IF INFORME DE FERIA

2021

ICEX España Exportación e Inversiones

SICW / Singapore International Cyber Week

Singapur
4-8 de octubre de 2021

Oficina Económica y Comercial
de la Embajada de España en Singapur

IF INFORME DE FERIA

13 de octubre de 2021
Singapur

Este estudio ha sido realizado por
Jose Manuel Castillo Machado, Clara Campa Roldán y Jose María Ponte Sánchez

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

http://singapur.oficinascomerciales.es

Editado por ICEX España Exportación e Inversiones, E.P.E.

NIPO: 114-21-013-8

Índice

1. Perfil de la Feria

1.1. Ficha técnica

Nombre del evento

Singapore International Cyber Week (SICW)

Fechas de celebración del evento

El evento se celebró del 4 al 8 de octubre

Web

https://www.sicw.gov.sg/

Frecuencia

Anual

Lugar de celebración

Online

Horario de la feria

9:00 – 23:00

Precios de entrada

Entrada gratuita

Sectores y productos representados

Ciberseguridad aplicada a distintos campos entre los que destacan: regulación, IoT, formación, colaboración internacional, limpieza de equipos, mantenimiento de sistemas o plataformas digitales.

2. Descripción y evolución de la Feria

La Singapore International Cyber Week es el evento más importante del sudeste asiático en materia de ciberseguridad. Lleva celebrándose anualmente desde el año 2016 y a él suelen acudir altos cargos, tanto empresariales como gubernamentales, relacionados con el sector.

La edición de 2021 se estructuró de manera virtual en dos series de charlas:

- **Singapore International Cyber Week Conference:** evento dividido en múltiples charlas especializadas en ciberseguridad aplicada a los siguientes campos: IoT, colaboración internacional, regulación y colaboración público-privada.

- **GovWare Conference 2021:** evento enfocado a explorar opciones de crecimiento y adaptación a los retos emergentes. Asimismo, a lo largo de las distintas sesiones se han identificado retos y oportunidades dentro del sector.

A continuación, se exponen las principales oportunidades tratadas a lo largo de cada uno de los eventos.

2.1. Singapore International Cyber Week Conference

2.1.1. International IoT Security Roundtable

Oportunidades en IoT

Durante la sesión se ha ahondado en los distintos retos y oportunidades relacionadas con la ciberseguridad aplicada a la tecnología IoT. Las oportunidades destacadas han sido las siguientes:

- **Eficiencia energética y descarbonización:** es esencial desarrollar sistemas que permitan detectar comportamientos anómales en factores tanto digitales como físicos en el ámbito de la generación de energía y la eficiencia energética.
- **Sector hospitalario:** tal y como se resaltó a lo largo de la sesión, el sector hospitalario es el más atacado por los ciberdelincuentes. Su vulnerabilidad se debe a la existencia de múltiples dispositivos con sistemas anticuados o de baja seguridad. Asimismo, es necesario segmentar las conexiones internas de manera que un dispositivo infectado no pueda expandir el ataque a todo el sistema. Esto generará oportunidades para empresas especializadas en la segmentación de redes internas.
- **Riesgo en la logística de envíos:** otro punto mencionado es la escasa seguridad durante el envío de dispositivos. Durante su trayecto y manipulación en puntos de carga y descarga

estos pueden ser alterados e infectados. Es necesario garantizar la seguridad y trazabilidad de todo el proceso logístico.

- **Colaboraciones con el sector público:** se ha resaltado el ejemplo de Japón, donde el Gobierno ha establecido una serie de programas para identificar y alertar a los propietarios de dispositivos IoT de posibles brechas en su seguridad.
- ***Machine Learning*:** en Singapur existen varias empresas especializadas en la creación de sistemas de seguridad basados en el *Machine Learning*. Estos emplean millones de datos con el objetivo de entender procesos y detectar irregularidades. Se espera un crecimiento en la importancia de estos sistemas a medida que se vaya elaborando una regulación más proclive a compartir datos. Ahora mismo existen muchos recelos a la hora de compartir datos corporativos.
- **Plataformas para compartir datos:** dos de las barreras que frenan la comunicación y el intercambio de datos son la inexistencia de una plataforma segura de referencia y el uso de distintos idiomas.
- **Seguridad relacionada con la nube:** uno de los principales efectos detrás de la popularización de los dispositivos IoT es el uso masivo del almacenaje en la "nube". Se espera que durante los próximos años se produzca un fuerte crecimiento en el empleo de esta forma de almacenaje.

Certificación e información a disposición del consumidor

Durante las jornadas sucesivas, los ponentes también reflexionaron sobre la necesidad de lanzar campañas de concienciación de los clientes, para educarlos en los riesgos de la ciberseguridad a través de sellos y etiquetados de ciberseguridad y de información para el consumidor.

El reto es comunicar los riesgos que un dispositivo IoT presenta para el usuario. Hay peligros que el cliente no percibe, porque cree que es algo que el Gobierno ha controlado de forma anticipada y si ese producto no fuese seguro, no estaría en el mercado.

¿Cuál es el nivel de sofisticación que se puede esperar de un cliente para identificar los sellos de calidad relacionados con la ciberseguridad? ¿Está el consumidor preparado para diferenciar entre un producto con medidas de protección en ciberseguridad y uno que carece de ellas?

Existen diferentes modelos de implementación de sistemas de etiquetado en ciberseguridad en función del país. El etiquetado en ciberseguridad en Singapur es opcional para la mayoría de los dispositivos IoT, pero obligatorio para los *routers* y dispositivos de uso en los hogares. Es un sistema híbrido. En Reino Unido el enfoque es similar, regulan de forma separada los *routers* del resto de bienes de consumo IoT. Según uno de los conferenciantes, debería haber un estándar mínimo, y no un segmento en el que es opcional el sello de ciberseguridad.

