grupo reunirá con bastante frecuencia las administraciones competentes del Primer Ministro, de los ministerios de Educación Nacional, de Enseñanza Superior y de Investigación, de Defensa, de Justicia, de Asuntos Sociales, de Sanidad y de Derechos de las Mujeres, del Interior, de Economía, Ministerio de Industria y del Ámbito Digital, entre otros. El grupo podrá asociar a sus actividades a protagonistas del sector privado y a personalidades cualificadas.

MISIÓN

La misión de este grupo será, entre otras cosas, identificar las tecnologías clave cuyo dominio es necesario para los sectores de la ciberseguridad y, en términos más generales, para el desarrollo de un entorno digital de confianza. Evaluará las necesidades de formaciones iniciales y continuas, participará en la mejora del asesoramiento de los jóvenes, y prestará particular atención a los trabajos de investigación.

Transferencia de conocimiento

Francia se preocupará por sacar todo el partido a los dinamizadores ofrecidos por la Unión Europea a fin de apoyar, promover y defender las competencias tecnológicas e industriales francesas en el campo de la ciberseguridad. Animará, además, a la UE a no limitarse a un papel de consumidor, sino a imponerse como un actor global imprescindible de la oferta de este sector.

- **Francia espera transferir los conocimientos adquiridos al sector privado para llevarlo a hacerse cargo de su ciberseguridad.**

Francia se ha dotado en los últimos cinco años de una capacidad de detección y de tratamiento de los ataques informáticos, sin embargo, corresponde al sector privado ocuparse de su propia ciberseguridad igual que en los otros ámbitos, solo en caso de crisis grave deben intervenir los servicios del Estado.

Gracias a la transferencia de los conocimientos adquiridos por las administraciones hacia el sector privado, la certificación de proveedores competentes y de confianza debería permitir detectar y tratar el inevitable incremento del número de ataques que las empresas enfrentan.

Colaboración y apoyo al ecosistema digital

Francia declara que espera contribuir a la estabilidad global del ciberespacio apoyando a los países voluntarios en la creación de capacidades de ciberseguridad.

A fin de garantizar la sostenibilidad y la durabilidad de los proyectos de refuerzo de las capacidades, Francia enmarcará su acción, preferiblemente, en asociaciones de confianza a largo plazo. Esta acción también deberá permitir que Francia refuerce su propia ciberseguridad.

Es necesario homogeneizar el ecosistema

Con el fin de contribuir a un despliegue fiable y sostenible de las tecnologías digitales en todos los países, y en particular de los países en vía de desarrollo, Francia debe contribuir al refuerzo de las capacidades de los países que desean aumentar la resiliencia y la seguridad de sus sistemas de información, especialmente en materia de protección de las infraestructuras críticas y la lucha contra la ciberdelincuencia.

Análisis *benchmark*

Programa de sensibilización a gran escala

Como parte del objetivo que tiene Francia de sensibilizar y desplegar formaciones, se promoverá desde la escuela justamente la sensibilización sobre la seguridad digital y los comportamientos responsables en el ciberespacio. Las formaciones iniciales superiores y continuas incorporarán un componente dedicado a la seguridad digital adaptado al sector correspondiente.

Sensibilizar a todos los franceses

En Francia están aparentemente dispuestos a impulsar un programa ambicioso de sensibilización de todos los franceses. Bajo la dirección del Ministerio de Educación Nacional, de la Enseñanza Superior y de Investigación y de la Secretaría de Estado para la Economía Digital, con el apoyo del servicio de información del Gobierno y de la agencia nacional de seguridad de los sistemas de información, se hará un llamamiento a la manifestación de interés para la realización de contenidos de sensibilización del público en general.

El Ministerio del Interior continuará la operación «Permiso de Internet» iniciada en 2014 por la gendarmería nacional en asociación con una fundación privada, y secundada desde comienzos de 2015 por la Policía Nacional. Esta operación permite sensibilizar sobre los riesgos y asesorar a más de 300.000 alumnos de CM2 [de 9 a 11 años] cada año para protegerlos en su navegación por Internet.

