Universidad de San Andrés

Escuela de Negocios

Maestría en Gestión de Servicios Tecnológicos y de Telecomunicaciones

Ciberseguridad para impulsar la competitividad empresarial

Alumno: Arnaud Nguyen

Mentor: Enrique Hofman

Año 2023

Agradecimientos

Quisiera expresar mi profunda gratitud a todas las personas que han contribuido a la realización de esta tesis. Su apoyo, consejo e inspiración han sido de suma importancia a lo largo de este viaje académico.

Quisiera expresar mi más sincero agradecimiento a Enrique Hofman como director del máster y tutor de la tesis. Su experiencia, su capacidad docente y sus valores humanos han sido claves para el desarrollo de este trabajo.

También quiero agradecer a todas las personas que me han acompañado en la Universidad de San Andrés, a todos los profesores y alumnos que me han permitido desarrollar y compartir sus conocimientos. Ellos han hecho posible esta investigación brindando recursos, un ambiente propicio para el aprendizaje y oportunidades de desarrollo.

También quiero agradecer a todas las personas que me han apoyado en ESCP. El aprendizaje y los encuentros que he tenido han dado forma a mi pensamiento y a mis métodos de trabajo.

Esta tesis no habría sido posible sin la dedicación y el apoyo de todos y cada uno de ustedes. Gracias por su contribución.

Abstract

El desarrollo exponencial de las nuevas tecnologías de la información y la comunicación ha conducido a una dependencia total de los sistemas de información. Esta digitalización de nuestro mundo también ha provocado la aparición de numerosas vulnerabilidades en materia de ciberseguridad. Sin embargo, muchas empresas tienen dificultades para integrar la ciberseguridad y no consiguen implantar un nivel de seguridad aceptable. Además de ser esencial, la ciberseguridad puede contribuir a permitir un crecimiento exponencial.

El objetivo de este estudio es, por tanto, poner de relieve cómo influye la ciberseguridad en la competitividad sostenible de una empresa. Abordaremos este tema de forma cualitativa, basándonos en una recopilación de información, artículos y una entrevista.

Para comprender el impacto de la ciberseguridad en la competitividad de las empresas, es esencial analizar todo el ecosistema de la ciberseguridad aplicado a las empresas. A través de un enfoque económico y técnico, nos hemos dado cuenta de que hay muy poca demanda de soluciones de ciberseguridad por parte de las empresas, teniendo en cuenta los daños causados. Además, la complejidad de los ataques y de las defensas de ciberseguridad es muy compleja. Es una batalla técnica, estratégica y de gestión. Es mucho lo que está en juego para las empresas, que deben hacer de la ciberseguridad parte integrante de su estrategia. Para motivar e impulsar el cambio, tenemos que ser capaces de justificar los beneficios de la ciberseguridad para las empresas. Para que la ciberseguridad mejore la competitividad de una empresa, podemos identificar tres palancas principales de actuación: la propuesta de valor, el impulso del cambio hacia una cultura de la ciberseguridad y la gestión de la rentabilidad. Para ir más allá y comprender lo que realmente se está haciendo, vamos a comparar la ciberseguridad desde diferentes ángulos. Esto nos ayudará a elaborar un roadmap para ayudar a las empresas a integrar la ciberseguridad. Este roadmap será una guía adaptada a los

diferentes tipos de empresa y se basará en los frameworks utilizados por la mayoría de las empresas.

Introducción, problema y objetivos

La ciberseguridad es un concepto cada vez más importante en nuestra sociedad digital ultraconectada. Los avances tecnológicos en comunicación e información han creado numerosas oportunidades, pero estos avances también han aumentado la vulnerabilidad de las empresas. Hoy en día, los ataques informáticos son cada vez más numerosos y sofisticados. Como resultado, las empresas se enfrentan a retos nuevos y en constante evolución. La ciberseguridad ya no es una opción para las empresas, sino una necesidad si quieren sobrevivir.

Cuando hablamos de ciberseguridad, podemos referirnos a muchas cosas. Definir el nombre de ciberseguridad no es fácil. Si atendemos a una definición técnica, "la ciberseguridad es un subcampo de la seguridad de la información.Se trata de la información y de los sistemas de información que almacenan y procesan datos en formato electrónico, mientras que la seguridad de la información abarca la seguridad de todas las formas de datos".

El concepto de ciberseguridad encierra significados e implicaciones amplios y complejos para las distintas partes interesadas. La ciberseguridad consiste en garantizar que personas no autorizadas no puedan acceder a su información personal, protegiendo así su privacidad. También se trata de asegurarse de que sus dispositivos informáticos funcionan correctamente y están libres de malware.

Los objetivos de la ciberseguridad se pueden resumir con lo que llamamos la Tríada de la CIA. Representa la confidencialidad, la integridad y la accesibilidad (Hoffmann et al. 2020)

La confidencialidad se refiere a los esfuerzos de una organización por garantizar la confidencialidad y seguridad de los datos. Para lograr este objetivo, hay que controlar el acceso a la información para evitar su divulgación no autorizada, ya sea intencionada o no. Un elemento clave para mantener la confidencialidad es garantizar que las personas no autorizadas no puedan acceder a los activos vitales de su empresa. Al mismo tiempo, un sistema eficaz también garantiza que quienes necesiten acceder a esta información dispongan de la autorización necesaria.

La integridad es la garantía de que los datos son exactos y completos. Exactos significa que los datos no han sido alterados por ninguna parte no autorizada ni por ningún problema técnico. Integridad significa que los datos no han sido borrados por ninguna parte no autorizada ni por ningún problema técnico.

La accesibilidad es el seguro de la disponibilidad de la información. Significa que todos los sistemas utilizados para almacenar y analizar y todos los procesos de comunicación están disponibles y funcionan. La accesibilidad es una parte importante de la ciberseguridad. Una de las razones es que el mantenimiento de la accesibilidad requiere a menudo la participación de numerosos profesionales no especializados en ciberseguridad.

A las empresas les resulta difícil cumplir estos objetivos y alcanzar un alto nivel de seguridad. La implantación de soluciones requiere inversión, tiempo y personal cualificado. Además, para lograr una integración óptima, la estrategia de ciberseguridad debe desarrollarse y aplicarse a todos los niveles de la empresa. Ya sea a nivel de los responsables de la toma de decisiones o a nivel operativo, todo el mundo debe ser consciente de la ciberseguridad. Una transformación de este tipo en el seno de la organización tropieza inevitablemente con numerosos obstáculos.

Sin embargo, aplicar una estrategia de ciberseguridad eficaz puede ser beneficioso para las empresas. Les proporciona una ventaja competitiva frente a sus rivales.

Pregunta de investigación

Además de ser esencial, la ciberseguridad es buena para las empresas. A las empresas les interesa adoptar esta tecnología. En este estudio, respondemos a la siguiente pregunta:

¿Cómo la ciberseguridad influye en la competitividad sustentable de las empresas ?

Objetivo

El objetivo principal de este estudio es, por tanto, comprender y analizar cómo la integración de la ciberseguridad puede mejorar la estrategia empresarial.

De este objetivo se derivan los objetivos secundarios:

- Presentar el entorno, los actores y las tecnologías de la ciberseguridad en nuestra sociedad.
- Examinar las estrategias de crecimiento exponencial de las empresas para incorporar en ellas el concepto de ciberseguridad.
- Analizar los métodos de gestión del cambio y de transformación digital para facilitar la integración de la ciberseguridad
- Aportar argumentos concretos para animar a las empresas a interesarse e invertir en ciberseguridad
- Estudiar las mejores prácticas en ciberseguridad para crear una hoja de ruta de implantación de la ciberseguridad en las empresas

Metodología de investigación

Metodología

Este estudio se basa en un enfoque cualitativo. El objetivo de la investigación cualitativa es desarrollar conceptos que nos ayuden a comprender los fenómenos sociales en contextos naturales (y no experimentales), centrándose en los significados, experiencias y perspectivas de todos los participantes". (Mays y Pope, 1995). Basaremos nuestra investigación en la observación y la recopilación de información relacionada con la ciberseguridad y las estrategias empresariales. También añadiremos una entrevista con un empleado de una empresa tecnológica que ha sido víctima de un ciberataque. También describiremos y recurriremos a métodos cuantitativos desarrollados en artículos que enriquecerán este estudio. Parte del trabajo también puede considerarse exploratorio, ya que cruzamos los conceptos de estrategia y ciberseguridad. Por último, proponemos un roadmap que personalmente consideramos óptimo y que puede abrir nuevas perspectivas para la integración de la ciberseguridad en las empresas.

Justificación

La ciberseguridad de las empresas es una cuestión que debe abordarse por varias razones. En primer lugar, la ciberseguridad es necesaria hoy en día para mantener intacta nuestra privacidad. De hecho, es un derecho fundamental para muchas empresas. Por eso es importante que analicemos este tema desde una perspectiva tanto social como individual. Además, las consecuencias de un ciberataque pueden tener otras repercusiones de carácter financiero y jurídico, y pueden dañar la reputación de todos. Por último, aplicar una estrategia de ciberseguridad eficaz puede ser beneficioso para las empresas. También puede aumentar el crecimiento del negocio y mejorar la rentabilidad.

Por ello, contribuiremos a que las empresas comprendan mejor el concepto de ciberseguridad. Como parte de nuestro impulso de mejora, trataremos de orientar a las empresas hacia una mayor resiliencia y animar así a todas las empresas a asumir los retos de la ciberseguridad.

Estructura de la tesis

Este estudio se divide en 8 partes.

El capítulo 1 analiza la ciberseguridad en su conjunto. Antes de avanzar en nuestro estudio, es importante tener una comprensión global de la ciberseguridad. Para ello, examinaremos el mercado de la ciberseguridad, las amenazas y las herramientas de defensa de que disponen las empresas.

El capítulo 2 es un análisis estratégico. Estudiaremos cómo pueden beneficiarse las empresas del crecimiento exponencial. Debemos comprender las palancas, los parámetros y las ventajas de una estrategia de este tipo. Esto nos permitirá establecer el vínculo con la ciberseguridad.

El capítulo 3 es la continuación del estudio de la estrategia de crecimiento exponencial. Tratamos de integrar la ciberseguridad en la propuesta de valor para alcanzar este objetivo.

El capítulo 4 también presenta la ciberseguridad como palanca del crecimiento exponencial en términos de gestión del cambio e innovación.

El capítulo 5 propone métodos de seguimiento de la aplicación de la ciberseguridad mediante KPI. El objetivo es también demostrar el retorno positivo de la inversión en ciberseguridad.

El capítulo 6 es un punto de referencia de la ciberseguridad desde diferentes ángulos. En primer lugar, esta sección nos permite comprender la realidad de la ciberseguridad en nuestra sociedad. A continuación, podremos determinar cuáles son los actores que mejor aplican la ciberseguridad y, por tanto, quiénes pueden beneficiarse de este crecimiento exponencial.

El capítulo 7 continúa el estudio y propone un roadmap para implantar la ciberseguridad en las empresas.

El capítulo analiza el futuro de la ciberseguridad en los próximos 5 a 10 años.

I. Panorama de la ciberseguridad

El mercado

La ciberseguridad ocupa un lugar cada vez más importante en las empresas. El desarrollo de las comunicaciones y la importancia de la gestión de datos han puesto de actualidad las cuestiones de seguridad informática. Hoy en día, prácticamente todas las empresas están vinculadas a la seguridad informática. En consecuencia, la demanda de productos y servicios seguros debe ser elevada.

Según mordor intelligence, el mercado mundial de la ciberseguridad tendrá un valor de 132.000 millones de dólares en 2021. Además, este mercado crecerá en los próximos años. Se prevé un fuerte crecimiento, con un CAGR del 14,1%. El mercado se está viendo estimulado por una serie de razones:

- el creciente número de ataques
- las numerosas normativas impuestas por los gobiernos
- la crisis COVID19 ha incrementado significativamente el teletrabajo, abriendo nuevas vulnerabilidades de seguridad
- la necesidad de soluciones de gestión de identidades
- el aumento del número de dispositivos conectados

Si nos fijamos en las previsiones de mercado publicadas por Statista para 2023, podemos ver el enorme potencial del mercado de la ciberseguridad.

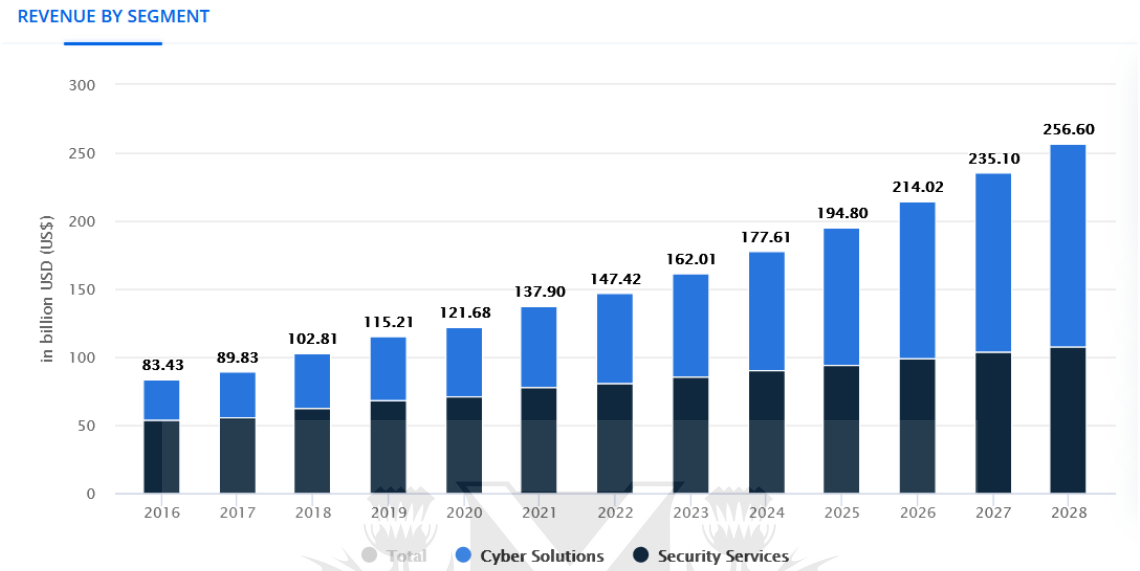


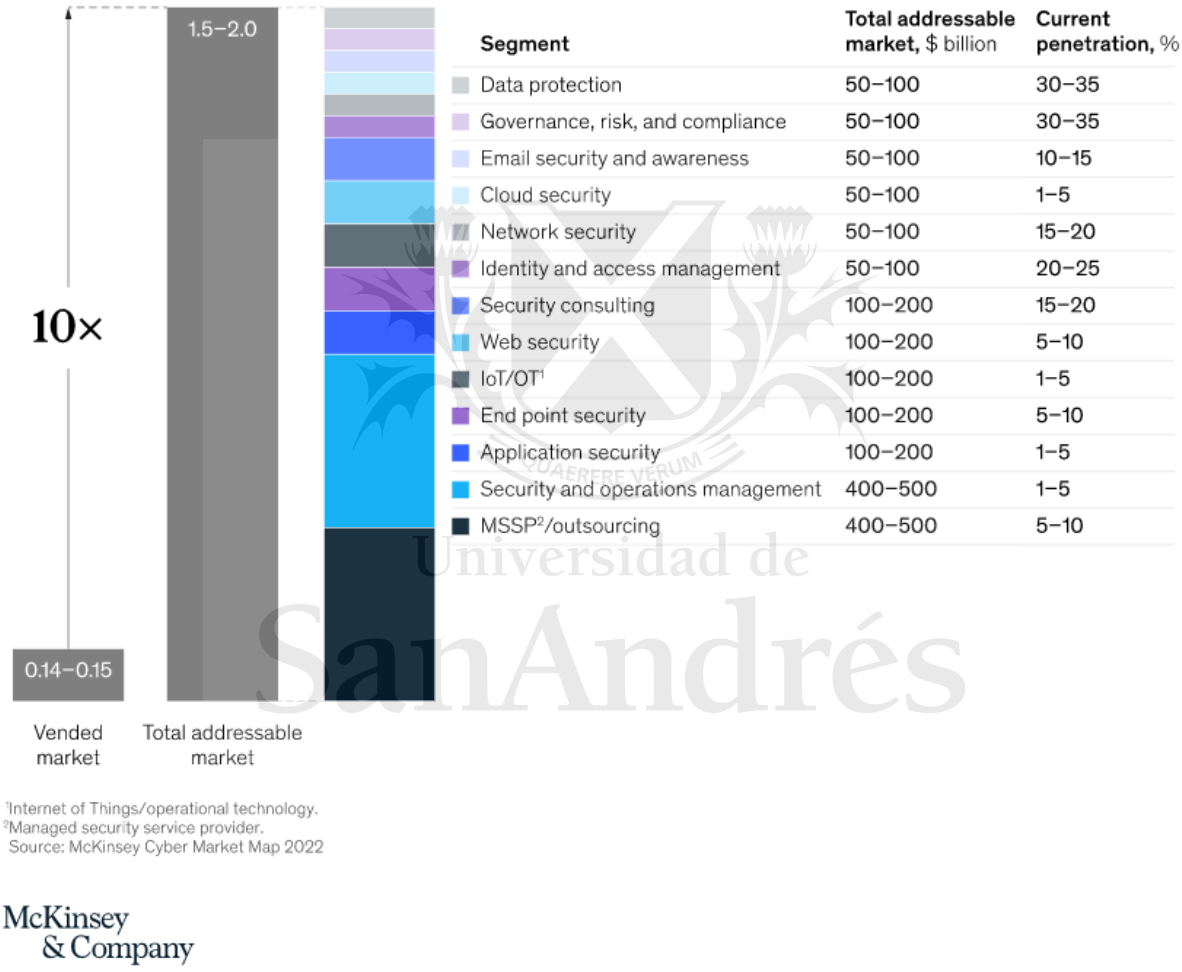
Figura 1. Ingresos en el mercado de la ciberseguridad

Vemos que la cuota de mercado mundial aumentará en unos cien mil millones de dólares en los próximos cinco años. Además, tenemos más información sobre los ingresos por segmentos. Se prevé que los servicios de ciberseguridad aumenten ligeramente, mientras que las soluciones cibernéticas crecerán con fuerza.