La opción más recomendable parece un sistema flexible: mantener un nivel de dificultad bajo para el usuario, sistemas simples para que el consumidor lo pueda comprender fácilmente. En Singapur el sistema está basado en estrellas, 1, 2, 3 o 4 estrellas, en función del nivel de protección del

producto. Nunca un producto podrá tener 5 estrellas, porque no existe el producto perfecto en materia de ciberseguridad, siempre hay nuevas amenazas.

El esquema ideal sería uno que disponga del apoyo de la industria y los gobiernos. La cooperación entre países para crear un sello internacional sería conveniente. Los proveedores no quieren tener que conseguir una certificación para cada mercado según distintos estándares. Es un tema complejo, porque los requisitos son muy distintos en función de las distintas áreas. No es lo mismo fijar los estándares de un *router* que puede ver comprometida la información personal de un individuo que, por ejemplo, los de un dispositivo IoT de transporte a gran escala que puede ver comprometida la seguridad y las vidas de mucha gente (distintos enfoques son necesarios para los bienes de consumo IoT y los bienes industriales).

Tiene su riesgo, según opinaron los participantes en el evento, darle a la industria, por ejemplo, una *check-list* de buenas prácticas de ciberseguridad, porque se dejaría de fomentar la innovación y de hacer que se plantearan cómo enfocar de distintas formas los peligros relacionados con el mundo digital.

La mejor solución sería encontrar el equilibrio entre una *check-list* de buenas prácticas para los fabricantes, animándolos simultáneamente a continuar innovando. Darles las líneas base, pero hacerles ver que tienen que encontrar la forma de ir más allá.

La diversidad de estándares es problemática, incrementa los costes y es improductivo tener que certificar el mismo dispositivo numerosas veces.

Se necesita encontrar un equilibrio, establecer las bases, pero no procesos de certificación y estándares poco flexibles que impidan la innovación. Sería nocivo. El enfoque debería ser fomentar la competencia en seguridad, que sea un punto clave para los fabricantes e innoven en esta área como una forma de diferenciación con respecto a su competencia y aportar valor añadido.

Armonizar los estándares

Gran alianza público-privada para realizar esto. Un buen ejemplo es el reconocimiento de estándares entre Singapur y Finlandia.

Probablemente la solución sería llevar a un comité común los estándares que están funcionando en distintos países en materia de ciberseguridad IoT e intentar fusionarlos en un único estándar internacional. O, al contrario, establecer un estándar básico internacional y que todos los países implementen su propio sistema basado en él.

Conclusiones: Nadie tiene todas las respuestas en esta materia. Parece claro que se está llegando a un consenso en cuanto a las líneas claves en materia de ciberseguridad. Existen algunas diferencias en las estrategias y en su implementación, pero el 80 %, aproximadamente, de los estándares coinciden. La clave sería concentrarse en los puntos en común en el futuro más próximo,

en la base, en las líneas claves. Conseguir un acuerdo de base y construir a partir de eso unos estándares internacionales.

La visión de Israel del panorama global en ciberseguridad

Ponente: Mr Yigal Unna, Director General, Israel National Cyber Directorate (INCD), Israel

La imaginación de los atacantes está volviéndose más creativa. En Israel, 1 de cada 5 empresas fueron víctimas de ciberataques. El 50 % de las compañías tecnológicas fueron víctimas de ciberataques y, al mismo tiempo, un 42 % de las grandes empresas del país. Sólo el 4 % ha reportado perdidas graves durante estos ataques. Sin embargo, el ponente manifestó que no le convencían estas cifras; a su juicio no son realistas, ya que muchas empresas son reticentes a reportar las perdidas. Aun así, un 4 % le parece suficientemente alarmante.

Los ciberataques están volviéndose peores, aun habiendo existido desde los inicios de la informática. Si quieres causar un daño enorme con un arma, por ejemplo, nuclear, necesitas materiales, físicos, ingenieros… En ciberseguridad no necesitas nada, es el arma más sencilla que cabe imaginar (una persona con un ordenador y los conocimientos necesarios desde su casa) y puede tener consecuencias fatales.

En lo que respecta al IoT, cada vez más dispositivos están conectados, lo cual es positivo para la humanidad, pero también incrementa el riesgo de ciberataques muy graves. Las reglas del juego han cambiado, un solo hombre puede manejar las armas más sofisticadas con un ordenador, encontrando, por ejemplo, ataques de *día cero* en redes empresariales o gubernamentales.

Según el ponente, vivimos en un mundo mucho más peligroso que hace unos años. Se puede ver en el ascenso meteórico de los ataques *ramsonware*, por ejemplo. La media del pago de un ataque *ramsonware* en EE. UU. el año pasado fue superior a 180.000 USD por caso. La media de recuperación tras un ataque *ransomware* en EE. UU. es de 16 días, lo cual puede ser devastador si, por ejemplo, se ataca el sistema financiero.

También destaca el auge de las campañas de influencia política basadas en ciberataques, como el caso de una prisión iraní donde se hackearon las cámaras para mostrar al mundo las atrocidades que el régimen cometía contra los prisioneros. No pidieron dinero, el único fin era desestabilizar al régimen. Las democracias liberales tampoco están libres de sufrir un ataque así.

Los gobiernos deben cooperar y compartir información para intentar atajar los ciberataques y detener a los perpetradores. Normalmente, nunca atacan en su propio país, atacan en el extranjero, por ello es crucial la cooperación internacional.

Hay que compartir información e incluso herramientas para combatir esta lacra y encerrar a quien está causando daños a nuestra sociedad y nuestros países. Para finalizar, el ponente destacó que Israel va a firmar un MOU con Singapur y la Agencia de Ciberseguridad de Singapur (CSA).

Estrategia de Japón frente a las amenazas en IoT

Ponente: Mr. Atsushi Umino. Director, Office of the Director-General for Cybersecurity, Ministry of Internal Affairs and Communications (MIC), Japón.