Francia reconocer estar un poco retrasado respecto a sus socios en materia de sensibilización de la población y esta es la determinación que tienen para lograr un cambio en el menos tiempo posible.

Conclusiones y recomendaciones

- *La estrategia nacional francesa para la seguridad del ámbito digital cuenta con 5 objetivos estratégicos. A pesar de que uno de ellos específicamente hace referencia a la sensibilización, formaciones iniciales y formaciones continuas, toda la estrategia se apoya en la formación de talento y la construcción de capacidades.*
- *El despliegue de la estrategia genera un compromiso de inversión cercano a los 1.000 millones de euros durante su ejecución.*
- *Desde 2009 se creó la Agencia Nacional de Seguridad de los Sistemas de Información (ANSSI). Se trata de una agencia interministerial dependiente del Primer Ministro. Es la autoridad en todo lo relacionado con ciberseguridad y despliegan desde allí varios recursos que fortalecen el ecosistema.*
- *El mercado de la ciberseguridad en Francia es robusto, alcanzó para 2020 los 6.000 millones de euros, genera más de 40.000 empleos, y según su estrategia el foco lo van a poner en la seguridad de la infraestructura crítica y en tecnología punteras como cloud computing.*
- *El gap de la fuera laboral está estimado en una cifra cercana a los 120.000 puestos de trabajo para 2020.*
- *Según las organizaciones en Francia, el conjunto de habilidades de ciberseguridad más escaso es "detección de intrusiones" lo cual es afirmado en el 73% de los casos, según estudio de McAfee en 2020.*
- *En su estrategia de ciberseguridad señalan la importancia de proteger la infraestructura crítica y es evidente que la consolidación de capacidades técnicas y científicas es una de las orientaciones clave.*
- *Una manera de darle continuidad a las capacidades en ciberseguridad en Francia es a través de la transferencia del conocimiento, donde se busca que el sector privado se ocupe de su propia ciberseguridad y que el estado solo intervenga en crisis graves.*
- *Las relaciones de confianza y de largo plazo con organismos y estados son una prioridad en Francia para garantizar las sostenibilidad de proyectos relacionados con el desarrollo de capacidades en ciberseguridad y por eso enmarca sus iniciativas en esa premisa. Se piensa que es una manera de mejorar consistentemente la ciberseguridad del país.*
- *SecNum es una de las iniciativas insignia en materia de ciberseguridad, reúne a los actores relevantes de la industria y garantiza educación de calidad en ciberseguridad.*

Rusia

Rusia

¿Qué orden seguiremos?

- Postura de ciberseguridad de Rusia.
- Análisis *benchmark*.
- Conclusiones y recomendaciones.

Postura de ciberseguridad

Los últimos años han sido testigos de los intentos de Rusia de cerrar y asegurar su propio espacio de información digital. Mediante el uso de una combinación de medios legales y técnicos, el Kremlin intenta imponer el control tanto sobre la infraestructura digital como sobre el contenido, esfuerzos que tienen como objetivo garantizar la independencia de la red mundial de internet y, por lo tanto, mejorar la seguridad de la información.

Para entender la agenda de ciberseguridad de Rusia, es importante entender su visión de la ciberseguridad y cómo esta ha evolucionado en las ultimas dos décadas. Rusia ve las actividades en el ciberespacio como un subconjunto del marco global de "confrontación de información", que se deriva de la comprensión rusa de las relaciones entre estados y, más específicamente, un subconjunto de la lucha entre las grandes potencias por la influencia en el mundo.

Según los pensadores rusos:

- La confrontación de información es constante y permanente, y se puede utilizar cualquier medio para ganar superioridad en esta confrontación.
- Las actividades en el ciberespacio son una de las varias herramientas de guerra en el entorno de la información, incluidas las operaciones psicológicas, la guerra electrónica (EW) y la acción cinética.
- El ciberespacio se puede utilizar tanto para ataques físicos a la infraestructura como para ataques cognitivos como la desinformación. Sin embargo, el centro de gravedad de la "confrontación de información" reside en la mente y la percepción de la gente de los acontecimientos, tanto a nivel nacional como internacional.