Esta tendencia creciente en el mercado de la ciberseguridad también se ve confirmada por un estudio publicado por Mckinsey en 2022 (Aiyer et al. 2022).

Los daños causados por los ciberataques son cada vez mayores. En 2025, podrían ascender a más de "$10.5 trillion", lo que supone un aumento del 300% con respecto a 2015. De hecho, se prevé que los grupos maliciosos y el malware aumenten considerablemente cada año. Sin embargo, las soluciones existentes en el mercado no satisfacen plenamente la demanda generada por esta amenaza creciente en términos de servicio, automatización y soluciones. Por ello, el mercado potencial se estima entre “1.5 to 2 trillion” de dólares. Esto no significa que el mercado vaya a alcanzar este

tamaño en un futuro próximo, pero subraya la importancia y el potencial de la ciberseguridad. También es un buen indicador de la diferencia entre las pérdidas financieras causadas por los ataques y la escasa demanda de protección por parte de las empresas.



Segment	Total addressable market, $ billion	Current penetration, %
Data protection	50–100	30–35
Governance, risk, and compliance	50–100	30–35
Email security and awareness	50–100	10–15
Cloud security	50–100	1–5
Network security	50–100	15–20
Identity and access management	50–100	20–25
Security consulting	100–200	15–20
Web security	100–200	5–10
IoT/OT[1]	100–200	1–5
End point security	100–200	5–10
Application security	100–200	1–5
Security and operations management	400–500	1–5
MSSP[2]/outsourcing	400–500	5–10

[1]Internet of Things/operational technology.
[2]Managed security service provider.
Source: McKinsey Cyber Market Map 2022

McKinsey & Company

Figura 2. Tamaño del mercado mundial de la ciberseguridad 2021

Las amenazas

Cuando hablamos de ciberseguridad, podemos identificar a los actores que tienen malas intenciones. Sus objetivos sirven a sus intereses personales e intentarán piratear para robar, manipular, influir o destruir. Los hackers con malas intenciones se conocen como hackers de sombrero negro.

Los hackers y piratas cibernéticos profesionales pueden dividirse en diferentes categorías.

Pueden ser entidades gubernamentales, espías corporativos, delincuentes o hacktivistas. Los hacktivistas utilizan métodos de pirateo para transmitir sus ideas y tener un impacto sociopolítico.

.

También hay riesgos que no son de piratería informática. Puede haber vulnerabilidades que dependan de factores externos, como catástrofes naturales, atentados o, como vimos con Covid19, pandemias.

Un incendio en un centro de datos podría hacer imposible el acceso a los datos o a una red. Este tipo de riesgo subraya la importancia de que las empresas dispongan de políticas de copia de seguridad, backup, en caso de pérdida de datos.

La pandemia que vivimos en 2020 perturbó las infraestructuras de las redes digitales, impidiendo a ciertos profesionales del mantenimiento mantener las operaciones.

Para comprender bien las implicaciones financieras de un ataque hacker, es importante entender cómo se las arreglan los hackers para ganar dinero (Joseph 2022, p. 76). Entre los diversos métodos para obtener dinero de usuarios o empresas, los hackers disponen de cuatro métodos de monetización:

-fraude financiero directo

-fraude financiero indirecto

-Ransomware

-Cryptominers

El fraude financiero directo consiste en obtener dinero directamente de los usuarios. Un hacker puede utilizar diversas técnicas para averiguar los datos personales de un usuario con el fin de recuperar dinero o comprar bienes y servicios a costa de otro usuario.

El fraude financiero indirecto adopta muchas formas, como la reventa de información confidencial, el robo de artículos mediante el secuestro de direcciones de entrega o el robo de datos de tarjetas de crédito y su posterior envío a la darkweb sin llegar a realizar directamente transacciones fraudulentas.

El ransomware es un programa informático que cifra los datos de un ordenador o espacio de almacenamiento. Como resultado, todos los datos dejan de ser accesibles para los usuarios que tenían privilegios sobre ellos. A continuación, se muestra un mensaje en el ordenador en el que se pide el pago de una determinada cantidad de dinero antes de una fecha concreta, sino se borrarán todos los datos pirateados. El uso de ransomware ha aumentado considerablemente con el incremento del almacenamiento de datos digitales.

Existen dos tipos de ransomware, el locker ransomware y el crypto ransomware. El Locker ransomware bloquea tu ordenador. En otras palabras, el usuario no podrá utilizar el ordenador con normalidad, por ejemplo, no podrá escribir ni mover el ratón. El usuario sólo podrá pagar el rescate.

El cripto ransomware no restringirá la funcionalidad del ordenador, pero imposibilitará el acceso a determinados datos. Por tanto, se pedirá al usuario que pague antes de borrar los datos. En otras palabras, cuanto más importantes sean los datos para el usuario, más dispuesto estará a pagar por ellos.

Los criptomineros son programas informáticos que utilizan la potencia de cálculo de determinados dispositivos. Al infectar y secuestrar las máquinas de los usuarios, los hackers pueden minar criptomonedas. En otras palabras, la potencia de cálculo de una

máquina y la energía utilizada para hacer funcionar estas máquinas generarán ingresos en criptodivisas que serán recaudados por el hacker.

Además de estos riesgos, las empresas corren riesgos jurídicos. Existe un entorno jurídico para proteger todas las actividades de los sistemas de información y comunicación. El incumplimiento de las leyes establecidas en cada país expone a las empresas a riesgos legales relacionados con la ciberseguridad. Hoy en día, muchas empresas están obligadas a declarar públicamente si sospechan que se ha producido una brecha.

En 2018, la Unión Europea introdujo el GDPR, el Reglamento General de Protección de Datos, que se aplica a todas las empresas de la zona. Las empresas tienen responsabilidades en materia de protección de datos de sus usuarios. El incumplimiento de estas normas puede acarrear sanciones económicas muy cuantiosas y también puede dañar la reputación de la empresa.

También existen normativas diferentes para los distintos sectores. En el sector de la salud, los datos de los pacientes deben ser confidenciales. En Estados Unidos, las empresas sanitarias están sujetas a la HIPAA (Joseph 2022, p. 76).

Dada la complejidad del entorno legal, cada empresa debe averiguar cuáles son sus obligaciones, en función de sus actividades y su sector.

Herramientas de defensa

Protección de datos

La protección de datos se basa en los principios de confidencialidad, integridad y accesibilidad (CIA) mencionados anteriormente. Para reducir los riesgos y aumentar la protección de los datos, pueden aplicarse las siguientes buenas prácticas:

- una buena gestión de los privilegios, es decir, que los datos sólo sean accesibles para quienes deban utilizarlos
- cifrar los datos para que, incluso en caso de robo o piratería, el pirata no pueda descifrarlos sin la clave de descifrado
- borrar los datos que ya no se utilizan y eliminarlos del sistema.
- la resiliencia de los datos implica la realización de copias de seguridad en caso de pérdida o robo de datos

Gobernanza, Riesgo y Cumplimiento

Gobernanza, riesgo y cumplimiento (GRC) en ciberseguridad es el conjunto de decisiones estratégicas aplicadas para proteger a la organización, gestionar los riesgos y garantizar el cumplimiento de la normativa más reciente.

- La gobernanza reúne todas las estrategias y procesos que se definirán para alcanzar los objetivos de seguridad. Por ejemplo, la empresa puede decidir llevar a cabo una auditoría de seguridad, o puede decidir crear una unidad dedicada a la ciberseguridad dentro de la propia organización.
- La gestión de riesgos permite prever y anticipar los puntos débiles de la empresa. Es necesario conocer el entorno y la exposición a los riesgos. Esto permite evaluar y enumerar los puntos débiles y las pérdidas potenciales.
- El cumplimiento es la observancia adecuada de las políticas y procedimientos de la empresa, así como de las leyes y reglamentos. Además, el cumplimiento y la gestión adecuada de estos tres pilares pueden ser necesarios para lograr la conformidad con determinados frameworks de ciberseguridad.

Seguridad del e-mail

La seguridad del e-mail también implica preservar la confidencialidad, integridad y accesibilidad (CIA) de los correos electrónicos. Esto significa protegerse contra los ataques de phishing y los programas maliciosos adjuntos a los correos electrónicos. Para protegerse, se pueden utilizar filtros antispam.

Además, es necesaria la educación dentro de la empresa para evitar caer en la trampa de ciertos ataques.

Seguridad en la nube (Cloud)

La nube permite acceder a distancia a recursos de almacenamiento, bases de datos y programas informáticos (What is Cloud Security ? Cloud Security Defined | IBM). Muchas empresas están optando por estas nuevas soluciones en lugar de tener su propia infraestructura de red in situ. Las empresas de la nube ofrecen diversas soluciones, entre ellas algunas de las más conocidas:

IaaS (Infrastructure-as-a-Service) es un enfoque híbrido en el que la empresa gestiona el middleware y las aplicaciones, y el proveedor de la nube gestiona los servidores, el almacenamiento y la red.

PaaS (Platform-as-a-Service) proporciona a las empresas un framework de aplicaciones que gestiona automáticamente los sistemas operativos, las actualizaciones de software y el almacenamiento.

SaaS (Software-as-a-Service) proporciona una aplicación en nube a través de Internet.

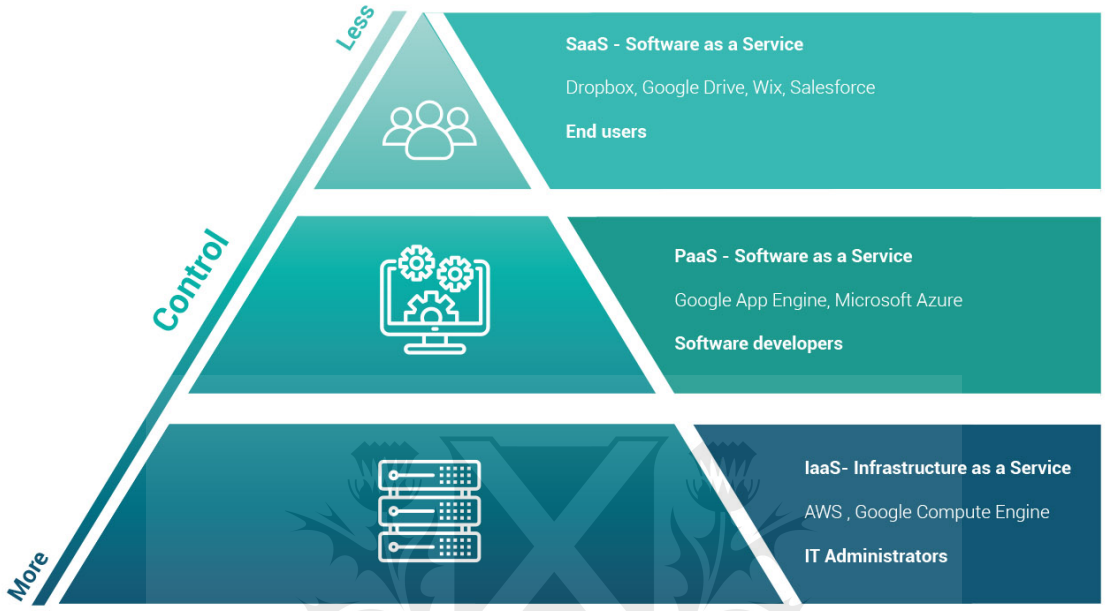


Figura 3. Esquema de las diferentes ofertas de la nube

Como resultado, se han producido muchas migraciones a estas tecnologías de nube. Aunque los proveedores son responsables de la gestión de la infraestructura, no son necesariamente responsables de la gestión global de la seguridad de los datos. Tal y como presenta IBM, son varios los retos a los que se enfrentan las empresas.

Network security

La seguridad de las redes es una parte esencial de la seguridad informática. Protege los dispositivos conectados a una red y los datos que circulan por ella. Para garantizar la seguridad de la red, hay que utilizar las tecnologías adecuadas. Hay tres aspectos diferentes en la seguridad de las redes (What is Network Security ?, Forcepoint): la seguridad física de las redes, la seguridad técnica de las redes y la seguridad administrativa de las redes. El objetivo de la seguridad física es impedir el acceso no autorizado a los componentes de la red. La seguridad técnica tiene por objetivo

proteger los datos accesibles a través de la red. Debe proteger contra el personal no autorizado y también contra las actividades malintencionadas de los empleados de una empresa. Por último, la seguridad administrativa consiste en establecer políticas y niveles de acceso de los usuarios a los servicios e infraestructuras.

Los distintos productos desarrollados para garantizar la seguridad de la red incluyen firewalls, sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS) y virtual private network (VPN).

Además, existen protocolos y políticas para conceder acceso a la red. Es lo que se conoce como control de acceso a la red.

La seguridad de las redes evoluciona constantemente. Por eso es importante que las empresas se mantengan al día de las últimas tecnologías para mantener un nivel óptimo de seguridad.

Identity and access management (IAM)

También conocido como IAM, Identity Access Management se utiliza para gestionar la identidad de los usuarios dentro de una empresa. Esto se aplica tanto a los empleados como a los clientes. Un sistema de gestión de identidad y acceso debe permitir controlar la identidad de todos. La identidad debe ser única, controlada y actualizada (Ishaq Azhar Mohammed, 2019).

Hay dos partes: identidad y acceso. Cuando hablamos de identidad, nos referimos a toda la información que permite reconocer a un individuo. Esta identidad se asignará al usuario cuando utilice los recursos de la empresa.

Cuando hablamos de accesibilidad, nos referimos a los permisos que se conceden a una identidad, como lectura, escritura o ejecución.

Web security

La seguridad web consiste en proteger todas las actividades accesibles a través de Internet. Al ser generalmente públicas, todas las actividades de los usuarios están

expuestas a numerosas vulnerabilidades. La seguridad de la Web también incluye otras ramas de la ciberseguridad, como la "Identity Access Management" (IAM) y la seguridad del correo electrónico.

En la web se utilizan numerosos protocolos para que las máquinas puedan comunicarse entre ellas. Los protocolos más conocidos son HTTP/HTTPS. Con la certificación SSL/TLS, el cifrado de los datos que circulan por la web garantiza un cierto nivel de seguridad.

También es importante sensibilizar a los usuarios sobre las buenas prácticas y asegurarse de que todos los usuarios actualizan sus aplicaciones.

Por último, también son muy frecuentes y conocidos los ataques en la Web. Hablamos del Dos, denial of service (denegación de servicio), que consiste en sobrecargar un servidor para dejarlo sin servicio. También son frecuentes los ataques de inyección SQL. Las inyecciones son el uso de vulnerabilidades para infiltrarse en una base de datos. Normalmente, los usuarios pueden interactuar con un sitio web vinculado a una base de datos. Si la aplicación no está bien diseñada, un usuario malintencionado puede añadir nuevas "requests" y tomar el control total o parcial de un sistema. Estos ataques crecen rápidamente y surgen nuevas vulnerabilidades con el desarrollo de BOTs y ChatGPT.

The Internet of Things (IoT)

La "Internet of Things" cubre un gran número de sectores y tiene muchas aplicaciones. Conecta las cosas entre sí e intenta que todo sea más inteligente. Todo el IoT está adquiriendo una mayor integración en nuestra sociedad y en nuestra vida.El desarrollo de nuevas tecnologías de comunicación favorece la aparición del IoT. Cada vez se crean más datos que transitan por la red. Según el diccionario Oxford, IoT es "La interconexión a través de Internet de dispositivos informáticos integrados en objetos cotidianos, lo que les permite enviar y recibir datos".