El National Institute of Information and Communications Technology (NICT) de Japón observa y rastrea ciberataques a nivel global, monitorizando más de 300.000 direcciones IP en desuso. Al hacer esto pueden encontrar tráfico hacia estas direcciones IP incluyendo escaneo de puertos o *malware*.

Ha habido un aumento significativo en los ataques desde 2019 y el objetivo de los ataques ha variado, siendo los dispositivos IOT uno de los objetivos prioritarios.

En relación con las medidas de seguridad para dispositivos IoT en Japón, cabe destacar que todo dispositivo conectado a la red debe tener un control de acceso en la función de control remoto, herramientas para recordar a sus usuarios que cambien la contraseña y así actualizar las medidas de seguridad constantemente. Si una empresa cumple con estos estándares, recibe un sello de conformidad llamado la Key Mark.

En Japón se han establecido unas directrices en lo que respecta a la seguridad, diseño y fabricación de los dispositivos IoT. Están en procesos de incorporarlas en los estándares globales como ISO, IAC o ITUT.

Entre las principales medidas que está adoptando Japón para asegurar la seguridad de los dispositivos IoT, destacan dos proyectos:

- **Notice Project** (observación activa): NICT escanea los dispositivos IoT de Japón que tienen IP internacionales e intenta acceder a su sistema vulnerando sus credenciales de acceso. Si NICT encuentra dispositivos vulnerables, informa a los dueños y propone cambios en las credenciales de acceso. Incluso llegan a hacer una notificación de alerta oficial a los usuarios por correo postal.
- **NICTER Project** (observación pasiva): sistema de observación que detecta dispositivos sospechosos enviando información a la *darknet*. Cuando se detectan, NICT informa a los usuarios para que tomen medidas al respecto.

Resultados de Notice Project: 1.790 dispositivos con vulnerabilidades detectados en un mes (agosto de 2021).

Resultados NICTER: 107 dispositivos detectados por día en un solo mes (agosto de 2021).

El departamento de I+D de NICT trabaja en tecnologías como:

- Determinación de prioridades: *screening technology* que utiliza *machine learning* y reduce las alertas en un 87 %, recomendando cuáles son las emergencias más relevantes y prioritarias.

- Identificación de *malware* en dispositivos IoT, autoclasificación mediante Inteligencia Artificial.
- Detección temprana de potenciales actividades de *malware* con *machine learning* que detecte ataques de *malware* simultáneos y los ataje evitando una infección a gran escala.

2.1.2. SICW Technology Conversation

Se ha realizado una extensa explicación sobre los riesgos más graves que afrontan los sistemas de seguridad a nivel geoestratégico. El crecimiento de las tensiones entre distintos países ha provocado que numerosos *hackers* decidan actuar desde países sin acuerdos de colaboración en materia de investigación criminal.

El principal motivo por el que se está produciendo una proliferación en el número de ciberataques es la disponibilidad de las empresas para pagar los chantajes. En este sentido, es habitual encontrar empresas consultoras especializadas en verificar el nivel de amenaza y proceder, en caso de que sea necesario, al pago del chantaje.

Esto lleva consigo importantes problemas regulatorios, especialmente aquellos relacionados con la legalidad de los pagos por rescates. Cabe destacar que una empresa puede perder millones por cada hora que pase sin poder usar un cierto portal.

2.1.3. SG Cyber Safe Partnership Programme & Panel Discussion

Tan Kiat How, Ministro de Estado de Comunicaciones, Información y Desarrollo Nacional, fue el encargado de presentar el nuevo programa.

Mas de 3.000 empresas en Singapur han empezado procesos de transformación digital en 2020. Esto ha provocado un aumento de más de 150 % en el número de ciberataques, los cuales se han centrado en las pymes. Puede ampliarse información sobre el panorama actual de los ciberataques en Singapur siguiendo el siguiente enlace.

El Cyber Safe Partnership Programme es un programa, lanzado por la Agencia de Ciberseguridad de Singapur, que pretende mejorar la resiliencia de las distintas organizaciones frente a los ciberataques. Para conseguirlo, el programa se articulará sobre dos ejes principales:

- **Concienciación de las organizaciones**: se desarrollarán programas enfocados a concienciar a los siguientes grupos:
  - *Empleados*: cómo pueden mejorar sus comportamientos y detectar fraudes.
  - *Equipo directivo*: mediante programas dedicados a explicar la importancia de la ciberseguridad y métodos para implementarla.

- *Departamentos de TI*: en 2022 se hará llegar a todas las empresas una guía con procesos para mejorar la resiliencia de su organización. Esta incluye desde procesos recomendados hasta herramientas para responder ante brechas en su seguridad. De esta manera, las empresas participantes podrán acceder a herramientas de seguridad suministradas por proveedores previamente aprobados por la agencia CSA.

- **Alianzas empresariales:** la agencia CSA se asociará con distintas corporaciones del sector privado con el objetivo de que estas desarrollen programas de formación, productos y servicios que ayuden a concienciar y animar a la adopción de buenas prácticas en materia de ciberseguridad. Asimismo, durante la presentación se ha hecho un llamamiento a la participación de nuevos **socios industriales** relacionados con la ciberseguridad.

2.1.4. SG Cyber Safe for Enterprises Panel Discussion

Mesa redonda en la que se expusieron los **riesgos del auge que los ataques *ransomware* suponen para la comunidad empresarial global**. Este es un problema que puede afectar a cualquier tipo de compañía, independientemente del sector o tamaño de la empresa.

- **Aspectos legales:** Se comentaron las acciones legales, riesgos y formas de actuación que una empresa puede considerar con respecto a los ataques *ransomware*:
  - Contratos, servicios y entregas que tiene que cumplir una empresa y no puede hacerlo por la imposibilidad de operar con normalidad durante un ataque de *ransomware*. Las posibles responsabilidades contractuales y demandas contra la empresa que pueden surgir si ocurre un ataque de *ransomware* y no puede cumplir sus obligaciones comerciales contractuales con sus clientes. Podría suponer años resolver todos estos problemas legales, incluso después de que el ataque sea resuelto.
  - Protección de los datos de los clientes.
  - Pérdida de datos con las interconexiones y riesgos, no sólo para la empresa, sino para los clientes y todas las empresas que trabajan con nosotros.