Desde la perspectiva rusa, la guerra cibernética o el equivalente ruso "guerra de tecnología de la información" es solo una parte del concepto general de "confrontación de información". El Ministerio de Defensa ruso describe la confrontación de información como el choque de intereses e ideas nacionales, donde se busca la superioridad apuntando a la infraestructura de información del adversario mientras se protege sus propios objetos de una influencia similar.

> Russia perceives the information space in very geopolitical terms, with their domestic information space representing a continuation of territorial state borders, which they view as constantly being violated by foreign intrusions.

La postura de ciberseguridad en Rusia es altamente defensiva.

Análisis *benchmark*

Industria de la ciberseguridad en Rusia

Algunas de las cifras que se han logrado identificar para el mercado de ciberseguridad en Rusia indican que dicho mercado podría haber crecido de 1,54 billones de euros en 2013 a 2,44 billones de euros en 2019, a una tasa compuesta anual del 7,30% para ese período. El mercado está impulsado principalmente por la relación bilateral entre Rusia y Estados Unidos para contrarrestar amenazas de ciberseguridad.

EUR 2.440M

Para 2019

Tasa de crecimiento anual compuesto a 6 años del

7.5%

Principales actores:

Kaspersky
Zer0Data
IBM
Cisco Systems
The Oracle of Liberty
Any.run
SiteSecure

Drivers de la industria:

Counter Cyber Security Threats from the US.

Secure and Resilient Cyberspace

Los eventos de ciberataques en los juegos olímpicos de Sochi 2014 han llevado a la industria a trabajar incluso con EE.UU para construir una estructura sólida que permita hacer frente a las amenazas.

La inversión en iniciativas y despliegue de la estrategia es indeterminada.

Análisis *benchmark*

Objetivos de aprendizaje en las escuelas rusas

Es importante poder conocer la manera y la doctrina en la que abordan la educación en las escuelas rusas, conectando las ciencias de la computación con la seguridad informática. Ante esto, se ha consultado un estudio de 2014 que explica los requerimientos y formación que reciben los estudiantes antes de pasar a realizar estudios universitarios. En este sentido, es de destacar que el nivel relativamente alto de educación escolar en informática en Rusia está determinado por un sistema metodológico bien establecido con una historia de 30 años, el tema está en la lista de disciplinas básicas en la escuela, así como la existencia de una sistema de educación patrocinado por el estado para profesores de informática.

En Rusia se introduce para los grados 9 y 10 la asignatura 'Fundamentos de la informática' en 1.985 en todas las escuelas de la Unión Soviética. El objetivo declarado era formar 'un pensamiento algorítmico y una alfabetización informática' de los estudiantes. Se identifican los siguientes componentes:

El elemento de mayor importancia en esta introducción escolar, es la preparación de los profesores.

- El concepto de algoritmo y sus propiedades, medios y métodos para describir algoritmos, el programa como forma de representación del algoritmo para computadoras.
- Fundamentos de la programación en un lenguaje de programación.
- Habilidades prácticas con computadoras.
- Principios de funcionalidad informática y sus elementos básicos.
- Aplicaciones informáticas, su papel en diferentes sectores de la actividad humana.

Durante dos años el estado ruso ha llevado a cabo una campaña para preparar a los profesores de matemáticas y física para enseñar informática en las escuelas. La campaña involucró a miles de maestros en todo el país.