Según la empresa Fortinet, existen tres enfoques principales para la seguridad IoT

- Conocer: con una visibilidad total de la red, las soluciones de seguridad pueden autenticar y clasificar los dispositivos IoT según un perfil de riesgo asignado a un grupo de estos dispositivos.
- Segmentar: una vez que la empresa conoce la superficie de ataque de IoT, los dispositivos IoT pueden segmentarse en grupos gobernados por reglas en función de sus perfiles de riesgo.
- Proteger: los grupos de IoT gobernados por políticas y la segmentación de la red interna permiten la supervisión basada en actividades, la inspección y la aplicación de políticas en diferentes perímetros de la infraestructura.

Endpoint security

La seguridad de los Endpoints implica proteger todos los dispositivos finales. Esto incluye todos los ordenadores, tabletas, teléfonos móviles, dispositivos IoT e impresoras. Todos estos dispositivos son puertas de entrada a la red a la que están conectados.

Juntos, estos subdominios de ciberseguridad ayudan a proteger las distintas partes vulnerables de una organización. Para tener un enfoque estructurado y coherente de la gestión de los riesgos de ciberseguridad, existen frameworks a seguir. Entre los frameworks más conocidos está el del Instituto Nacional de Estándares y Tecnología (NIST). Este framework se basa en cinco pilares: identificación, protección, detección, respuesta y recuperación. Igualmente, existe la organización internacional de normalización IOS que establece normas internacionales para mejorar la seguridad de la información. En materia de ciberseguridad, entre ellas figuran ISO 27001 e ISO 27002.

II. El impacto de la ciberseguridad en la competitividad empresarial

Las mayores empresas innovadoras que conocemos hoy en día, como Amazon, Apple, Ebay, Google y otras, han conseguido aplicar una estrategia de crecimiento exponencial. Cuando hablamos de crecimiento exponencial, nos referimos a un aumento muy acusado del volumen de negocio en un periodo de tiempo limitado. Este crecimiento es rápido y puede ser difícil de gestionar.

Todas las empresas tienen interés en beneficiarse de este crecimiento exponencial para desarrollarse en su mercado y ser competitivas. Para alcanzar este objetivo de crecimiento, las empresas necesitan adoptar la estrategia adecuada y, una vez puesto en marcha este proceso, la estrategia debe permitir a la empresa capitalizar sus ganancias para mantenerse en el tiempo.

Hay muchas maneras de lograr una competitividad sostenible. Hay palancas importantes para aplicar esta estrategia. Entre estas palancas hay tres elementos en los que la ciberseguridad puede ayudar a mejorar la estrategia de una empresa para lograr una mayor competitividad y un crecimiento exponencial (Thomson, 2005).

La ciberseguridad puede mejorar la propuesta de valor, formar parte de la cultura de innovación de una empresa, y tener un crecimiento exponencial.

Según el estudio de Cisco (2016), el sesenta y nueve por ciento de los encuestados sigue considerando que el objetivo principal es la reducción de riesgos. Mientras que el treinta y uno por ciento de los encuestados cree que el objetivo principal de la ciberseguridad es el crecimiento.

Hemos investigado la ciberseguridad en su conjunto. Hemos presentado una base de conocimientos sobre ciberseguridad desde diferentes puntos de vista. Hemos

respondido a las primeras preguntas generales, es decir, qué es la ciberseguridad y cuáles son sus objetivos. Analizamos el mercado y su potencial futuro. Analizamos el ecosistema de la ciberseguridad, presentando los riesgos y los productos disponibles. Esta investigación nos permitió comprender el entorno de la ciberseguridad. Además, a través de este estudio preliminar pudimos identificar varios puntos importantes:

- Dado el gran número de ataques y los daños causados, debería haber mucha más demanda por parte de las empresas en el mercado de la ciberseguridad. Hay una falta de inversión en este sector.
- Los ataques y las defensas en materia de ciberseguridad son muy complejos. Es una batalla técnica, estratégica y de gestión.

Estas dos cuestiones exigen que se preste mayor atención a la ciberseguridad. Es mucho lo que está en juego para las empresas, que deben hacer de la ciberseguridad parte integrante de su estrategia. Para motivar e impulsar el cambio, tenemos que ser capaces de justificar los beneficios de la ciberseguridad para las empresas.

Para ello, vamos a entender cómo influye la ciberseguridad en la competitividad sostenible de las empresas.

Para justificar una inversión y una estrategia, es necesario demostrar los beneficios y el rendimiento de la inversión. Si estuviera claro que la ciberseguridad tiene un retorno de la inversión positivo, las empresas ya habrían adoptado todas la ciberseguridad. Sin embargo, es difícil establecer y cuantificar claramente su impacto en la empresa.
A continuación, examinaremos las palancas disponibles que influyen en estos indicadores y permiten a las empresas beneficiarse de una competitividad sostenible en su mercado.
Buscamos integrar la ciberseguridad en las estrategias de crecimiento exponencial. Para garantizar que la ciberseguridad mejore la competitividad de las empresas, podemos identificar tres palancas principales de actuación:

- Propuesta de valor
- Impulsar el cambio hacia una cultura de ciberseguridad
- Gestión de la rentabilidad

Durante este estudio, también queremos examinar los límites y las diferentes formas de medir los beneficios de la ciberseguridad para una empresa.

III. Propuesta de valor

La propuesta de valor es el primer paso clave. La propuesta debe ofrecer algo único, y esto puede lograrse de varias maneras. Implica proponer un producto o servicio que sea revolucionario dentro de su mercado.

Para construir una propuesta de valor correctamente, hay que seguir varios pasos y realizar una serie de análisis. Hay seis pasos importantes para construir esta propuesta (6 pasos para crear una propuesta de valor, 2021):

1. Definir el cliente ideal
2. Identificar el problema que se quiere abordar
3. Determinar las ventajas de la oferta frente a la competencia
4. Proponer una solución clara y única
5. Validar la propuesta de valor y los supuestos
6. Expresar la propuesta de valor

Así pues, vamos a analizar cada una de estas etapas para ver qué papel puede desempeñar la ciberseguridad en la mejora de la propuesta de valor y permitir así a las empresas ser más competitivas.

Definir el cliente ideal

Necesita estudiar diversos parámetros y características de sus clientes. Para ello, debe estudiar y crear un perfil de sus clientes potenciales. En marketing, esto se conoce como Buyer Persona, un perfil semi-ficticio de un cliente ideal. Esto permite obtener el máximo número de clientes potenciales que tienen más probabilidades de comprar el producto o servicio. Por tanto, es necesario establecer los perfiles tipo. A continuación, hay que establecer la personalidad, los temas y los problemas de estos perfiles. Por último, hay que estudiar su comportamiento, sobre todo en línea y en las redes. De este modo, se podrá adoptar un enfoque más personalizado para cada cliente

potencial, ahorrando tiempo y aumentando el impacto.

Por lo tanto, será importante para una empresa identificar los perfiles que son o no sensibles a la ciberseguridad. Por lo tanto, durante las campañas de marketing, puede ser una buena idea destacar la estrategia de seguridad de la empresa en relación con su oferta o producto.

Identificar el problema que debe abordarse

Podemos identificar dos categorías de problemas a los que podemos responder. Puede tratarse de un problema funcional o de un problema emocional. El problema puede abordarse de tres maneras diferentes (Thomson, 2005):

-Creando un nuevo mercado,

-Redefinir un mercado

-Optimizar un mercado

Cuanto más pueda una empresa pasar de lo funcional a lo emocional, más clientes tendrá. Esto le permitirá crear una base sólida de clientes fieles.

El lado funcional de la ciberseguridad es innegable, pero es más difícil apelar a las emociones cuando se trata de esta tecnología. Por regla general, las emociones asociadas a la ciberseguridad son negativas. El estudio de Renaud et al, 2021, muestra que los usuarios tienen cuatro veces más emociones negativas que positivas sobre estas tecnologías. La inseguridad y lo desconocido son las emociones más recurrentes ante una ciberseguridad desconocida y compleja. El estudio afirma que "si los usuarios se sienten inseguros sobre qué información o consejo seguir, de entre la plétora de consejos disponibles, o si se sienten abrumados por la cantidad de información, esto podría influir negativamente en su compromiso con los temas de ciberseguridad" y "los planteamientos sugieren que las personas con miedos relacionados con la ciberseguridad, o las personas que relacionan un tema con el estrés y la frustración basándose en condicionamientos previos, no se comprometerán constructivamente con

un tema, sino que lo evitarán o incluso se abstendrán de utilizar las nuevas tecnologías."

Este problema es obviamente uno de los principales obstáculos para la integración de la ciberseguridad. Esto subraya la importancia de sensibilizar al personal a todos los niveles de la organización.

Además, para sacar partido de estos problemas, las empresas tienen todo el interés en sensibilizar a los clientes sobre los riesgos y las soluciones seguras. Es necesario un cambio en la forma de percibir esta tecnología. Hay que pasar de emociones de miedo y ansiedad a emociones de necesidad, curiosidad e interés.

Identificar las ventajas de la oferta frente a la competencia

Análisis del mercado

Es importante que las empresas conozcan el mercado en el que operan. Conocer su mercado tiene muchas ventajas.

La definición del cliente ideal variará mucho en función del sector empresarial. Una empresa que venda productos alimentarios no tendrá los mismos requisitos que un banco en materia de ciberseguridad. Hay que conocer las expectativas del mercado. Esto será específico de los distintos sectores empresariales. La mayor demanda de ciberseguridad se da en los sectores bancario, sanitario, informático y manufacturero. En estos sectores, la ciberseguridad tendrá el máximo impacto como palanca para lograr un crecimiento exponencial. Por lo demás, los demás sectores de actividad están muy poco expuestos a los riesgos de ciberataque. Por lo tanto, será imposible destacar la ciberseguridad en la propuesta de valor. Más adelante en el estudio, examinaremos más de cerca los diferentes sectores de la ciberseguridad.

El primer paso es comprender el entorno. Para ello se pueden utilizar los análisis PESTEL, político, económico, sociológico, tecnológico, medioambiental y jurídico. En el

contexto de la ciberseguridad, es importante comprender este entorno, sobre todo en lo que se refiere a los aspectos tecnológicos y jurídicos. Debe ser capaz de integrar estos factores en su estrategia de ciberseguridad para evitar tomar decisiones estratégicas equivocadas.

Podemos resumir esta situación utilizando el modelo DAFO. Esto nos dará una visión global de la situación de la empresa, así como de las amenazas y oportunidades de su entorno macroeconómico. Este análisis también nos permite establecer la mejor estrategia empresarial posible, transformando las debilidades en fortalezas y explorando las oportunidades sin dejar de tener en cuenta las amenazas potenciales. La ciberseguridad entrará inevitablemente en una de estas categorías: puntos fuertes, puntos débiles, oportunidades y amenazas. Por lo tanto, será cuestión de ajustar la estrategia para convertirla en un activo.

Para terminar, el modelo de las cinco fuerzas de Porter es una herramienta importante para entender las principales fuerzas competitivas de un sector. Puede ayudarle a evaluar el atractivo de un sector y a señalar las áreas en las que puede ajustar su estrategia para mejorar la rentabilidad.
El análisis se basa en los siguientes 5 ejes: intensidad de la competencia, poder de negociación de los clientes, poder de negociación de los proveedores, amenaza de nuevos participantes y amenaza de sustitutos.

Crear una ventaja competitiva

En su mercado, las empresas compiten con otras empresas. Cada empresa trata de mantener su actividad en su mercado para sobrevivir, crecer y prosperar. Las empresas deben encontrar formas a corto y largo plazo de distinguirse de sus competidores y recuperar la mayor cuota de mercado posible. Para lograr una competitividad sostenible, las empresas deben responder a los desafíos del mercado y centrar su

estrategia en distintos tipos de ventajas competitivas. Por tanto, deben identificar y trabajar en su ventaja competitiva. (¿Qué es una ventaja competitiva?, 2022)

Existen tres ventajas competitivas:

- Una ventaja de costes: le permite diferenciar sus precios de los de otras empresas. Puede posicionarse muy alto o muy bajo en términos de precio para resultar muy atractivo a sus clientes. Para conseguirlo, las empresas deben controlar sus costes, lograr economías de escala o aprovechar las sinergias.
- Una ventaja desde el punto de vista de la oferta: necesita ofrecer un producto o servicio que destaque entre la multitud. Necesita un valor añadido que no ofrezcan sus competidores. Esta diferenciación puede ser objetiva o subjetiva. Puede ofrecer características diferentes o puede ser percibido de forma diferente y, por tanto, utilizar su imagen de marca.
- Una ventaja en activos intangibles: es la ventaja más difícil de identificar. Incluye los conocimientos técnicos, la propiedad intelectual, las patentes y el capital humano.

Las empresas pueden utilizar la ciberseguridad como ventaja competitiva. Según el estudio realizado por Cisco (2016), el cuarenta y cuatro por ciento considera que la ciberseguridad es una ventaja competitiva para su organización Existen tres ventajas competitivas para las empresas (Kosutic, 2021).

En primer lugar, la ciberseguridad ayuda a proteger una ventaja competitiva existente. Si la actividad de una empresa sufre un ataque, las operaciones pueden detenerse total o parcialmente. La ventaja competitiva ya establecida se perderá o disminuirá. Además, algunas empresas derivan su ventaja competitiva de la propiedad intelectual o de los conocimientos técnicos como ventaja sobre los activos intangibles. Tras un ataque, una empresa puede perder esta ventaja competitiva.

En segundo lugar, las empresas pueden obtener una ventaja de su oferta de productos. Añadir seguridad a un producto como característica adicional permite a las empresas diferenciarse de sus competidores, haciendo que sus productos sean más innovadores. Por último, representa un criterio de satisfacción del cliente y, por tanto, sería una ventaja frente a los activos inmateriales.

Los clientes del comercio electrónico conceden más importancia a la protección de sus datos personales que a un precio más atractivo (La ciberseguridad, ¿una nueva ventaja competitiva para los minoristas electrónicos?) . Se trata del tercer criterio de selección más importante, después de la calidad y la disponibilidad del producto, que son ventajas competitivas. Los resultados del estudio pueden verse en el siguiente gráfico.

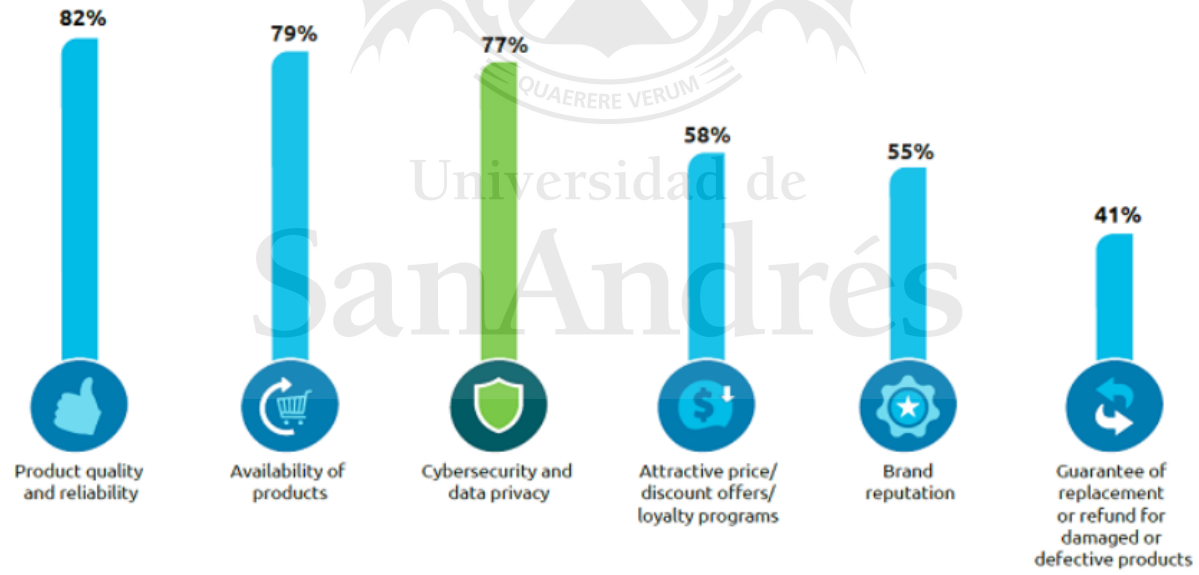


Figura 4. Porcentaje de consumidores que consideran los siguientes factores como uno de los cinco criterios principales para seleccionar a su proveedor principal

Además, según el estudio, "el 40% de los encuestados estaría dispuesto a gastar un 20% más en una tienda electrónica que garantizara la protección y confidencialidad de

sus datos personales" y "garantizar métodos de ciberseguridad sólidos aumentaría incluso la satisfacción de los clientes en Francia en una media del 11%".
Por último, según el mismo estudio, los minoristas equipados con métodos de seguridad eficaces podrían percibir un aumento del 5,4% de sus ingresos anuales".

Por lo tanto, la ciberseguridad proporciona a las empresas una ventaja competitiva. Hemos visto que la consideración de la ciberseguridad es beneficiosa para la propuesta de valor de varias maneras. Estos beneficios son difíciles de medir, pero la aplicación de una estrategia adecuada tendrá un impacto positivo en la empresa.