- ***Cyber insurance*:** para cubrir ciberriesgos como los ataques *ransomware*, que están creciendo de forma desmesurada. Un seguro no es la panacea, por ejemplo, si tu casa se quema, recibes un cheque para reconstruirla, pero sigues perdiendo muchas cosas y pierdes mucho tiempo haciéndolo. Hay aspectos que anteriormente los ciberseguros no cubrían, se centraban en cubrir las obligaciones de cara a los clientes, ahora empiezan a cubrir tasas legales y de asesoramiento en caso de ataque, incluso ayudan con los aspectos reputacionales.

- **Consejos prácticos:** Prevenir es mejor que curar.
  - No olvidar los básicos, las *best practices*: identificación de acceso adecuada, correcta formación del personal contra *phishing emails* y tener copias de seguridad.
  - Importancia de DMARC en el dominio de la empresa.

- Prepararse para dar respuesta a un ataque de *ransomware*, tener los procesos diseñados y realizar simulacros.
- Tener una relación previa con las aseguradoras y las fuerzas del orden, no esperar a un ataque para presentarse, que te conozcan.
- EDR y recursos *antiransomware* que escanean la red en busca de indicios de actividad de *ransomware*.
- Se debe tener una estrategia, una mentalidad de que no necesariamente se debe pagar, tener *backups*, hablar con las organizaciones al mando y pensar en cómo actuar.

- **Pago del rescate en un ataque *ransomware*:** El CSA recomienda no pagar; si se efectúa el pago no hay garantía de que se recuperen los datos y la compañía parece vulnerable para próximos ataques.

1. El pago de *ransomware* podría ser perseguido por la ley, al ser entendido en algunos países como algo en lo que no debería verse envuelta la empresa. Va en contra de las leyes antiterroristas o contra el tráfico de drogas, entre otras.
2. Las empresas tienen que aprender a resistir, y es conveniente tener un equipo legal o de asesoramiento en estas situaciones.

Existe cierta polémica con los ciberseguros, ya que contratar una póliza podría incentivar a los cibercriminales a atacar a la empresa y pensar que a la hora de solicitar los rescates la compañía podría ser más propensa a pagar al estar cubierta por el seguro. Han ocurrido múltiples ataques a aseguradoras robando información de clientes para luego proceder contra ellos con ataques *ransomware* y pedir un rescate al saber que tienen seguro. No es tan fácil no pagar, porque muchas compañías normalmente no tienen opción al no tener copias de seguridad de sus servidores clave o al haber sido encriptadas las mismas.

- Temas adicionales interesantes para la empresa española:
  - Singapore Data Protection Trustmark: puede consultar información sobre esta certificación y el proceso de obtención en el siguiente *enlace*.
  - CSA SG Cybersafe programme: incluye iniciativas para ayudar a las empresas a protegerse mejor en el mundo digital, *cybersecurity toolkits* para líderes de empresas y empleados.

2.2. GovWare Conference 2021

2.2.1. Primera jornada

Nuevos riesgos

Cuando Singapur entró en el confinamiento por la COVID-19, las empresas no estaban preparadas para tener a todo su personal teletrabajando y asumir los riesgos que eso conlleva. Esta rápida digitalización ha traído nuevos peligros y amenazas. Ahora los dispositivos externos como los wifi de los empleados forman parte de los puntos débiles de las empresas.

Casi la mitad de los crímenes en Singapur fueron cibercrímenes en el año 2020 (43 % del total): 16.000 casos, casi el doble con respecto al año anterior, 9.000.

Están apareciendo nuevas amenazas más sofisticadas.

- **Internet de las Cosas (IoT):** Singapur está embarcada en la digitalización y la administración pública intenta predicar con el ejemplo, animando a las empresas a digitalizarse. Muchas de estas empresas dependen de dispositivos IoT, diseñados pensando en el coste o en la funcionalidad, pero no en la seguridad. Esto los hace muy vulnerables. En la industria manufacturera, los dispositivos IoT suelen tener credenciales sencillas de descifrar y son fáciles de hackear. Al procesar datos, normalmente están equipados con *apps*, servicios y protocolos de comunicación. Muchas de sus vulnerabilidades vienen de interfaces inseguras y pueden comprometer el dispositivo, sus datos y posiblemente la red en la que operan.

- ***Operational Technology* (OT):** La tecnología operacional tradicionalmente se basaba en sistemas aislados que, a partir de la adopción del acceso y mantenimiento remotos, se han visto comprometidos. Muchas de estas tecnologías operativas tienen impacto directo en nuestras vidas, como, por ejemplo, el caso de la planta de tratamiento de agua en Florida en el cual los *hackers* subieron el nivel de ciertos parámetros en el agua a niveles mortales mediante el control remoto. El ataque fue detectado a tiempo por un empleado, pero podría haber supuesto una masacre. La ciberseguridad ya no sólo se limita a ataques de datos, puede costar vidas.

- ***Supply Chain Attacks* e implantes:** se están volviendo más sofisticados, ya que los atacantes están consiguiendo moverse hacia arriba en la cadena de suministro y atacar cada vez eslabones más importantes, incluso pivotando entre distintas cadenas de suministro. Solarwinds, una empresa que ofrece servicios de *computing network*, sufrió un ataque pot el cual se implantó un código malicioso en el *software* de gestión clave. Las actualizaciones que contenían ese código permitieron a los *hackers* acceder al sistema de más de 18.000 compañías a las que Solarwinds prestaba servicios. Expertos en ciberseguridad creen que después de este ataque los *hackers* continuaron atacando a un grupo reducido de empresas tecnológicas, como Cisco o Microsoft y a algunas entidades públicas. Dado el nivel de expansión a nivel mundial de estas compañías, los *hackers* podían conseguir acceso a otras cadenas de suministro distintas e independientes de Solarwinds.