Evolución del esquema de educación en Rusia

A partir de la década de los 90 se vio una nueva etapa en la forma en que se enseñaba informática. Durante esa década se comenzó a trasladar el conocimiento de los niveles 9 y 10, a estudiantes en niveles inferiores y poder dar acceso a estudiantes de más corta edad. Adicionalmente, con la expansión de las computadoras personales y el desarrollo de *software*, el paradigma de la alfabetización informática cambió. Hubo una transición parcial de la programación a operar una PC como usuario.
El contenido educativo está determinado por los *Estándares Educativos Federales* (FES). Estos incluyen:

- La estructura de los programas educativos (incluida la relación entre la parte obligatoria de un programa educativo y la formada por una institución educativa) y su intensidad de estudio.
- Las condiciones para la implementación de los programas educativos, incluidos los relacionados con el personal, las finanzas y la logística, entre otros.
- Los resultados de aprendizaje esperados en los programas educativos.

Además de que los programas educativos tienen cierta autonomía, se desarrollan y se aprueban independiente por la institución que lleva a cabo la educación, en 2010-2012, se introdujo una nueva generación de estándares (FES). Según este documento, cada escuela tuvo aún mayores oportunidades para ampliar el alcance del contenido educativo más allá del mínimo obligatorio especificado por la FES. La informática es ahora una asignatura obligatoria en la escuela secundaria, y cualquier escuela puede optar por incluirla en su plan de estudios de secundaria en un nivel básico o avanzado. En la escuela primaria, los elementos de Informática se enseñan dentro de las materias básicas 'matemáticas' y 'tecnología'. Además, cada escuela primaria tiene derecho a incluir la asignatura 'informática' en su plan de estudios.

La FES o estándares funcionan más como una guía que establece ciertos requisitos para garantizar ciertos resultados del aprendizaje.

Educación en la escuela secundaria

Los *Estándares Educativos Federales* (FES) determinan los objetivos de aprendizaje de las asignaturas escolares. Con objetivos de aprendizaje específicos definidos individualmente para cada materia, la educación en su conjunto se presenta como un sistema de resultados personales, en el que el desarrollo personal y la educación son los objetivos primordiales de todas las etapas educativas. En esencia, significa el desarrollo de habilidades intelectuales y la formación de cualidades conductuales de importancia personal y social.
Los resultados de aprendizaje requeridos actualmente son:

Nivel básico

- Formación de los conceptos de los roles de la información y procesos relacionados.
- Capacidad para usar habilidades de pensamiento algorítmico y comprender la descripción formal de algoritmos.
- Capacidad para comprender programas escritos en un lenguaje algorítmico seleccionado, conocimiento de construcciones básicas de programación, capacidad para analizar la ejecución paso a paso de algoritmos.
- Uso de métodos estándar para crear programas en un lenguaje algorítmico usando diseños básicos estándar para programar y depurar dichos programas; uso de aplicaciones informáticas listas para usar.
- Formación del concepto de modelos informáticos y matemáticos, y capacidad para analizar el modelo y el objeto simulado (proceso).
- Formación del concepto de bases de datos y capacidad para trabajar con ellas.
- Capacidad para utilizar métodos de presentación y análisis de datos.
- Formación de habilidades y conocimientos básicos sobre seguridad e higiene, cuando se trabaja con el ordenador.
- Conocimiento de los conceptos básicos de los aspectos legales de los programas de ordenador y el uso de internet.

Nivel avanzado

- Adquirir conocimientos básicos sobre la contribución de la informática a la formación del mundo científico moderno.
- Dominio de lenguajes universales de alto nivel (opcional), conceptos básicos de tipos de datos y estructuras de datos, y capacidad para utilizar las estructuras algorítmicas básicas.
- Habilidades y experiencia en desarrollo de software en el entorno de programación elegido, incluyendo programas de prueba y depuración; habilidades básicas aplicadas a la formalización de problemas y documentación de programas.
- Creación de objetos digitales, sus propiedades, algoritmos para su análisis, codificación y decodificación de datos, identificación de las razones de la pérdida o distorsión de los datos en la transmisión, sistematización del conocimiento relacionado con los objetos matemáticos de la informática, capacidad para construir objetos matemáticos, incluyendo fórmulas lógicas.
- Formación del concepto de estructura de los ordenadores modernos; tendencias del desarrollo de tecnologías informáticas; funciones básicas de los sistemas operativos; creación y operación de aplicaciones de internet.
- Formación de los conceptos de redes informáticas y su papel en el mundo moderno; conocimiento de los principios básicos de organización y operación de redes de ordenadores, ética de la información y reglas de derecho, principios de seguridad de la información, formas y medios para asegurar el funcionamiento confiable de las herramientas de TIC.