Proponer una solución única y clara

Esta fase se basa en las secciones anteriores. Para poder exponer su propuesta con claridad, debe conocer bien a sus clientes, sus necesidades, su solución y el mercado en el que opera. Una solución clara es aquella que los clientes potenciales pueden entender en cuestión de segundos. Cuando exponga su propuesta de valor, no es necesariamente una buena idea incluir las características de la ciberseguridad. Esto dependerá de la investigación de marketing que se haya llevado a cabo.

Validar la propuesta de valor y los supuestos

Existen varios métodos para poner a prueba los supuestos que ha hecho sobre su propuesta de valor. Esto garantiza que el producto tiene potencial de venta. Puedes desarrollar un producto mínimo viable (MVP), hacer pruebas A/B o pruebas beta.
En el contexto de la ciberseguridad, puede ser interesante interesarse por las pruebas A/B. Las pruebas A/B permiten comparar dos versiones de un producto que difieren en un único criterio. Así, podríamos tener una versión con ciberseguridad y otra sin ella.

Hay que interesarse y analizar las opiniones y los comentarios de los usuarios. Esto le permitirá validar o invalidar sus hipótesis.

Expresar la propuesta de valor

Será necesario entonces proponer su propuesta de valor a sus clientes. Dependerá de cada empresa y de los resultados de los estudios preliminares que se haga hincapié o no en la ciberseguridad. No obstante, es importante mantener el mensaje claro y sencillo, y apoyarse en un buen marketing para garantizar que la propuesta de valor se comunica correctamente a los clientes potenciales.

Estudio de caso: ciberseguridad para la Internet de los objetos (IoT)

Un estudio publicado por Mckinsey (Caso et al., 2023) explica el potencial de la ciberseguridad para los objetos conectados. Afirma que el futuro del IoT está estrechamente ligado a la integración de las tecnologías de ciberseguridad con los objetos conectados. Ambas áreas deben poder converger para que los usuarios y las empresas puedan aprovechar al máximo la conectividad con los dispositivos. Se ha realizado un estudio de previsión de mercado que muestra el potencial que se puede obtener en los distintos sectores.

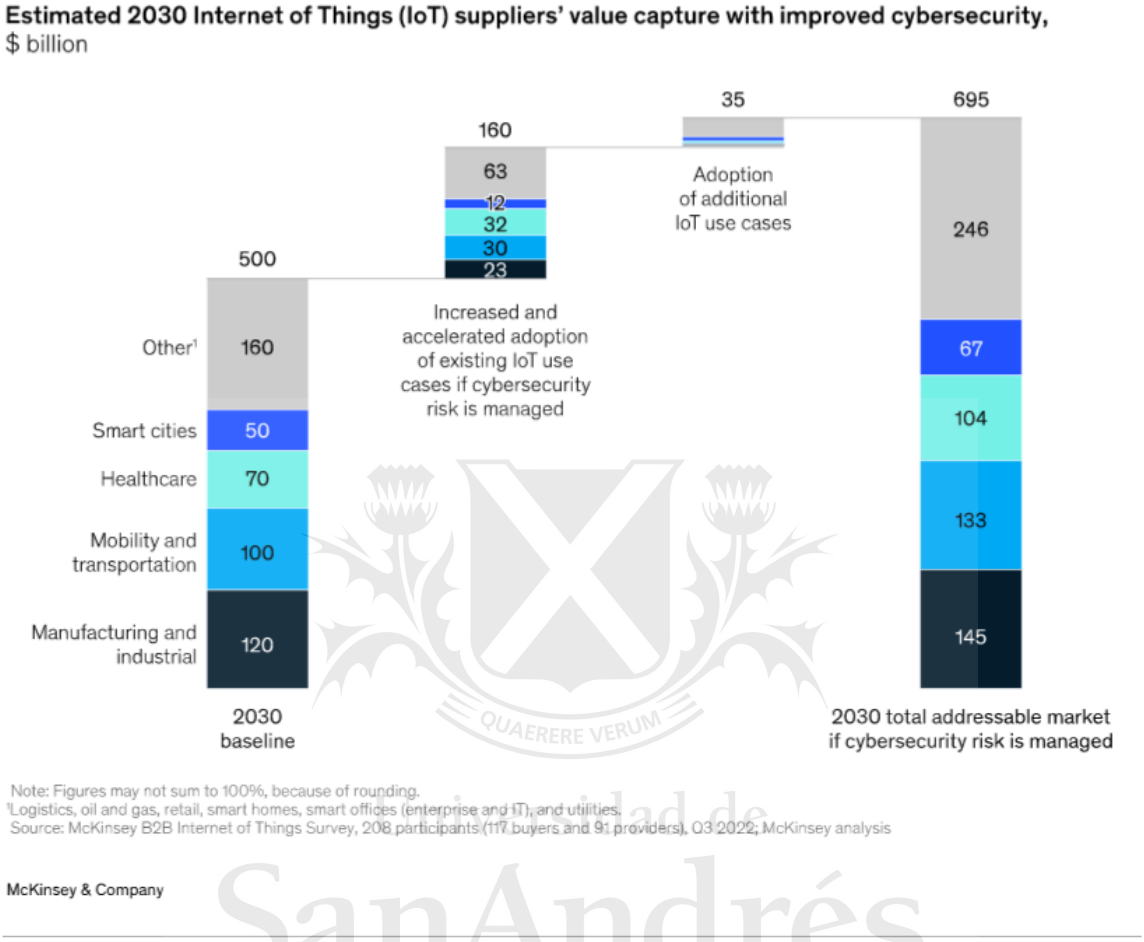


Figura 5. Mercado estimado de IoT en 2030 si se integra la ciberseguridad

Sin embargo, la adopción de objetos conectados por parte de los consumidores sigue siendo difícil. Sigue habiendo obstáculos que frenan a los consumidores, y el principal es la seguridad. De hecho, en el mercado B2B, la ciberseguridad es el obstáculo número uno, como muestra el siguiente gráfico:

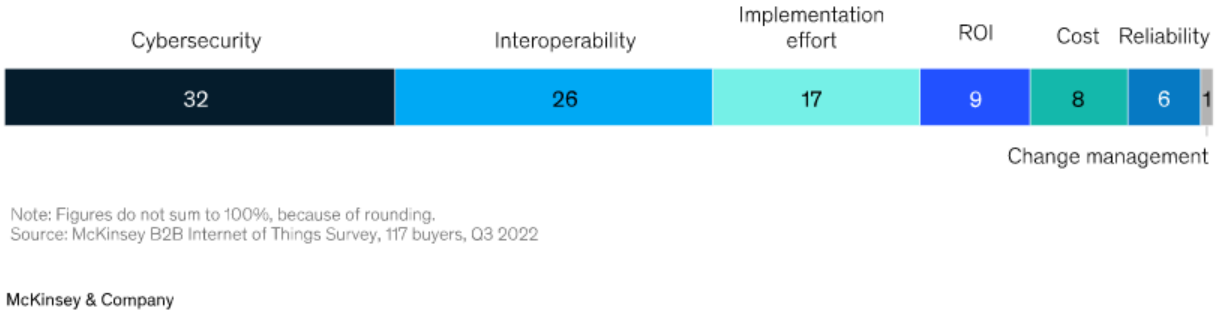


Figura 6. Principales obstáculos para la adopción del "Internet of Things"

Por ello, el estudio destaca la importancia de aplicar medidas de seguridad sólidas e incorporarlas a los productos.

Además, los sectores más expuestos, como el de la salud, son los que más pueden beneficiarse de la ciberseguridad. Este es el caso del sector sanitario, del transporte y de muchos otros sectores.

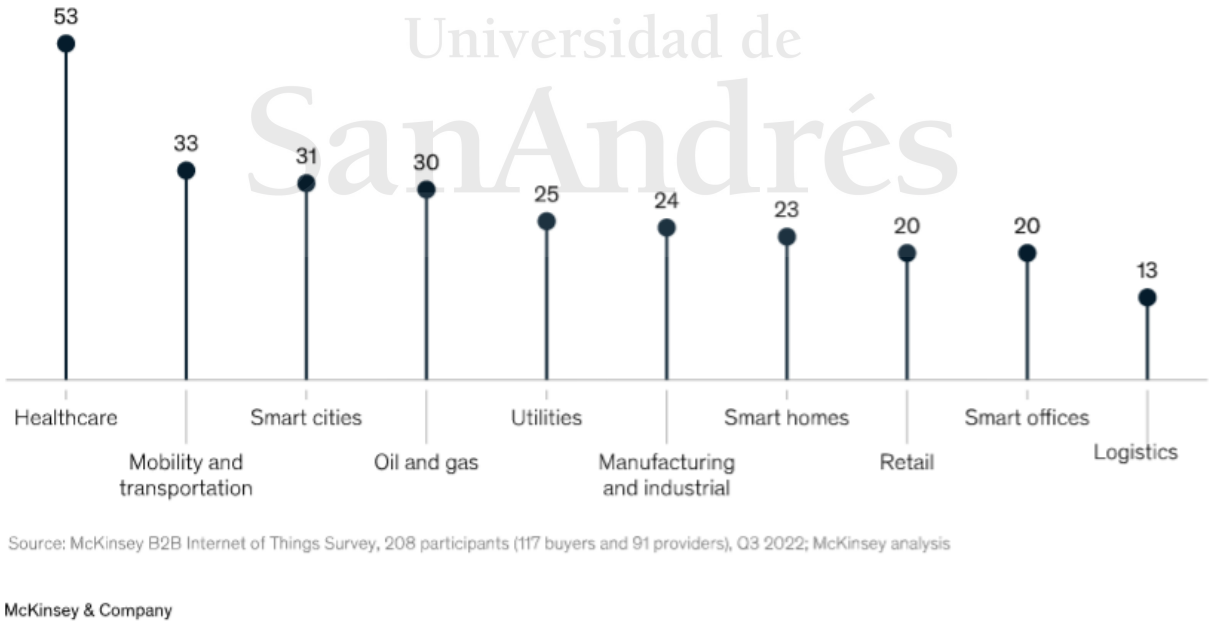


Figura 7. Crecimiento porcentual del gasto si se gestionan bien los riesgos de ciberseguridad

Este estudio demuestra la ventaja competitiva de la ciberseguridad. Esto permitiría una mayor adopción de los productos y aumentaría el gasto en el sector. La ciberseguridad sería, por tanto, una palanca para aumentar los ingresos. Todas las empresas del mercado de la IO tienen interés en aprovechar las ventajas de la ciberseguridad para diferenciarse de sus competidores.

Aunque el futuro de la IOT es prometedor, la convergencia de estos dos campos se enfrenta a una serie de obstáculos. Todo el ecosistema está fragmentado. Existen diferentes proveedores de dispositivos, plataformas y protocolos. Esta fragmentación dificulta la integración de la ciberseguridad, y es difícil que un proveedor de IoT proteja toda la cadena.

Sin embargo, la ciberseguridad desempeña un papel clave para liberar el potencial del IoT. Esto mejorará la experiencia del cliente. También tendrá un impacto beneficioso en toda la cadena IoT, creando una red más transparente y ágil de dispositivos interconectados.

IV. Gestión del cambio para una cultura de ciberseguridad

Una cultura de la innovación

Cultivar una cultura de la innovación es esencial si queremos beneficiarnos de competitividad sostenible. Las empresas deben aprender a adaptarse y responder constantemente a las expectativas de sus clientes. En un ecosistema en el que la tecnología evoluciona constantemente, es importante establecer una cultura de la innovación dentro de la empresa. Esto garantizará que la estrategia de la empresa sea lo suficientemente ágil como para adaptarse a las nuevas necesidades de los clientes y que no se quede rezagada con respecto a sus competidores. Es más, una estrategia empresarial innovadora bien aplicada mantendrá el dinamismo de la empresa, le dará una ventaja competitiva sobre sus competidores y atraerá a nuevos clientes. También mejorará la satisfacción, el compromiso y las condiciones de trabajo de los empleados. Por último, la introducción de una cultura de la innovación estimulará la creación de ideas. Reforzará y acentuará esta cultura, creando un círculo virtuoso.

Por tanto, esta cultura de la innovación ofrece muchas ventajas que beneficiarán a la empresa en su conjunto y le permitirán ofrecer una propuesta de valor de mayor calidad y, por tanto, más atractiva para sus clientes.

La ciberseguridad forma parte obviamente de esta cultura de la innovación. Nos permitirá añadir tecnologías seguras a nuestra oferta. También es una buena manera de garantizar que los empleados sean conscientes de los retos de la ciberseguridad. Por tanto, todas las nuevas ideas incorporarán algún aspecto de estas tecnologías.

Si nos fijamos en las doce dimensiones de la innovación, la ciberseguridad puede desempeñar un papel en todos los niveles: oferta, plataformas, soluciones, clientes, experiencia del cliente, valor captado, organización, cadena de suministro, presencia, redes y marca.

Universidad de SanAndrés

Interview

¿Puede presentarse?

Me llamo Valentin, tengo 28 años y soy desarrollador de software desde hace tres años en una empresa estadounidense. Desarrollo aplicaciones para el sector de las telecomunicaciones. No mencionaré el nombre de la empresa por motivos de confidencialidad.

¿Tiene formación en ciberseguridad?

No tengo formación universitaria en ciberseguridad. Sin embargo, he recibido formación dentro de la empresa.

A lo largo de mi experiencia profesional, he adquirido conocimientos gracias a los consejos de mis compañeros. También ha habido cursos de formación en la empresa, en particular el curso "KnowBe4", que ha sido especialmente beneficioso. Aunque algunos elementos pueden parecer obvios, el contenido estaba bien pensado y era informativo.

¿Tiene en cuenta el ciberespacio cuando codifica?

Sí, tengo que tener cuidado cuando codifico. Intento aplicar buenas prácticas de ciberseguridad, sobre todo porque trabajo en telecomunicaciones.

A menudo tengo que crear servidores http que generan tráfico, así que tengo que tener mucho cuidado de que sólo las direcciones autorizadas puedan comunicarse con mi servidor. También tengo cuidado con las inyecciones de datos que puedan ser peligrosas.

¿Se ha encontrado alguna vez con un problema de seguridad en su empresa?

Sí, ya hemos sido víctimas de un ataque. Fue un ataque DDoS. Los hackers querían hacer caer el producto en el que estábamos trabajando.

Durante un ataque DDoS, el sistema se inunda de peticiones y, como consecuencia, todo el sistema se vuelve lento. También teníamos herramientas para ver las peticiones. Eran demasiadas, así que enseguida nos dimos cuenta de que se trataba de un ataque DDoS.

La empresa pertenece a un sector responsable, ya que gestiona llamadas de emergencia, que pueden tener un impacto directo en la vida de las personas, como cuando tienen que ponerse en contacto con los servicios de emergencia.

¿Cómo reaccionaron?

Para contrarrestar los ataques, los agresores diversifican sus direcciones IP, a menudo desde los mismos países, como Rusia y China. En respuesta, la empresa decidió bloquear el acceso desde estos dos países, lo que le permitió establecer una defensa rápida y eficaz contra los ataques.

Los atacantes suelen intentar comunicar un mensaje a través de estas solicitudes, por ejemplo anunciando que son una organización y pidiendo que se envíe dinero a una dirección Bitcoin.

La empresa tuvo que ponerse en contacto con el FBI, y nosotros tuvimos que intentar mantener el contacto con los atacantes sin responder a sus peticiones. Al mismo tiempo, tuvimos que gestionar y asegurar el negocio de la empresa.

Al mismo tiempo, nos pusimos en contacto con una empresa externa, Cloudfare. Esta empresa gestiona el tráfico entrante, bloqueando las direcciones IP y filtrando las solicitudes.

¿Cuáles fueron las consecuencias de este ataque?

Una vez contratados, éramos mucho menos vulnerables.

El impacto del ataque se dejó sentir, aunque fue difícil cuantificarlo con precisión. Supuso la pérdida de clientes y de ingresos para la empresa. Además de las pérdidas financieras, también hay que tener en cuenta la considerable cantidad de tiempo que

tuvieron que invertir durante uno o dos meses para hacer frente a las consecuencias del ataque.

¿Está concienciada su empresa en materia de ciberseguridad?

En general, somos una empresa tecnológica, por lo que la gente está más sensibilizada y concienciada con la ciberseguridad. Además, como ya he dicho, tenemos una formación constante en ciberseguridad.

Mi nivel de conocimientos de ingeniería social es bastante limitado. Conocemos las reglas básicas, como la necesidad de bloquear el ordenador. En los cursos de formación, se suele hacer hincapié en temas relacionados con el correo electrónico, y hay frecuentes pruebas para engañarnos. Luego, en función de los resultados, se puede pasar al departamento de informática.

¿Ha observado algún cambio en la cultura de la ciberseguridad en su empresa?