- ***Ransomware*:** Hace años los ataques de *ransomware* consistían en encriptar los archivos del portátil de un particular y solicitar un “rescate” para liberarlos. Hoy en día, el *ransomware* es una opción muy lucrativa para los *hackers*. Están consiguiendo pasar de ser un riesgo de TI a serlo de tecnología operacional. La digitalización forzada por la COVID-19 trajo la adopción de prácticas de seguridad poco apropiadas. El ataque a la empresa petrolera Colonial Pipeline es un ejemplo del alcance que los ataques de *ransomware* pueden llegar a tener. Los atacantes hackearon la compañía, anulando los sistemas de OT y cortaron el suministro de gas y petróleo en la costa este de los Estados Unidos durante casi una semana. El *ransomware* creció un 62 % en el último año a nivel global, lo que confirma el

alarmante crecimiento de este tipo de ataques. Esta amenaza se ha hecho más popular con las criptomonedas y la imposibilidad (o al menos enorme dificultad) de rastrear el pago.

- ***Zero Days*:** Caso Accellion. Un grupo criminal consiguió encontrar una vulnerabilidad en su sistema, robó documentos sensibles sin desplegar *ransomware* y amenazó con publicarlos si no se abonaba un rescate. Otro caso fue el de Microsoft. Un ataque de día cero es un ataque contra una aplicación o sistema que tiene como objetivo la ejecución de un código malicioso gracias al conocimiento de vulnerabilidades que son desconocidas para los usuarios y para el fabricante del producto. Esto supone que aún no hayan sido arregladas.

¿Entendemos cómo defendernos de estos riesgos?

Para desarrollar una estrategia efectiva contra estos nuevos riesgos, hay que contemplar una mejora en tres dimensiones principales:

- **Mano de obra**: Singapur, al igual que el mundo en general, sufre una carencia muy grande de mano de obra especializada en ciberseguridad. Para mitigarla, han implantado cursos y carreras en sus instituciones educativas, pero no pueden esperar a que estos nuevos profesionales se formen, necesitan "atajos". Por ejemplo, en el caso de la Tecnología Operativa barajan dos vías: formar a los actuales expertos en dicha Tecnología Operativa en ciberseguridad o formar en la tecnología operativa concreta a los expertos en ciberseguridad actualmente disponibles.
- **Procesos: OT Cybersecurity Experts Panel de CSA (OTCEP)**, lanzado en 2020 en la CSW, permitirá a los profesionales de la ciberseguridad OT de Singapur, los operadores, la industria, los investigadores, los formuladores de políticas del Gobierno, los sectores de las tecnologías de información crítica, las instituciones académicas y otras industrias de OT tener acceso directo a expertos de renombre internacional. A partir de la experiencia respectiva de los miembros designados en los dominios de OT en ingeniería, operaciones y gobernanza, estos actores involucrados pueden aprovechar sus capacidades existentes para mejorar la resiliencia cibernética del sector de OT de Singapur.
  Tecnología: Es evidente la necesidad de tecnologías de ciberseguridad con el panorama actual de ciberataques que pueden costar mucho dinero a las empresas, o incluso vidas humanas. El CSA no puede crear un ecosistema seguro por sí solo y busca continuamente acuerdos con el sector privado para desarrollar tecnología y soluciones de ciberseguridad. Para ello ha lanzado el **Cyber Security Industry Call for Innovation**, programa que fomenta el desarrollo de nuevas soluciones de ciberseguridad. Las inscripciones siguen abiertas hasta el 30 de octubre. Para encarar el problema de los dispositivos IoT vulnerables a ciberataques (porque han sido diseñados pensando en costes y funcionalidad, pero no seguridad), el CSA lanzó el **Cyber Security Labelling Scheme** el año pasado para fabricantes de dispositivos IoT.

Nuevas oportunidades

Se necesita reinventar los riesgos y las amenazas y ver la oportunidad de cambio:

- Invertir en ciberseguridad mejora la reputación de la empresa y es una oportunidad de negocio. Muchas empresas se han dado cuenta de que ser eficientes en ciberseguridad y proteger correctamente a sus clientes y sus datos supone una ventaja competitiva que puede ser diferencial a la hora de adquirir un dispositivo.
- Entender la ciberseguridad como un facilitador en el proceso de digitalización de las empresas.
- Reducir la lista de "tareas pendientes" en ciberseguridad, a base de cooperación y alcanzar soluciones más seguras.
- Una mayor conciencia entre los líderes empresariales y los consumidores sobre los riesgos de ciberseguridad puede abrir y ofrecer nuevas oportunidades.
- Los nuevos vectores de amenazas y tácticas de ataque podrían impulsar un aumento en la innovación para la ciberseguridad, así como un aumento en la demanda de mejores productos.

Temas principales que afrontar

(El ponente facilita una lista de 9 aspectos de los que comenta los 5 primeros)

1. Validación de las medidas de seguridad mediante test: realizar constantemente simulacros, test de ataques.
2. Defensa contra ataques *ransomware*:
   - Reducir el radio de expansión de los ataques (*blast radius*): chequear que es difícil moverse horizontalmente por el sistema, hay que tener copias de seguridad y una buena gestión de las credenciales de acceso. Segmentar por zonas geográficas y funcionalidades para reducir el *blast radius*. Y evitar que el despliegue de *ransomware* sea general. Que no puedan alcanzar todos los servidores.
   - Aumentar la resiliencia de los sistemas y la velocidad de recuperación: Tener copias de seguridad de los servidores claves de los activos principales y ver cuánto tiempo se tarda en ponerlos a operar con normalidad de nuevo.
3. *Supply Chain Security*: se recomienda vigilar la cadena de suministro y ver quiénes son los proveedores claves y si tienen un perfil de riesgo o aplican buenas medidas de ciberseguridad.
4. *Zero trust Networks*: prevenir movimiento lateral mediante la implantación de redes de confianza cero (del inglés *Zero Trust Network*, ZTN), en el marco de la Tecnología la Información (TI), describe un enfoque de diseño e implementación de redes TI. A grandes rasgos, la "confianza cero" consiste en que los dispositivos conectados, como computadores o teléfonos inteligentes, no deben ser considerados fiables, independientemente de que estén vinculados y verificados desde una red corporativa. Este modelo exige una estricta verificación de autenticidad para cada persona y dispositivo que intente acceder a recursos de una red privada, independientemente de donde se intenten conectar.
5. Saber a quién hay que informar de qué y cuándo en un incidente en función de las consecuencias y ver cómo de preparados estamos para afrontar un ataque.