Capacitando a los profesores

La formación regular de los profesores de Informática se inició en 1985, año en que la asignatura apareció por primera vez en el currículo escolar. Para muchos profesores, la informática se ha convertido desde entonces en su principal o único campo de instrucción.

- Inicialmente, el curso tuvo una duración de 5 años, y se otorgó a los egresados la calificación de ´Profesor de Informática'. Hoy en día, un esquema de 2 niveles es más común. La educación básica tiene una duración de 4 años (un programa de licenciatura con una sola especialización en Informática) o 5 años (un programa de licenciatura con una doble especialización, por ejemplo, 'Matemáticas e Informática"). Algunos de los graduados se inscriben posteriormente en programas de maestría. Los cursos incluyen Informática Teórica y Tecnología de la Información, Educación, Psicología y Métodos de Enseñanza de la Informática, y muchos otros. Además hay una práctica docente.

- No todos los graduados continúan trabajando en las escuelas como profesores de informática. La gran demanda de especialistas en tecnologías de la información en Rusia les permite encontrar trabajos que son más remunerativos que la docencia. Aquellos que trabajan en las escuelas, sin embargo, forman una élite de profesores de informática altamente calificados.

- Muchos profesores con otras especializaciones llegan a la informática después de haber realizado cursos profesionales ofrecidos por una variedad de instituciones de formación de profesores.

- Se han implementado varias medidas para apoyar a los docentes en servicio. Los institutos pedagógicos, las universidades y los institutos especiales de formación profesional para profesores realizan periódicamente cursos de actualización en los que se revisan métodos innovadores de enseñanza de la informática. Las sociedades metodológicas de profesores de informática funcionan en varias ciudades y regiones.

Rusia refleja que uno de las activos más valiosos del sistema educativo son los educadores, quienes se encargan de realizar las diversas actividades encaminadas a mejorar el nivel de competencias de las diferentes industrias.

Conclusiones y recomendaciones

- *La estrategia de ciberseguridad de Rusia está basada en la premisa de la "confrontación de información". La percepción que tienen del ciberespacio la relacionan con temas políticos y geográficos y estructuran la política considerando posiciones de confrontación.*
- *El mercado de la ciberseguridad en Rusia es robusto (casi 2,5 billones de euros) y crece a tasas similares a las encontradas en otros países europeos como Francia, cercanas al 8% en periodos de 5 años (CAGR).*
- *El nivel de educación es alto comparado incluso con el sistema educativo K12 (EE.UU) y esto lo determina, entre otras cosas, un sistema financiado por el estado que garantiza la constante capacitación y formación para los profesores rusos.*
- *En Rusia se han destacado por ampliar el contenido educativo y porque las escuelas tengan cierta autonomía para diseñar e implantar sus programas de estudio. Esto podría ser una señal de dinamismo en la generación de conocimiento, caso contrario es la rigidez burocrática.*
- *La formación de conceptos básicos y avanzados en temas relacionados con la informática y la seguridad están desarrollados en Rusia. Es notable que han avanzado en este aspecto para que los estudiantes estén preparados para optar de manera más decidida por una carrera profesional relacionada con la computación.*
- *Rusia refleja que uno de las activos más valiosos del sistema educativo son los profesores, quienes se encargan de realizar las diversas actividades encaminadas a mejorar el nivel de competencias de las diferentes industrias. Por eso tienen una notable trayectoria desde 1.985 emprendiendo planes de formación para este grupo.*