Mi empresa ha crecido considerablemente. En tres años, hemos pasado de cincuenta a doscientos cincuenta empleados. Al principio, no había formación. Hoy en día, los empleados reciben formación y, como parte de nuestro proceso de contratación, intentamos evaluar los conocimientos de nuestros candidatos en materia de ciberseguridad.

Los riesgos son demasiado altos para ignorarlos. Aunque lleve tiempo, todos los empleados están alerta. También porque somos una empresa tecnológica, todos somos conscientes de ello. Sin embargo, es crucial que las medidas puestas en marcha no tarden demasiado.

¿Ha contribuido la ciberseguridad a la creación de valor para la empresa?

La empresa tiene que obtener certificaciones para nuestros productos. Para obtener estas certificaciones, tienen que cumplir normas estrictas. En un entorno competitivo, todos los actores han sido víctimas de ciberataques de tipo DDoS.

Ninguna empresa se ha distinguido especialmente en términos de ciberseguridad frente a estos ataques.

¿Qué le gustaría mejorar en materia de ciberseguridad?

La gestión de la ciberseguridad es compleja porque es difícil determinar con certeza si las medidas aplicadas son suficientes. Es un campo muy amplio y yo no soy un experto.

Lo principal es no dejar escapar las oportunidades de mejora una vez que se sabe que existen. Por eso la empresa trabaja activamente para maximizar su seguridad, y ya contamos con dos profesionales de la ciberseguridad.

Análisis de la entrevista:

Esta entrevista esclarece una situación bastante común que viven las empresas con demasiada frecuencia. Podemos ver que, al final, la situación se gestionó bien, aunque tuvo repercusiones en la empresa.

Si intentamos establecer las razones por las que esta situación salió bien, podemos identificar varios puntos.

En primer lugar, la empresa y sus empleados comprendieron inmediatamente que había un problema y pudieron reaccionar rápidamente bloqueando las direcciones de determinados países y recurriendo a otra empresa especializada.

Esta rapidez de análisis y reacción fue posible gracias a los conocimientos de ciberseguridad de los empleados.

Valentin subrayó que todos estaban algo sensibilizados con la ciberseguridad porque son una empresa tecnológica. Ese es el punto clave de la ciberseguridad de la empresa.

Sin embargo, no todas las empresas tienen este nivel de sensibilidad. Así que hay que insistir en esta cultura de la innovación en materia de seguridad, y formar a las personas que no tienen conocimientos suficientes.

Como explicó muy bien al final de la entrevista, no sabe qué medidas serían interesantes para mejorar la seguridad porque es un sector demasiado amplio y no es su área de especialización. Por eso hay expertos encargados de la estrategia de ciberseguridad.

Impulsar el cambio para adoptar la ciberseguridad

Los expertos en ciberseguridad son esenciales para apoyar a las empresas. Una cultura de ciberseguridad puede ser una ventaja competitiva y el primer paso para crearla es contratar a un líder en ciberseguridad (Pearlson y Huang 2020).
También se menciona en esta revisión que para construir una cultura de ciberseguridad no basta con ofrecer formación y poner a prueba a los empleados de forma regular.
De hecho, para gestionar con éxito el cambio, es necesario llevar a cabo un trabajo en profundidad. La idea principal de la gestión del cambio se basa en los valores, creencias y actitudes que influyen en el comportamiento.
Por lo tanto, tiene sentido examinar la teoría que subyace a estos diferentes términos para comprender lo que realmente motiva a las personas a cambiar su comportamiento y adoptar nuevas prácticas. El estudio de (Grube, Mayton y Ball-Rokeach 1994) presenta la teoría del sistema de creencias mencionado en el artículo de revisión del MIT (Pearlson y Huang 2020).

Para entender por qué es posible el cambio tanto a nivel organizativo como individual, es importante comprender la psicología de los individuos. Para ello, hay que distinguir entre creencias, valores y actitudes.

Las creencias son convicciones o juicios que las personas tienen sobre objetos, personas, grupos o situaciones.
Los valores son un conjunto de creencias que definen la manera ideal de comportarse.

Los valores son, por tanto, traducciones de las necesidades individuales a una forma socialmente aceptable.

Las actitudes son emocionales. Las actitudes son evaluaciones positivas o negativas de objetos y situaciones.

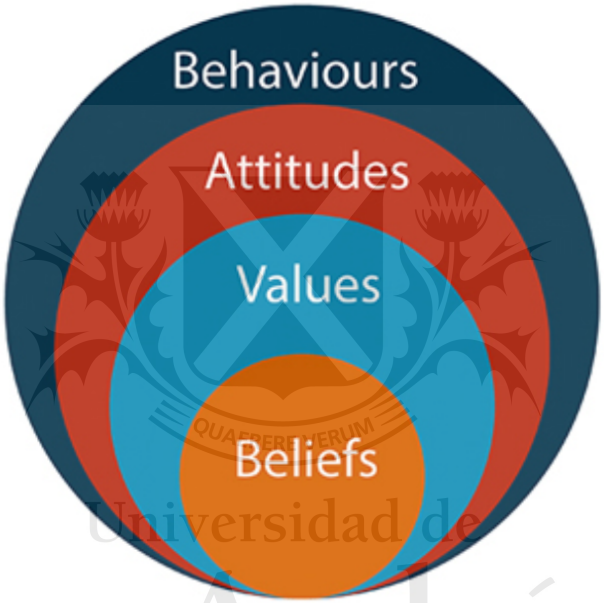


Figura 8. Diagrama de creencias, valores, actitudes y comportamientos

Las creencias, los valores y las actitudes están influidos por factores externos y mecanismos de gestión (Pearlson y Huang 2020).

Los factores externos pueden ser específicos de cada sector, de la competencia y de las actividades de la empresa. El directivo debe comprender estas interacciones para poder influir en los empleados El objetivo del gestor es la aceptación de la innovación, es decir, que los individuos o el grupo en cuestión utilicen la innovación.

Los mecanismos de gestión incluyen la formación y la sensibilización de los empleados. Sin embargo, esto no es suficiente. También se indica que existen

evaluaciones y recompensas para fomentar la adopción de la ciberseguridad en la empresa.

Se pueden distinguir dos tipos de adopción de innovaciones (Frambach y Schillewaert 2002). Se trata de la adopción por parte de una organización y la adopción por parte de un individuo dentro de la organización. La plena adopción de una cultura de la innovación depende del resultado de estas diferentes categorías. Además, la adopción por parte de una organización no puede tener lugar si no hay aceptación por parte de los individuos.

La adopción de la ciberseguridad no es un hecho en las empresas. A menudo es impulsada por las empresas para sus empleados. Esto se conoce como adopción forzada.

Nivel organizativo

El proceso de adopción de una organización se desarrolla en varias fases.

En la fase de iniciación, hay una fase de toma de conciencia de la innovación. Esto crea una actitud de evaluación positiva o negativa hacia esta innovación, en nuestro caso la ciberseguridad. La iniciación también tiene en cuenta las actitudes de sensibilización y consideración.

La decisión de adoptar la innovación tiene lugar entre la fase de iniciación y la fase de aplicación.

La fase de implementación es cuando la organización decide utilizar la innovación.

El proceso de adopción se considera exitoso cuando la innovación es aceptada, integrada y se convierte en parte de un uso continuado en el tiempo.

Varios factores influyen en el éxito de la gestión del cambio. Como puede verse en el siguiente gráfico, la decisión de adopción implica un uso continuado. En esta decisión de adopción influyen la percepción de la innovación, las características de la organización y factores externos (Pearlson y Huang 2020).

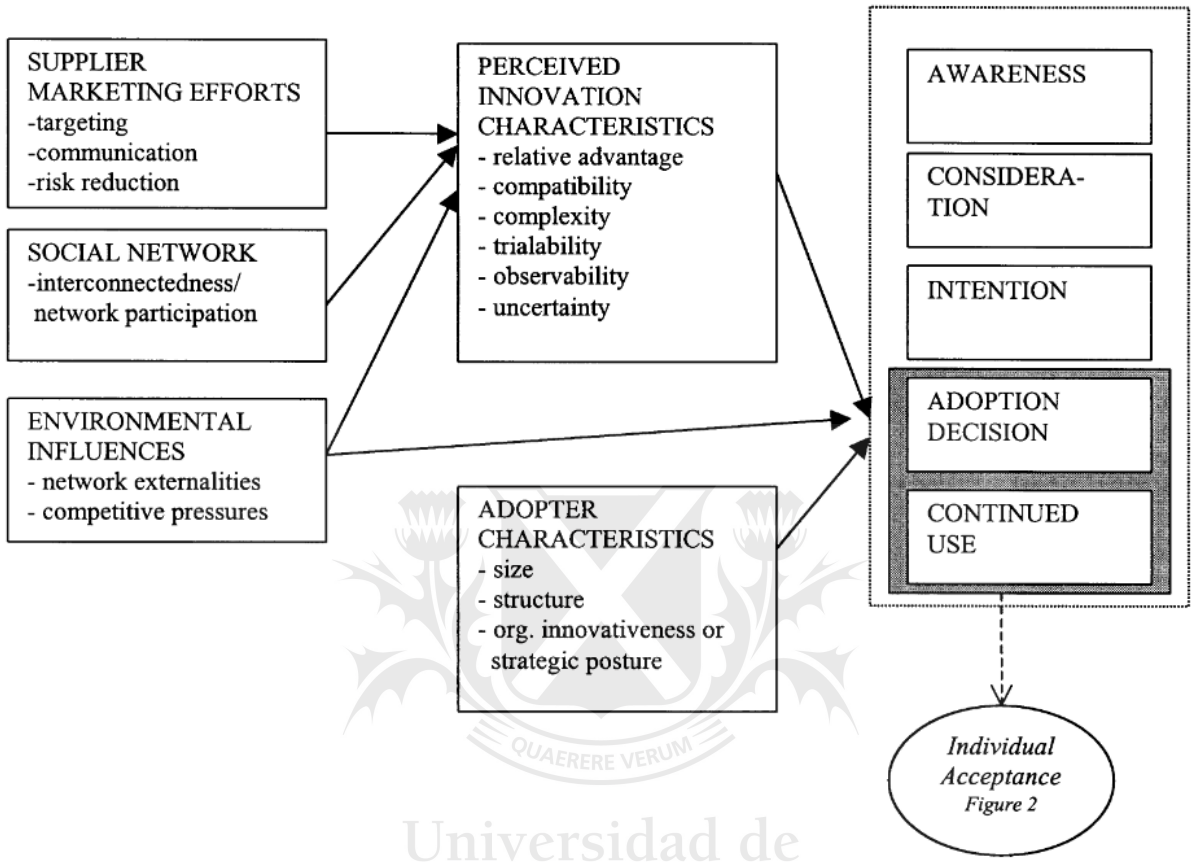


Figura 9. Framework de adopción organizativa

La percepción de la innovación por parte de los responsables de la toma de decisiones dentro de la organización reviste una importancia capital. Esta percepción adopta varias formas. Las principales características que crean la percepción de la innovación dentro de las empresas son obviamente los beneficios, y más concretamente los beneficios económicos. En el contexto de la ciberseguridad, hemos demostrado que podemos aportar pruebas cuantificables de los beneficios de esta innovación.

Además del incentivo económico, otros factores como la compatibilidad, la complejidad y la observabilidad conforman una percepción global por parte de los responsables de la toma de decisiones.

El efecto red es un factor influyente en el sentido de que el valor de una red depende de su número de usuarios. Cuantas más personas y entidades compartan una innovación, más importante será esa red, lo que facilitará una percepción y aceptación positivas.

Las estrategias de marketing de los proveedores también influirán en la percepción de los responsables de la toma de decisiones, en función de su orientación específica hacia los clientes potenciales, su comunicación y su gestión del riesgo.

Así pues, estos dos factores y la influencia de los factores del entorno externo conformarán la percepción de la innovación a nivel organizativo. Como hemos visto antes, el experto en ciberseguridad no puede influir directamente en estas fuerzas. Debe comprenderlas e identificarlas para crear una percepción positiva de la ciberseguridad.

A nivel individual dentro de la organización

Las creencias están influidas por factores externos (Frambach y Schillewaert 2002). Los factores externos también pueden influir en las actitudes de un individuo.

A nivel individual, la aceptación se consigue a través del vínculo entre las creencias y las emociones sobre la innovación. Se indica que las creencias, la utilidad percibida, la facilidad de uso percibida y la respuesta emocional a la innovación son los factores centrales de la aceptación.

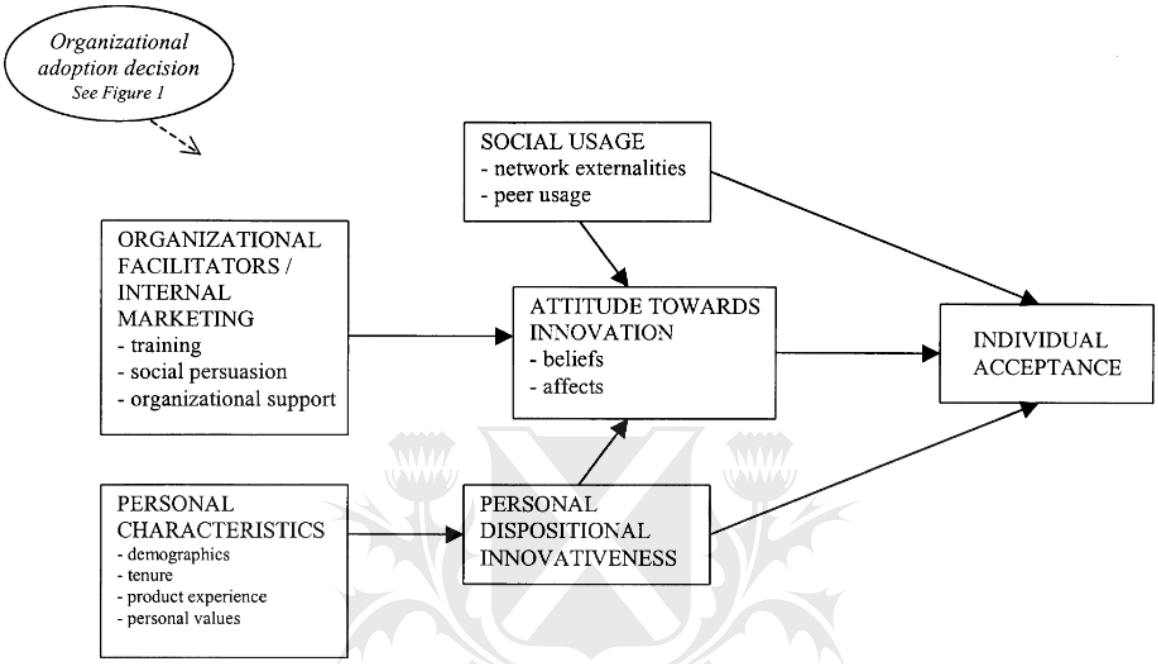


Figura 10. Framework de adopción a nivel individual dentro de una organización

Observamos que ciertos factores no pueden utilizarse dentro de una empresa para fomentar la adopción. Un especialista en ciberseguridad no podrá cambiar la "personal dispositional innovativeness". De hecho, algunas personas son más sensibles que otras a la adopción de una tecnología debido a sus características personales.

Las influencias sociales pueden influir tanto en las actitudes como en los comportamientos. El uso de la ciberseguridad por parte de colegas tendería a señalar la importancia de su aplicación. Esto animaría a los individuos a imitar estos comportamientos. Las normas sociales también desempeñan un papel en la adopción. Se trata de la percepción que tiene una persona de que la mayoría de las personas importantes piensan que debe o no realizar el comportamiento en cuestión. Así pues, la estrategia de adopción debe venir de arriba y los empleados deben ser capaces de seguir el ejemplo de sus superiores.

Por último, los "organizational facilitators" dependen de las estrategias, acciones y políticas puestas en marcha. Entre ellos figuran la formación, las pruebas y las recompensas.

En conclusión, este modelo nos permite comprender el proceso de adopción en las empresas. Para implantar con éxito una política de transformación digital aplicada a la ciberseguridad, es importante comprender los factores que influyen. Tras el análisis, esto también nos permitirá identificar los puntos de bloqueo y probar nuevas estrategias de influencia para garantizar el éxito de la adopción.

V. Ciberseguridad para el crecimiento exponencial

El crecimiento

Cuando consideramos el crecimiento de una empresa, este crecimiento puede adoptar varias formas. Puede ser interno, orgánico o externo. El crecimiento puede dividirse en tres partes (Baghai et al., 2007).

El crecimiento orgánico puede dividirse en dos subcategorías. Está el " portfolio momentum " y el " market share performance ".

El portfolio momentum representa el crecimiento de las ventas de una empresa debido al crecimiento de los segmentos de mercado de su portfolio.

El "Market share performance" representa las ganancias y pérdidas de cuota de mercado.

Por último, el crecimiento inorgánico se basa en fusiones y adquisiciones.

Si analizamos el crecimiento en función de sus diversos componentes, podemos ver que algunas palancas son más eficaces que otras en general.