Los 4 puntos siguientes mencionados fueron:

6. *Cloud Defense*
7. *Machine Learning AI (next gen)*
8. Identificar mejoras
9. XDR (detección y respuesta extendidas)

Ciberanalítica basada en Inteligencia Artificial (IA) aplicada a la ciberseguridad

Singapur continúa siendo un objetivo prioritario y vulnerable para los *hackers*. La pandemia ha forzado la rápida digitalización de muchos sectores, por lo que ha aumentado considerablemente la "superficie atacable" de la ciudad-Estado. Esto, sumado al elevado nivel de penetración de Internet, y la adopción de soluciones IoT u OT, hacen de Singapur un objetivo atractivo y vulnerable. Esto puede suponer, a su vez, una oportunidad de negocio.

Los principales problemas en las operaciones de ciberseguridad son lidiar con amenazas desconocidas (como *Zero Days*, APT, *Black Swan events*) y con cantidades masivas de datos. La **ciberanalítica** basada en Inteligencia Artificial (IA) puede ayudar a gestionar esas cantidades masivas de datos para poder sacar conclusiones y prevenir esos ataques desconocidos. Se puede clasificar en tres tipos, de menos a más complejo:

1. **Análisis basados en reglas y firmas (*rules and signature based analytics, simple statistical analytics*)**: bloqueo de indicadores de compromiso (IOC, según sus siglas en inglés) conocidas a través de listas blancas, listas negras, reglas de fuentes de inteligencia en cadena.
2. ***Machine learning***: puede detectar amenazas que se están desarrollando y analizar experiencias pasadas para detectar ataques similares.
3. **Ciberanalítica basada en Inteligencia Artificial multifuncional**: Detección de amenazas basada en el comportamiento con la capacidad de entrenar directamente en datos parcialmente etiquetados, lo que reduce la necesidad de etiquetar grandes conjuntos de datos.

Las conclusiones a las que se puede llegar en cuanto a este bloque son las siguientes:

- El panorama de ciberamenazas continúa siendo muy hostil e inseguro para los usuarios que no están bien protegidos. La amenaza es real y ya está aquí.
- La detección temprana de los ataques continúa siendo de vital importancia.
- Hay enorme necesidad de un enfoque que pueda marcar alertas precisas contra las amenazas conocidas y desconocidas.
- La ciberanalítica basada en IA del comportamiento y autoaprendizaje ha demostrado ser muy efectiva.

Defensa colectiva y cooperación internacional en ciberseguridad frente al panorama creciente de amenazas

Los ciberataques siguen aumentando con la extensión del teletrabajo. Ataques como *ransomware* se hacen cada vez más populares y beneficiosos para los atacantes. Actualmente, los gobiernos

tienen una habilitad limitada para defenderse de los ataques. Un *enfoque colectivo* de defensa podría aportar a los gobiernos, empresas y sectores una defensa más efectiva contra ciber ataques.

Con la llegada de los teléfonos inteligentes, la cantidad de datos en la red ha aumentado y sigue creciendo cada año. Estamos doblando la cantidad de información y la velocidad a la que la volcamos en la red. También el número de aplicaciones que utilizamos. Todo este crecimiento conlleva para todos los países o empresas unos riesgos y unas vulnerabilidades enormes, los cuales la ciberseguridad pretende mitigar y los atacantes aprovechar. Estos ataques han pasado de ir a por empresas específicas a atacar directamente la cadena de suministro y acceder a miles de empresas.

Naciones enteras están usando los ciberataques como una herramienta para desestabilizar a otras naciones e ir tras otros gobiernos (Ejemplo: Rusia contra Ucrania o Georgia).

Los ataques de *ransomware* crecieron un 151 % en la primera mitad de 2021 frente al mismo periodo de 2020. Hubo un notable incremento incluso entre los dos primeros trimestres del presente año, 115 millones de ataques de *ransomware* en el primer trimestre de 2021 frente a los 188 millones del segundo trimestre.

Para interceptar ciberataques es necesario:

- Analítica de comportamiento que detecte anomalías.
- Un sistema que pueda clasificar esas anomalías por orden de importancia y pueda detectar aquellas que suponen un riesgo para el sistema.

Esas anomalías detectadas por *behavioural analytics* en los sistemas de numerosas empresas y particulares se compartirían en la nube de una forma segura y una red de miles de analistas vigilaría esas anomalías en tiempo real y compartiría con el Gobierno los posibles ataques para poder actuar a tiempo y atajarlos. El futuro de la ciberseguridad debería ser algo parecido a eso: cooperación, defensa colaborativa, compartir el conocimiento y la información a través de la nube. Las naciones tienen que trabajar conjuntamente para atajar las amenazas del mundo virtual actual mediante una defensa colectiva.

2.2.2. Segunda jornada

Aumentar la resiliencia

Durante la sesión se ha hecho hincapié en los últimos ataques cibernéticos llevados a cabo, especialmente aquellos dirigidos a bancos y a gobiernos. El ponente destacó la complejidad de estos y su amenaza para la seguridad de todo el país.

Respecto a los mecanismos de seguridad actuales, el método más usado es el sistema de usuario y contraseña. Sin embargo, es un sistema vulnerable. Se necesitan **herramientas para detectar comportamientos sospechosos.**

Adicionalmente, la transformación digital está creando nuevos retos. Especialmente relevantes son aquellos relacionados con la "nube". Otros retos que tendrá que afrontar Singapur son:

- Aumento en el número de aplicaciones *online*.
- Vulnerabilidades en ciertas webs y aplicaciones.
- Número desmesurado de alertas.
- Visibilidad de riesgos limitada.
- Demasiados vendedores y con sistemas muy heterogéneos.
- Presiones regulatorias.
- Recursos insuficientes por parte de muchas organizaciones.

A lo largo de la sesión se incidió en la necesidad de mejorar la visualización de operaciones **para mejorar la detención, investigación y respuestas** frente a las amenazas.

Mejorar la concienciación colectiva

Las técnicas de hackeo han mejorado significativamente en los últimos 5 años. Esto ha provocado que el gasto en ciberseguridad haya aumentado en un 75 %.

En Singapur se han producido varios ataques a lo largo de toda la cadena de suministro, por lo que es esencial desarrollar **métodos de prevención integrales**. Asimismo, debe incrementarse la velocidad en la identificación de riesgos.

La mayoría de las brechas en la seguridad son causadas por errores humanos. Por ello, es necesario invertir en **formación** sobre los distintos riesgos. Adicionalmente, es necesario que los trabajadores cobren relevancia a la hora de reportar elementos sospechosos.

Otro aspecto fundamental es el correcto **mantenimiento de los sistemas de seguridad**. Muchas empresas locales tienen sistemas desactualizados. El gran problema que afronta el tejido empresarial local es elevado número de pymes con presupuestos insuficientes en materia de ciberseguridad.

Construir un futuro más seguro

Existen oportunidades relacionadas con la ciberseguridad en las siguientes áreas:

- **Personal:** especialmente en las áreas de la formación y creación de procesos.
- **Desarrollo de *software*:** relacionado con los sistemas informáticos y con el acceso a recursos.
- **Infraestructura:** centros de datos, protección de la "nube", identificación y construcción de aplicaciones.

Uno de los aspectos en los que se ha incidido a lo largo de la ponencia son los ataques a lo largo de la **cadena de suministro**. Muchas veces las empresas tienen una confianza no justificada en

sus cadenas, lo que es aprovechado por grupos organizados para penetrar sus sistemas de seguridad.

Asegurando la cadena de suministro

Las empresas cada vez se están viendo más afectada por brechas en su seguridad provocadas por sus relaciones con terceros. La aceleración en el proceso de digitalización ha provocado un aumento sin precedentes en el número de delitos ciberneticos.

Existen muchas empresas que no se han preocupado por instaurar y actualizar sus sistemas de ciberseguridad.

Durante el último año se ha detectado un incremento cercano al 100 % en el número de páginas web falsas. Estas muchas veces buscan extraer información de sus usuarios.

Los suministradores externos es la forma mas extendida y más facil para acceder a los sistemas de una empresa. Identificar como y mediante que ruta han accedido a los sistemas es esencial para poder remediar el impacto.

No se puede controlar a todos los suministradores, pero sí se puede identificar cuándo se ha producido un comportamiento sospechoso.

Asimismo, es necesario desarrollar mecanismos y tecnologías que impidan el contagio a lo largo de una industria. En este sentido, surgirán oportunidades relacionadas con los siguientes procesos:

- **Identificación**: entender dónde se ha producido el problema y cómo se puede contagiar a lo largo de una organización y entre los clientes.
- **Análisis**: consiste en comprender y evaluar de dónde pueden provenir los clientes.
- **Mitigación**: deben especificarse los procesos a seguir para suavizar el impacto de un ataque.

Protección de datos

Oportunidades relacionadas con la seguridad en los datos provenientes de tecnologías IoT. Cabe destacar que estos datos muchas veces son subidos a plataformas vulnerables.

Deben destacarse las buenas perspectivas auguradas para empresas especializadas en remediar equipos infectados. Una vez que el problema es grave, existen dos líneas de negocio enfocadas a aportar soluciones para evitar una filtración de datos:

- ***Softwares* de limpieza.**
- **Destrucción física de los equipos:** sin embargo, este proceso no es tan fácil y requiere de la contratación de empresas especializadas. Existen oportunidades para aquellas empresas de destrucción de equipos que cumplan con los estándares internacionales.

Panorama actual de los ciberataques

Pueden existir oportunidades para trabajar con instituciones públicas y grandes empresas que quieran asegurar infraestructuras estratégicas. Un ejemplo es el sector hospitalario, donde durante los próximos años se espera que surjan proyectos promocionados por entidades públicas.

2.2.3. Tercera jornada

Prácticas internacionales en el ámbito de la ciberseguridad

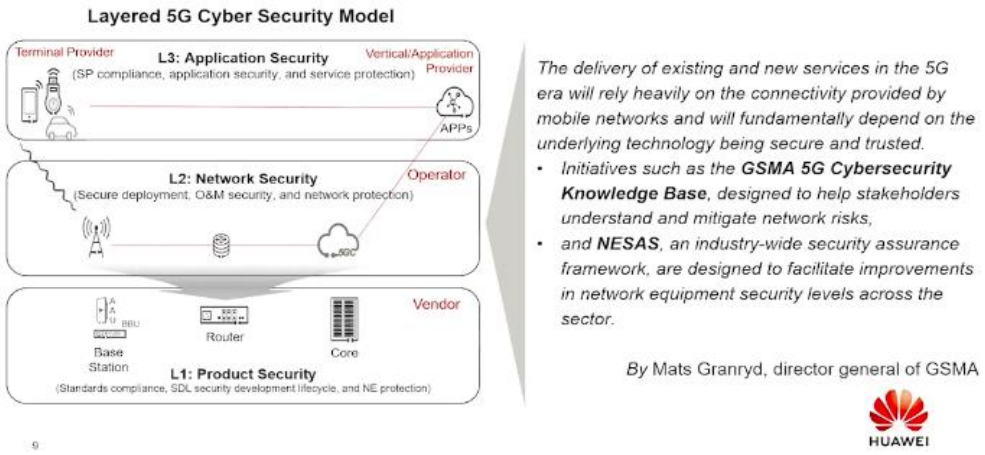
La charla impartida por el director de ciberseguridad de Huawei, John Suffolk, se centró en las prácticas internacionales que se pueden adoptar en el ámbito de la ciberseguridad. En el entorno actual globalizado, las amenazas, lejos de minimizarse, se encuentran en continuo aumento y ningún sistema es inmune. En la actualidad, existen tendencias globales como la sostenibilidad, la economía digital, las ciudades inteligentes y la creciente preocupación por la experiencia del consumidor.