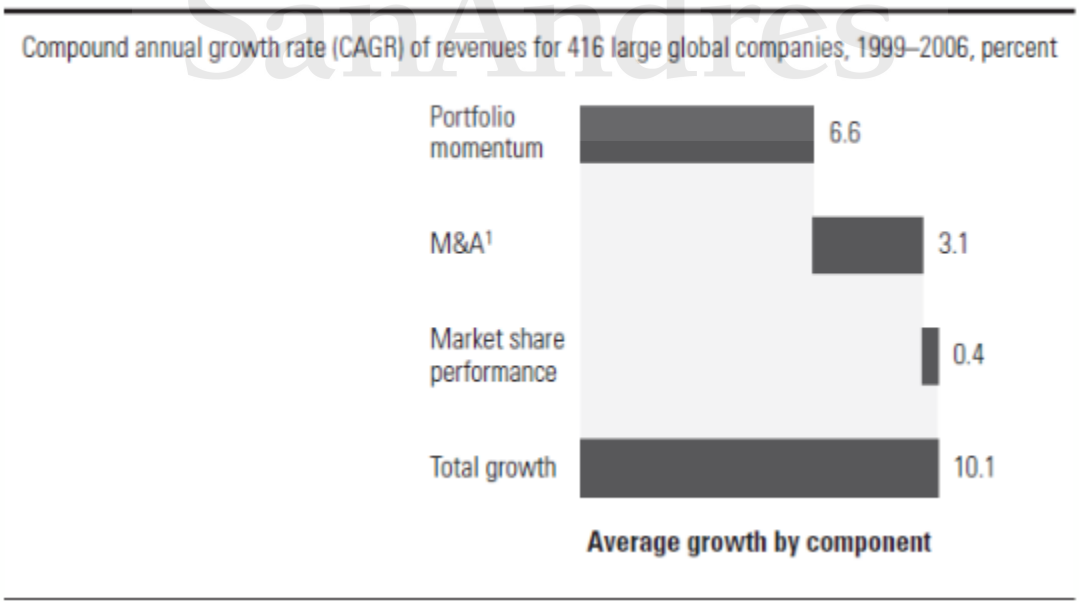


Figura 11. Composición del crecimiento

Las empresas centran la mayor parte de su atención en ganar cuota de mercado en los mercados existentes mediante una ejecución superior. Sin embargo, la cuota de mercado sólo contribuyó un 0,4% al crecimiento global. Para cosechar todos los beneficios del crecimiento global del mercado, una empresa necesita mantener su posición en el segmento. El éxito a la hora de mantener o ganar cuota de mercado depende de la calidad de su ejecución. Así es como la ciberseguridad puede ayudar a las empresas a mantener su posición y luego pasar a ganar cuota de mercado.

Existen tres categorías de crecimiento. Crecimiento bajo, medio y alto.

En primer lugar, el crecimiento bajo es el que no crea valor. Las empresas pueden ganar cuota de mercado a costa de sus competidores mediante la innovación incremental. Los competidores tienen la capacidad de reproducir estas innovaciones y recuperar a sus clientes.

Los intentos de ganar cuota de mercado a expensas de los competidores mediante la promoción de productos y la fijación de precios pueden dar lugar a rápidas represalias por parte de los competidores, ya que pueden ajustar sus propias estrategias de precios y promoción en respuesta.

En segundo lugar, para un crecimiento medio, las empresas pueden ganar cuota de mercado en un mercado de rápido crecimiento: Los competidores pueden seguir creciendo aunque pierdan cuota de mercado. Las empresas pueden realizar adquisiciones complementarias para acelerar el crecimiento de sus productos.

Por último, para aprovechar al máximo el crecimiento exponencial, las empresas crean nuevos mercados con nuevos productos. No habrá competidores establecidos. También convencerán a los clientes existentes para que compren más de un producto y atraerán nuevos clientes al mercado.

La dificultad para aprovechar el crecimiento exponencial es mantener ese crecimiento a lo largo del tiempo. El crecimiento sostenible es difícil porque depende del ciclo de vida

natural de los productos. Estos ciclos de vida tienen las siguientes curvas, que siguen una S.

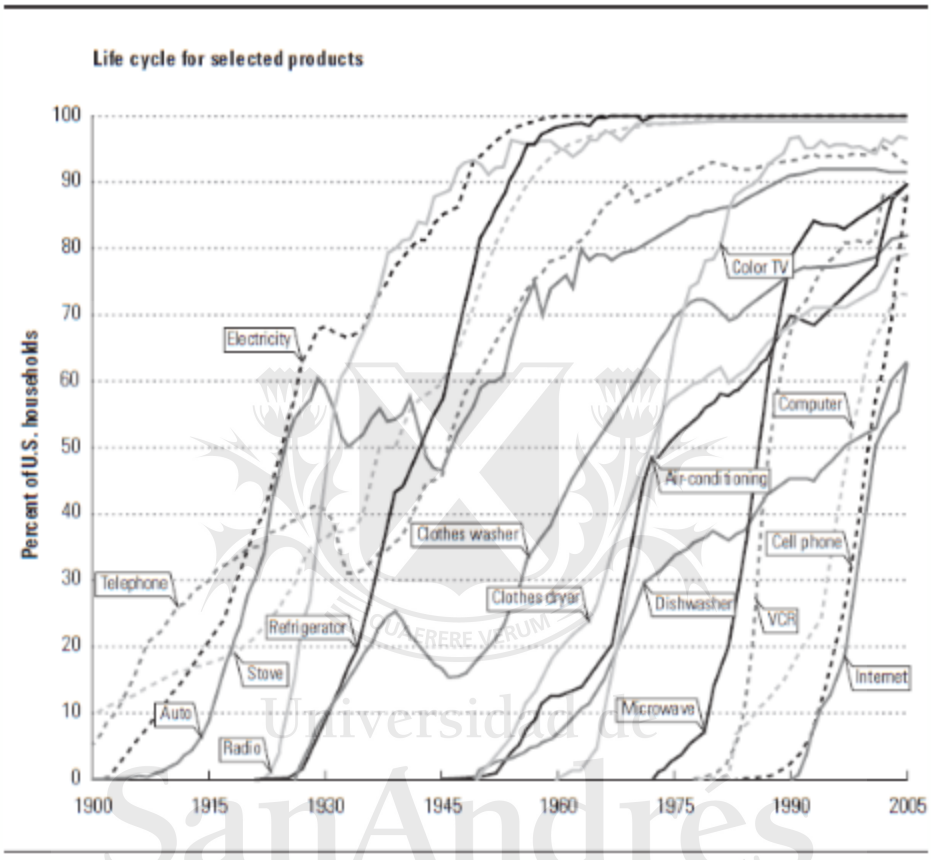


Figura 12. variación en el ciclo de vida del producto

La única forma de lograr el crecimiento es encontrar constantemente nuevos mercados para los productos y servicios. También es necesario introducir nuevos productos y servicios con éxito y en el momento adecuado para aprovechar su fase de crecimiento más rentable. Así es como la ciberseguridad desempeña su papel en el crecimiento exponencial.

Para conquistar nuevos mercados, la propuesta de valor que incluye la ciberseguridad debe permitir a la empresa abrirse paso en nuevos mercados. Como hemos visto en la sección anterior sobre la propuesta de valor, es posible obtener una ventaja

competitiva. Además, al adoptar una cultura de innovación y ciberseguridad, las empresas son capaces de operar con agilidad y en el momento adecuado para posicionarse plenamente para un crecimiento exponencial.

Sin embargo, en todos los sectores, al cabo de 3 años, las elevadísimas tasas de crecimiento empiezan a retroceder hasta un valor medio del 5%. Al cabo de 5 años, la diferencia de crecimiento entre las empresas de alto crecimiento y las de bajo crecimiento es inferior al 5%.

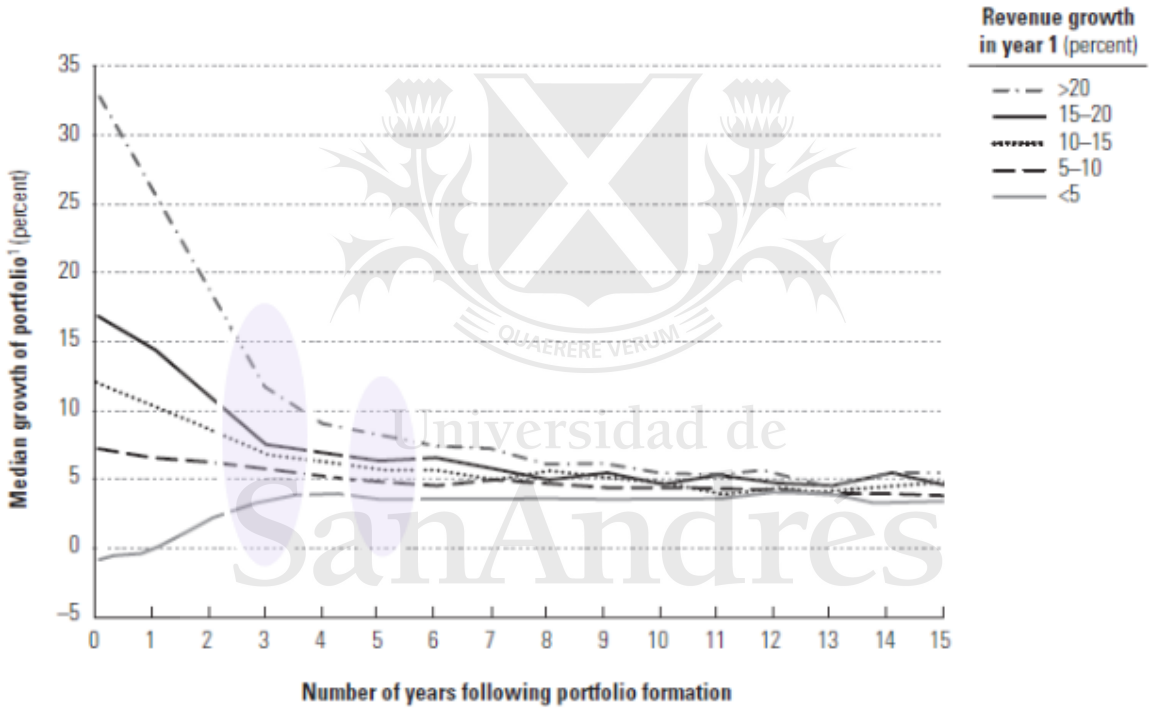


Figura 13. trayectorias de crecimiento

Este crecimiento es difícil de mantener durante mucho tiempo y estos procesos tienen que renovarse constantemente en función de los ciclos de vida de los productos.

Las empresas necesitan aprovechar este crecimiento exponencial, pero será difícil tener este tipo de crecimiento para siempre. Esto debería permitirles desarrollar y luego beneficiarse de rendimientos de la inversión más estables en el tiempo. De hecho,

estos dos indicadores pueden compararse a lo largo del tiempo (Penman y Nissim (2003)).

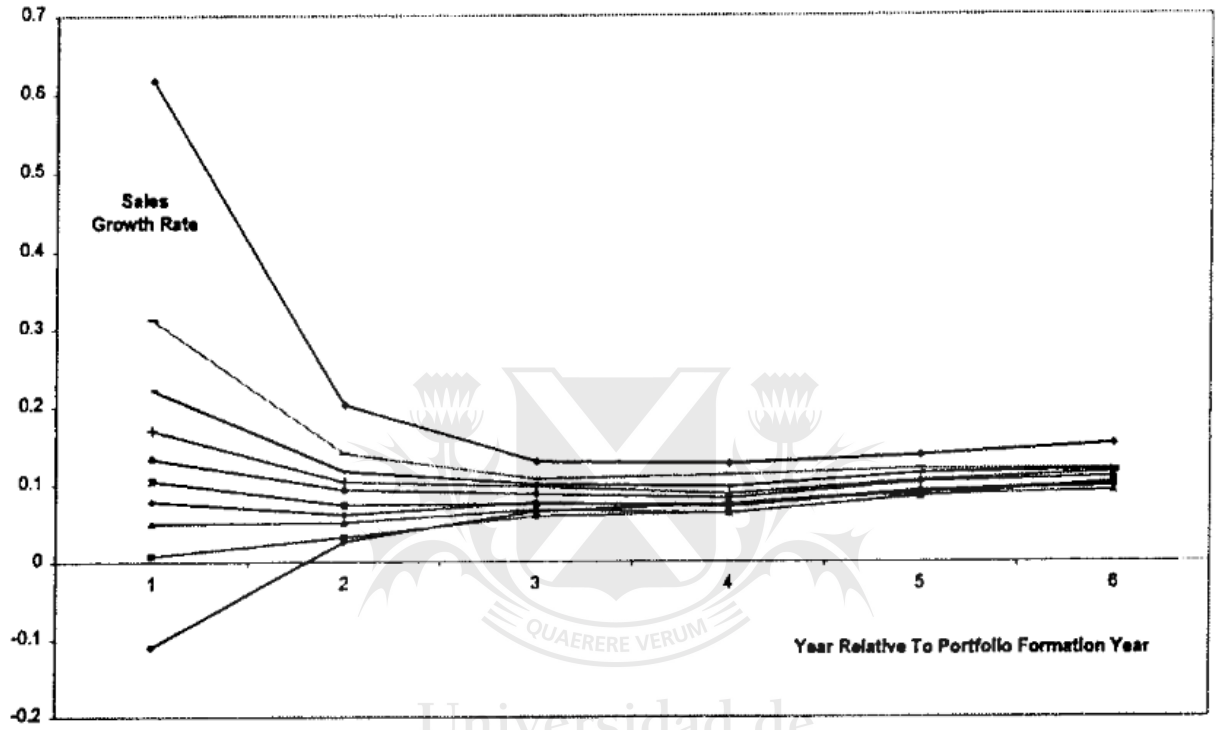


Figura 14: tasa de crecimiento de las ventas a lo largo de los años

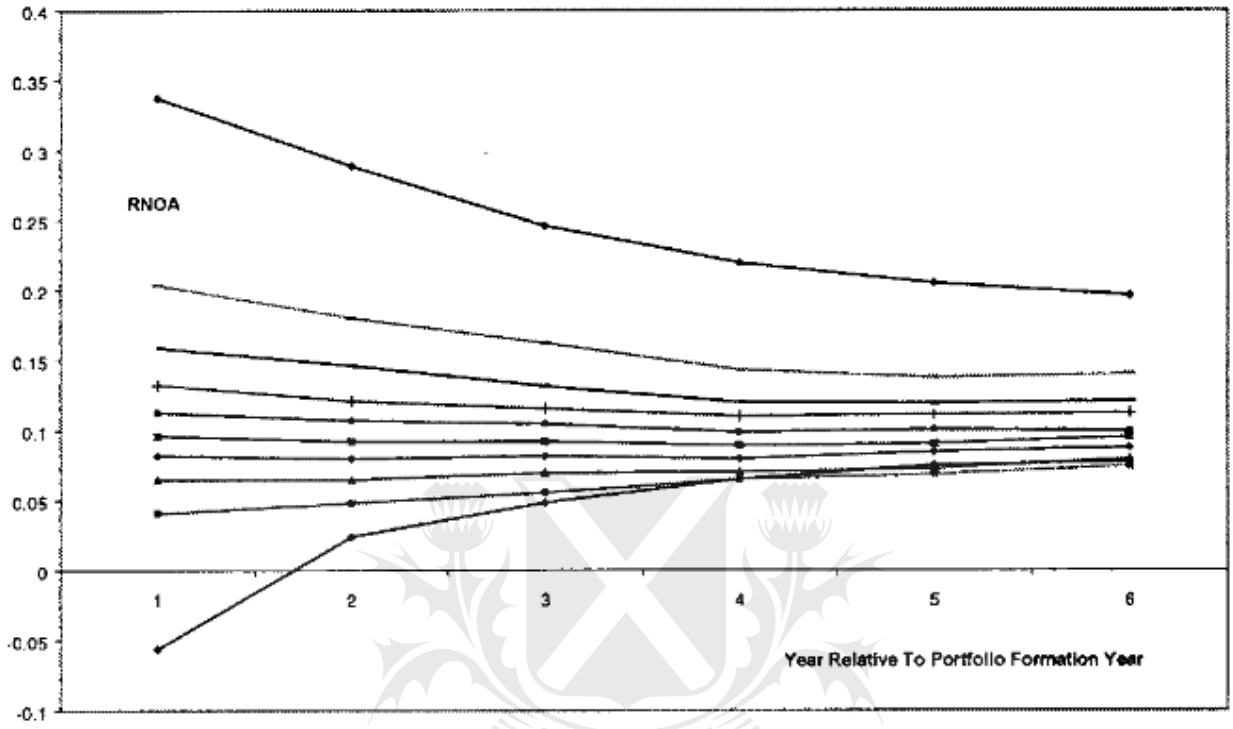


Figura 15. rentabilidad a lo largo de los años

El RNOA es similar al rendimiento del capital invertido (ROIC) ajustado a la deuda operativa.

Esto muestra lo que impulsa el crecimiento exponencial y lo que crea valor. Es importante que las empresas aprovechen este crecimiento exponencial. Esto debe hacerse comprendiendo los ciclos de vida de los productos e introduciendo nuevos productos a un ritmo cada vez mayor.

Por último, los estudios realizados en todos los sectores demuestran la dificultad de mantener niveles tan altos de crecimiento a lo largo del tiempo. Como puede verse en los gráficos anteriores, es posible mantener a largo plazo un alto nivel de rentabilidad. Siguiendo esta estrategia de crecimiento, las empresas necesitan cambiar su estrategia y seguir siendo rentables a largo plazo.

En el contexto de la ciberseguridad, analizaremos las ganancias y pérdidas de cuota de mercado. Nuestro objetivo es mostrar cómo la ciberseguridad puede aumentar la rentabilidad de las empresas. Para ello, primero tenemos que entender cómo cuantificar el rendimiento de la inversión en ciberseguridad.

Estrategia tras el crecimiento exponencial

Medir el impacto de la ciberseguridad: indicadores y KPI

Las empresas necesitan indicadores para dirigir su estrategia empresarial. Las medidas cuantitativas conocidas como KPI ("key indicator performance" o indicadores clave de rendimiento) permiten a los responsables cuantificar el rendimiento de una empresa para alcanzar sus objetivos. Los KPI se controlan y analizan en varios departamentos de la empresa. Los indicadores recurrentes suelen encontrarse en marketing, finanzas e inversiones.

En ciberseguridad, también hay muchos KPI específicos de la seguridad.

Sin embargo, es difícil cuantificar el impacto de la ciberseguridad en los resultados globales de una empresa. Es difícil medir los beneficios indirectos obtenidos gracias a la estrategia y la inversión en seguridad.

KPIs de ciberseguridad

Los KPI de ciberseguridad dan una idea global de la situación en materia de ataques y del nivel de defensa. Estos KPI son importantes a nivel de la actividad de la empresa y dan una idea de su nivel de seguridad. Permiten comprender los puntos fuertes y débiles de la empresa.

Por ejemplo, el número de incidentes, el número de intentos de intrusión, el tiempo medio entre dos "fallos", el tiempo medio de detección, el tiempo medio de recuperación, el número de ataques de phishing con éxito y muchos otros.

El análisis de estos indicadores permite a las empresas y a los responsables de ciberseguridad tomar medidas para mantener un nivel de seguridad aceptable. Estos KPI se limitan a la seguridad. Analizar y mejorar estos KPI reflejaría una mayor seguridad para la empresa. Sin embargo, no cuantifican el impacto de la ciberseguridad en la competitividad de una empresa.

Indicadores clave de rendimiento que vinculan la ciberseguridad y la estrategia empresarial

Return on Security Investment: RoSI

No hay consenso entre las empresas para vincular la ciberseguridad a los resultados empresariales. Es un tema muy complejo y ningún estándar o indicador ha sido adoptado unánimemente.

En el informe realizado por Cisco (2016):“Sin embargo, las empresas invertirían aún más en ciberseguridad si pudieran cuantificar el valor de sus beneficios. De hecho, el 81% de los ejecutivos financieros afirmaron que sería "mucho más" o "moderadamente más" probable que aumentaran su gasto en ciberseguridad si tuvieran una mejor forma de medir estos resultados empresariales."

Hay un doble interés. En primer lugar, medir los beneficios y, en segundo lugar, fomentar la inversión en seguridad.

Una empresa que invierte en un proyecto necesita poder medir su impacto financiero. En general, se establece un modelo financiero y el objetivo es maximizar el rendimiento de la inversión (ROI).

En ciberseguridad, el ROI no puede medirse tan sencillamente. Un departamento de ciberseguridad (para una empresa que no vende productos o servicios de seguridad), no genera ingresos directamente.

Existen varios métodos potenciales para establecer un sistema de métricas y KPI (Onwubiko y Onwubiko 2019). Esto permitiría establecer un "Return on Security Investment" (RoSI).

El RoSI puede desglosarse de la siguiente manera:

$$RoSI = \frac{(Benefits\ of\ Investment - Cost\ of\ Investment)}{Cost\ of\ Investment}$$

Es fácil cifrar el coste de inversión de una empresa. Sin embargo, el problema suele residir en evaluar los beneficios de la inversión. Los beneficios de una inversión son numerosos, y la valoración de cada persona es única. Se trata de una medida subjetiva. Dos personas que intentaran calcular este KPI probablemente obtendrían resultados diferentes.

Para medir este RoSI, proponemos evaluar 6 métricas principales que también son la composición de otras métricas. En total, hay 20 métricas diferentes.

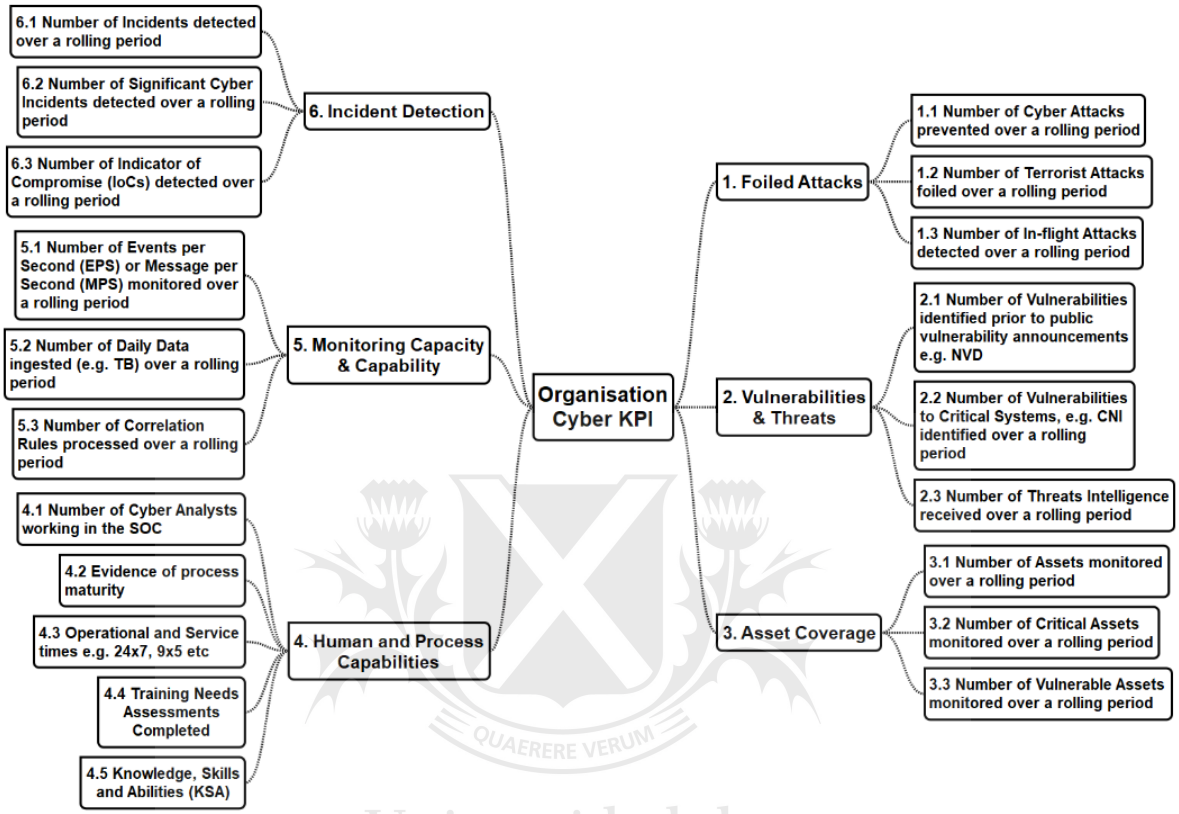


Figura 16. Vinculación de Cyber KPI

Este estudio no es completo. Nos da una idea de los parámetros que hay que tener en cuenta a la hora de establecer los KPI. Sin embargo, no tenemos ejemplos concretos y cuantificables que poner.

Return on Cyber Investment y Return on Investment: RCI & ROI

Otro estudio (Garvey, Moynihan y Servi 2012) tiene en cuenta estos diferentes parámetros y propone una metodología para medir el impacto de las medidas de defensa. Se construyen dos indicadores, el return on cyber investment (ROCI) y el return on investment (ROI).

El ROI se desglosa de la siguiente manera:

$$RCI = \frac{Net\ Savings}{Total\ Cost\ Impact\ Before\ Investment}$$

$$Net\ Savings = Savings\ from\ Investment - Cost\ of\ Investment$$

Este KPI es un porcentaje. Permite evaluar el porcentaje del coste ahorrado gracias a la inversión en ciberseguridad. Esto da una idea de la reducción de las pérdidas financieras gracias a una inversión en comparación con las pérdidas financieras sin ninguna medida de protección.

El ROI se desglosa de la siguiente manera:

$$ROI = \frac{Net\ Savings}{Cost\ of\ Investment}$$

El ROI también es un porcentaje. Se utiliza para calcular el ahorro obtenido como resultado de invertir en ciberseguridad.

El "Cost of Investment" puede cuantificarse y aproximarse fácilmente. Corresponde al dinero que usted invertirá para protegerse.
La dificultad de estos KPI estriba en cuantificar el " Total Cost Impact Before Investment " y el " Net Savings " y, más concretamente, el " Savings from Investment ".
Para ello, el estudio propone un enfoque cualitativo y cuantitativo. Se trata de partir de una evaluación cualitativa del riesgo para, a continuación, transformar este riesgo en una pérdida financiera. Planteamos el problema en forma de matriz y luego aplicamos funciones matemáticas para obtener valores numéricos.

Cyber Intrusion Event	Impact Criteria: Performance Reduced by x%			
	Operate Mission	Prevent	Detect	Quarantine
	Color or Linguistic Rating, x%			
Trojan BOTs	Very High, 95%	Orange, 65%	Yellow, 30%	Yellow, 40%
Denial of Service	Green, 20%	Orange, 60%	Red, 95%	Moderate, 40%
Malware Insertion	Red, 80%	Orange, 50%	Orange, 65%	Orange, 60%
Mass SQL Injection	Yellow, 40%	Red, 95%	Orange, 55%	Orange, 70%
Confidentiality Intrusion	Red, 95%	Green, 20%	Yellow, 40%	Red, 80%

Cyber Intrusion Event	Impact Criteria (Merit Points)			
	Operate Mission	Prevent	Detect	Quarantine
Trojan BOTs	3.3	26	61	50
Denial of Service	73	30.5	3.3	50
Malware Insertion	14	39.9	26	30.5
Mass SQL Injection	50	3.3	35.1	21.9
Confidentiality Intrusion	3.3	73	50	14

Cyber Intrusion Event	Impact Criteria (Dollars)			
	Operate Mission	Prevent	Detect	Quarantine
Trojan BOTs	$475K	$325K	$150K	$200K
Denial of Service	$100K	$300K	$475K	$200K
Malware Insertion	$400K	$250K	$325K	$300K
Mass SQL Injection	$200K	$475K	$275K	$350K
Confidentiality Intrusion	$475K	$100K	$200K	$400K

Figura 17. Matriz de eventos, matriz de puntos de mérito y equivalente en dólares

Los datos que se introducen en la matriz de entrada pueden proceder de diversas fuentes y métodos, como modelos de ingeniería, opiniones de expertos o información de la comunidad de seguridad. Estas entradas son cualitativas en el sentido de que a cada suceso se asocian riesgos muy bajos, bajos, medios, altos y muy altos.

A continuación, las entradas se transforman en puntos de mérito. Para ello se utilizan funciones de mérito. Se pasa así de una evaluación porcentual aproximada a puntos muy precisos. Una vez más, se aplica una función para convertir los puntos de mérito en costes equivalentes.

A continuación, puede elegir una acción (COA). Esta acción representa un coste de inversión conocido. Esta acción tendrá inevitablemente un impacto en las matrices anteriores. Cada acción tendrá un impacto en uno o más eventos. Se utiliza el mismo principio, es decir, pasamos de una evaluación cualitativa a datos cuantitativos.

Cyber Intrusion Event	COA investment options strengthen ability to …			
	Operate Mission	Prevent	Detect	Quarantine
Trojan BOTs	COAs 1, 2, 3, 4, 5	COAs 3, 4, 5	COAs 1, 3, 8	COAs 2, 3, 4, 5
Denial of Service	COA 8	COA 1, 8	COAs 2, 4, 7	COAs 2, 4, 7, **9**
Malware Insertion	COAs 5, 6, 7, **9**	COAs 4, 5, 6, 10	COAs 5, 6, 10	COA 10
Mass SQL Injection	COA 8	COA 8	COA 8	COA 8
Confidentiality Intrusion	COA 8	COAs 8, **9**	COAs 4, **9**	COAs 4, **9**

Cyber Intrusion Event	Impact Criteria (Merit Points)			
	Operate Mission	Prevent	Detect	Quarantine
Trojan BOTs	3.3	26	61	50
Denial of Service	73	30.5	3.3	50, **80**
Malware Insertion	14, **80**	39.9	26	30.5
Mass SQL Injection	50	3.3	35.1	21.9
Confidentiality Intrusion	3.3	73, **75**	50, **65**	14, **85**
Cyber Intrusion Event	**Impact Criteria (Dollars)**			
	Operate Mission	Prevent	Detect	Quarantine
Trojan BOTs	$475K	$325K	$150K	$200K
Denial of Service	$100K	$300K	$475K	$200K, **$72K**
Malware Insertion	$400K, **$72K**	$250K	$325K	$300K
Mass SQL Injection	$200K	$475K	$275K	$350
Confidentiality Intrusion	$475K	$100K, **$92K**	$200K, **$133K**	$400K, **$53K**

Figura 18.. Coste de reducción de una acción aplicada a las matrices de eventos, puntos de mérito y equivalente en dólares.

Ahora es posible calcular el " Total Cost Impact Before Investment " y el " Savings from Investment ". Por tanto, podemos calcular el "ROI" y el "ROI".

A continuación, se puede utilizar un algoritmo para maximizar las opciones de inversión en términos de coste y seguridad. Esto nos permitirá decidir qué estrategias queremos poner en marcha ante eventos de intrusión.

Este modelo nos da una idea de cómo cuantificar y orientar las inversiones en ciberseguridad. El enfoque utilizado es pertinente. Cada elemento de la ciberseguridad

está disociado e intentamos tener en cuenta soluciones con múltiples impactos. Sin embargo, este modelo se basa en hipótesis que también son subjetivas en términos de insumos y beneficios de la inversión. Las matrices pueden variar de una empresa a otra y de un profesional de la ciberseguridad a otro.
Sería interesante combinar ambos modelos. Para ser más precisos, convendría tener en cuenta todos los KPI mencionados en el primer estudio y adaptarlos en el segundo método.

Es importante tener en cuenta las limitaciones de estos modelos. Los métodos miden el impacto económico directo de la ciberseguridad en una empresa. No tienen en cuenta las consecuencias no financieras de un ciberataque. Una empresa está expuesta a numerosas consecuencias tras un ataque. Podría, por ejemplo, perder la confianza de sus clientes y, por tanto, su reputación.

La creación de KPI que vinculen la ciberseguridad y los resultados de la empresa es, por tanto, muy compleja. Es difícil obtener un KPI que describa una imagen global y completa de la situación. Sin embargo, es posible cuantificar y aproximar los beneficios financieros de invertir en ciberseguridad. Esto podría, por tanto, fomentar y justificar la inversión en ciberseguridad.

Optimizar una inversión en ciberseguridad

Las empresas que crecen exponencialmente consiguen generar beneficios exponenciales (Thomson, 2005). Para lograrlo, las empresas deben ser capaces de generar márgenes atractivos. Evidentemente, las pérdidas financieras vinculadas a la seguridad de las empresas reducen este margen y tienen un impacto negativo en la rentabilidad de las empresas.

Se ha realizado un estudio sobre la rentabilidad del coste de la ciberseguridad (Lee 2021). El objetivo es crear y comparar un análisis de costes y un análisis de riesgos.

El primer paso consiste en evaluar las pérdidas financieras asociadas a un ciberataque. Para ello, cada empresa debe identificar los distintos ataques potenciales a sus activos. Se puede elaborar una primera matriz de riesgos teniendo en cuenta la frecuencia de los ataques y la pérdida financiera media por ataque.