Pero John Suffolk se preguntaba es si los gobiernos realmente están dispuestos a colaborar. Tal y como expuso durante la charla, la colaboración entre gobiernos es en ocasiones difícil, ya que algunos actúan como *hackers* de otros y viceversa. También explicó que los gobiernos tienen mucho por hacer para protegernos y, sin embargo, las mejoras en lugar de hacerlas de manera preventiva las realizan una vez el sistema ha fallado. Además, existen diferentes visiones con respecto al tratamiento de datos, algunos países consideran que estos deben ser protegidos mientras que otros creen que son esenciales para maximizar beneficios.

Con respecto a la IA, Suffolk afirmó que es un área que está avanzando de manera muy exitosa y sin embargo la regulación y la seguridad no le siguen el ritmo. Por tanto, explicó, para protegerse de las amenazas, es esencial adoptar un enfoque de "*Cero confianza*" por todas las partes implicadas en el proceso: “La ciberseguridad siempre ha sido una responsabilidad compartida por todas las partes y debe ser gestionada a través de **estándares comunes, incluso aunque no exista confianza mutua entre determinados gobiernos”.** Para ello, las organizaciones internacionales jugarán un papel importante y se deberá asegurar que se cumple con un proceso como el siguiente:

Con respecto a las empresas, se mostró partidario de que adopten un enfoque de **confianza cero,** que deberá implantarse en todos los niveles de la organización y en todas las tecnologías internas. Para ello, Suffolk explicó el modelo denominado “Layered 5G Cybersecurity Model”, que se puede observar en el siguiente esquema:

LAYERED 5G CYBERSECURITY MODEL



La principal conclusión que se puede obtener es que se deberá trabajar en implantar estándares comunes a nivel internacional siempre desde un enfoque de confianza cero en que deberán estar implicadas todas las partes de proceso.

Confianza cero: barreras, beneficios y cómo evitar errores

En esta conferencia, impartida por el vicepresidente de LogRhythm Labs, Andrew Hollister, se siguió tratando la temática de confianza cero. Para ello, el ponente compartió los éxitos y fracasos de su experiencia personal en la empresa LogRhythm Labs.

Tal y como explicó Hollister, LogRhythm Labs es una plataforma que implementa sistemas de seguridad ante las ciberamenazas. Para ello, proporciona una plataforma completa con la última funcionalidad de seguridad, incluyendo analítica de seguridad; detección y respuesta de red (NDR); análisis de comportamiento de usuarios y entidades (UEBA); y orquestación, automatización y respuesta de seguridad (SOAR).

3. Conclusiones

Durante la Singapore International Cyber Week se ha puesto de manifiesto el auge de nuevas amenazas en materia de ciberseguridad como los ataques de ransomware, las brechas de seguridad en dispositivos IoT, cadenas de suministro y dispositivos OT. Además de amenazas prácticamente imposibles de detectar como los *Zero Day Attacks*. Asimismo, se han identificado distintas oportunidades para la oferta española y áreas de mejora a nivel global relacionadas con:

3.1. Oportunidades para la oferta española

- **Ciberanalítica basada en Inteligencia Artificial (IA)**: Los avances que más destacan en este campo son los relacionados con machine learning y detección de amenazas basadas en la evidencia empírica pasada.
- **Análisis, identificación y mitigación de amenazas en el ámbito de la defensa de las cadenas de suministro**
- **Colaboración público-privada:** Distintas fuentes gubernamentales han manifestado la necesidad de una colaboración con el sector privado para afrontar los retos que plantea el panorama actual en materia de ciberseguridad. Es especialmente interesante el **Cyber Security Industry Call for Innovation** de CSA, programa que fomenta el desarrollo de nuevas soluciones de ciberseguridad.
- ***Cyber insurance***: ganan popularidad en el ámbito de la ciberseguridad los ciberseguros. Cada vez más necesarios frente al auge de los ataques ransomware, especialmente ligados al pago del rescate e, incluso, el asesoramiento legal y reputacional.
- **Seguridad y trazabilidad de la cadena logística**: es necesario asegurar la cadena logística para blindar el acceso a los dispositivos durante su transporte y manipulación y evitar la implantación de cualquier tipo de malware o software infeccioso.

3.2. Áreas de mejora en el ecosistema de ciberseguridad local

- **Cooperación internacional y sistemas para compartir datos:** con el fin de detectar y evitar ciberataques.
- **Estandarización de criterios y procesos de certificación de productos**: para facilitar la comercialización de los nuevos avances tecnológicos al mismo tiempo que se garantiza la seguridad y adecuación de los nuevos productos.
- **Formación de personal especializado en ciberseguridad**
- **Concienciación colectiva y educación de los consumidores y trabajadores:** destacó la presentación del SG Cyber Safe Partnership Programme, con el doble objetivo de fomentar

la concienciación dentro del tejido empresarial singapurense e impulsar la formación en ciberseguridad de los trabajadores locales.

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

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

Para buscar más información sobre mercados exteriores siga el enlace

www.icex.es

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, COMERCIO Y TURISMO
ICEX España Exportación e Inversiones