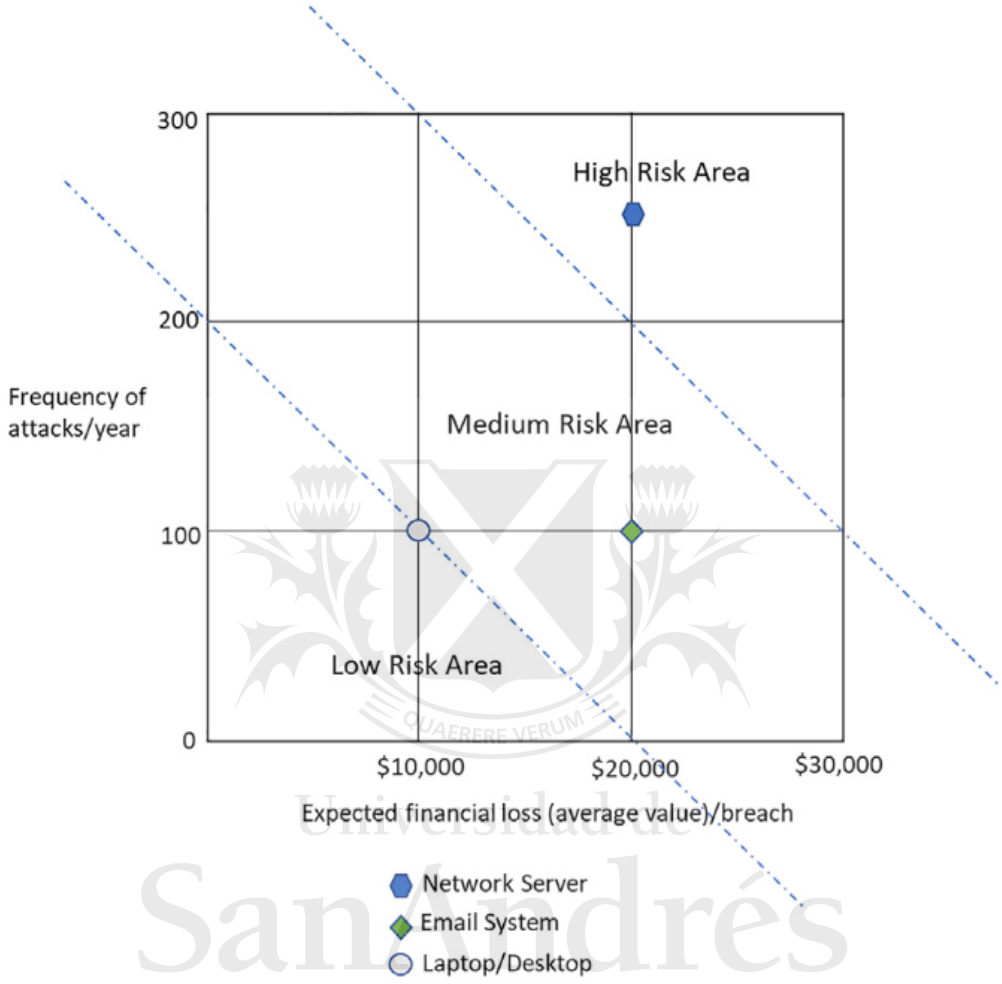


Figura 19. Matriz de riesgo para tres tipos de ataque

A continuación, adoptamos un punto de vista probabilístico considerando las pérdidas reales como las pérdidas medias ponderadas por la probabilidad de defensa, es decir, la probabilidad de que la organización sea capaz de defenderse contra un ataque.
Esto nos da las siguientes pérdidas financieras:

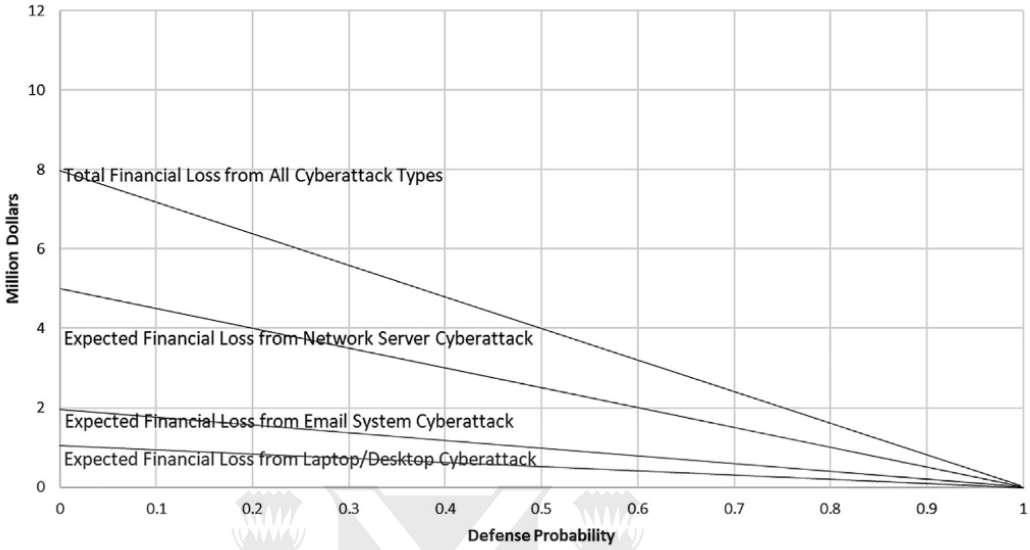


Figura 20. Relación entre pérdidas financieras y probabilidad de defensa

A continuación, debemos evaluar el coste de invertir en ciberseguridad. Para ello, necesitamos identificar los costes de desarrollar herramientas y políticas de ciberseguridad, junto con la probabilidad de defensa.

Así se obtiene una comparación entre la inversión y las pérdidas.

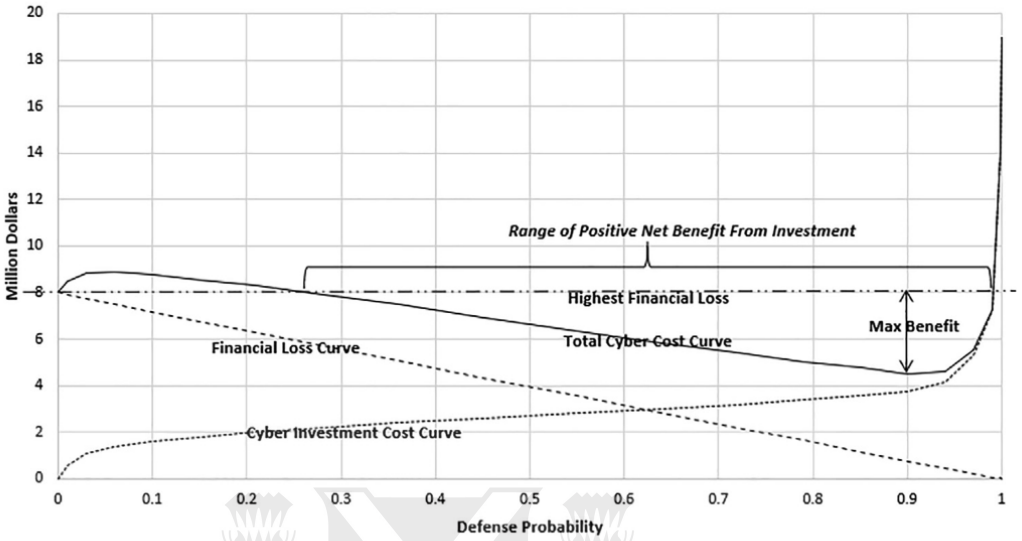


Figura 21. Análisis de los costes de ciberinversión

Estas curvas nos permiten visualizar el coste total de la ciberseguridad diferenciando entre coste e inversión. Podemos ver que el coste de la ciberseguridad se convierte en un mejor escenario cuando el coste de la ciberseguridad es inferior a la pérdida financiera máxima. Por tanto, resulta rentable invertir y alcanzar este rango de datos. Además, también existe un escenario ideal en el que los beneficios son máximos.

Este modelo es interesante para cuantificar la importancia de la estrategia de inversión. Pone de relieve los beneficios a muy corto plazo de invertir en ciberseguridad. Podemos ver que los beneficios directos de la inversión superan rápidamente las pérdidas financieras. Por tanto, las empresas rentabilizan rápidamente su política de ciberseguridad, habida cuenta de las pérdidas potenciales.

Este tipo de modelo se basa en un análisis de costes. Desde un punto de vista financiero, no se tienen en cuenta los ingresos de la empresa. La rentabilidad de las empresas aumenta reduciendo los costes, no aumentando los ingresos.

Este modelo no tiene en cuenta el aumento de los ingresos que se consigue indirectamente gracias a las ventajas competitivas, como hemos visto antes. Estos beneficios siguen siendo imposibles de cuantificar.

En conclusión, este método muestra que la ciberseguridad mejora la rentabilidad de las empresas en comparación con otro escenario. De hecho, la rentabilidad de la empresa mejorará si previamente ha sufrido un ataque que haya aumentado sus pérdidas financieras.

Si la empresa no ha sufrido ningún ataque o pérdida financiera, desde un punto de vista financiero saldrá perdiendo en términos de rentabilidad, ya que el coste total de la ciberseguridad tendrá un impacto negativo en el balance de la empresa.

Sin embargo, el retorno de la inversión es muy rápido. Por tanto, sigue siendo una muy buena herramienta para animar a las empresas a invertir en seguridad, y les proporciona información sobre la estrategia que deben poner en marcha para maximizar su rentabilidad.

Opinión personal

Evaluar el rendimiento de la inversión en ciberseguridad es muy difícil. Desde un punto de vista global, creo que a todas las empresas les interesaría cuantificar el rendimiento de la inversión en la medida de lo posible, utilizando métodos matemáticos y estadísticos. Si cada vez más empresas adoptan estos métodos cuantitativos, podremos crear bases de datos de todos los incidentes. Así, con todos estos datos y la potencia de cálculo disponible hoy en día, podríamos desarrollar modelos aún más precisos. Esto contribuirá en gran medida a establecer un método común para gestionar los riesgos y justificar la inversión en ciberseguridad sobre la base de argumentos concretos.

También creo que los expertos en ciberseguridad están en la mejor posición para justificar las inversiones en ciberseguridad. La experiencia de un profesional en su mercado tendrá sin duda un valor añadido que las cifras no pueden expresar. Por lo tanto, creo que los métodos cuantitativos que hemos visto deberían ser utilizados por todas las empresas para justificar y basarse en los números para convencer. Sin embargo, la objetividad de los profesionales va más allá del aspecto financiero.

Pudimos ver de qué palancas disponían las empresas para beneficiarse de la ciberseguridad. Una evaluación comparativa del sector de la ciberseguridad es esencial para comprender la realidad del mercado. Nos permitirá saber qué actores, qué sectores y qué naciones utilizan la ciberseguridad para beneficiarse de un crecimiento exponencial.

VI. Benchmark de empresas, sectores y países

Los distintos benchmarks nos permitirán conocer las empresas de sus sectores y su geografía. Esto nos permitirá identificar los vínculos que existen entre cada uno de los benchmarks. También nos permitirá elaborar un roadmap más acorde con la realidad.

Benchmark de empresas

No todas las empresas están al mismo nivel en materia de ciberseguridad. Las empresas más seguras han comprendido los retos de la ciberseguridad y la han integrado en su estrategia corporativa. Vamos a hacer un análisis comparativo de las empresas más seguras y a entender qué las hace tan exitosas. Sin embargo, sigue siendo difícil evaluar el nivel de defensa de las empresas, ya que también mantienen un nivel de confidencialidad en su estrategia.
Para evaluar la seguridad de una empresa, necesitamos evaluar varios parámetros de protección corporativa.

La revista Forbes ha elaborado una clasificación de las empresas estadounidenses más seguras en 2023. La clasificación se ha realizado en colaboración con SecurityScorecard, una empresa especializada en auditorías de seguridad. Las empresas se clasificaron en función de una serie de factores, como la seguridad de la red, los posibles exploits de malware, la regularidad de los parches y la solidez del equipo de ciberseguridad de la empresa. Las empresas se compararon dentro de su propio sector porque industrias se enfrentan a peligros distintos y requieren estrategias diferentes. Las empresas deben facturar al menos 1.000 millones de dólares en 2022 y no haber sufrido ninguna brecha desde el 1 de enero de 2022.

Ranking	**Name**	**Industry**
1	Intel	Technology

2	Western Alliance Bancorp.	Banking and Finance
3	Virtusa	Software
4	Palantir Technology	Software
5	MetLife	Insurance
6	Pacific Western Bank	Banking and Finance
7	Houlihan Lokey	Banking and Finance
8	Wayne-Sanderson Farms	Food and Beverage
9	Neiman Marcus Group	Retail
10	Rooms to go	Retail

Tabla 1. Las empresas más ciber seguras de Estados Unidos

Es importante analizar estas empresas y comprender los factores que las hacen más seguras. Observamos que estas empresas operan en sectores diferentes y que los retos son distintos para cada una de ellas.

Tecnología

Intel es la empresa más segura. Es la única empresa de las diez primeras que opera en el sector tecnológico, si lo distinguimos del sector del software.

Intel fabrica y comercializa equipos informáticos. Fabrica principalmente microprocesadores, placas base, tarjetas gráficas y otros productos. Opera en los segmentos Client Computing Group (CCG), Data Center Group (DCG), Internet of Things Group (IOTG), Non-Volatile Memory Solutions Group (NSG) y Programmable Solutions Group (PSG).

Por la naturaleza de su negocio, Intel está muy expuesta a riesgos de ciberseguridad. Por tanto, parece lógico que la empresa haya invertido fuertemente en este ámbito.

Luego está el sector bancario y financiero. Western Alliance Bancorp, Pacific Western Bank y Houlihan Lokey figuran entre las empresas más seguras. Por un lado, tienen requisitos que provienen del propio mercado. El sistema bancario cuenta con infraestructuras y datos sensibles que no pueden permitirse ser atacados. Por otra parte, el sistema bancario es responsable del almacenamiento y el flujo de dinero. Por lo tanto, los piratas informáticos se interesan principalmente por este sector, ya que es allí donde pueden acceder más fácilmente y de forma directa al dinero.

Banca y Finanzas

Western Alliance Bancorp es el decimotercer banco más grande de Estados Unidos, pero uno de los más seguros del país.

El director de seguridad de la información explica la política de ciberseguridad del banco en su sitio web. "El panorama laboral ha experimentado un cambio drástico, y es importante encontrar formas innovadoras de capacitar y educar a los empleados de una manera que les resulte cómoda y eficaz.", (Victor Vinogradov, *Western Alliance Bank Cyber Security*, s. d.).

Inicialmente, su objetivo es mantenerse en el cuartil superior de los bancos más seguros. Los objetivos del banco son claros. El banco se basa en el marco jurídico y en normas del sector como NIST, FFIEC, COBIT e ITIL para orientar su estrategia. Esto les permite ser lo más coherentes posible con el mercado.

Se detallan varios elementos de la estrategia de ciberseguridad.

Los empleados tienen tareas obligatorias de ciberseguridad que cumplir. Como hemos visto, este es un factor de adopción de la ciberseguridad en la empresa. El banco también tiene asociaciones con expertos en ciberseguridad. La creación de asociaciones también es indicativa de una buena integración de la ciberseguridad. El banco es consciente de sus limitaciones y del valor añadido de establecer vínculos con expertos.

También mencionan el contexto geopolítico, con la guerra en Ucrania, como motivo para integrar estrategias y adaptarse a las diferentes amenazas, lo que indica una forma de agilidad en su estrategia de ciberseguridad.
Por último, también demuestran un conocimiento técnico de la ciberseguridad. Siguen desarrollando la innovación y atrayendo talento en ciberseguridad, en particular con este HUB (*Western Alliance Bank launches new technology hub*, s. d.) para impulsar esta cultura y mantener el máximo nivel de seguridad.
El banco parece tener una estrategia de ciberseguridad muy buena. También tiene una buena estrategia de comunicación y no duda en compartir sus principales temas. Esto beneficia tanto a la empresa, que establece sus propios estándares elevados, como a sus clientes, que pueden percibir la confianza y profesionalidad del banco. Los demás bancos del top 10 no son tan exhaustivos en sus comunicaciones.

Pacific Western Bank advierte a sus usuarios contra el fraude en línea. En su sitio web, el banco explica cómo garantiza un nivel de seguridad suficiente a sus usuarios protegiendo las comunicaciones entre navegadores y servidores, gestionando la identificación y aislando sus terminales de Internet.

Houlihan Lokey es uno de los principales bancos de inversión del mundo, centrado en fusiones y adquisiciones (M&A). El banco es experto en el mercado de la ciberseguridad, ya que también opera en este sector. Publica informes de mercado durante todo el año. Su equipo de tecnología de fusiones y adquisiciones es, por tanto, un experto estratégico y financiero en este campo. Además, cuentan con un equipo técnico dedicado a la seguridad operativa.

Seguros

Metlife está especializada en seguros de vida. Por tanto, la empresa tiene que satisfacer las exigencias tanto del mercado de seguros como del mercado sanitario.

Metlife hace hincapié en la protección de los datos de sus clientes y en el cumplimiento de la legislación vigente. La empresa sensibiliza sobre la importancia de la ciberseguridad y proporciona a los empleados los recursos necesarios para protegerse. Participan en eventos de ciberseguridad. También tienen programas de seguridad de la información. No hay información real sobre la estrategia de ciberseguridad de la empresa.

Software

Palantir es una de las mayores empresas de software y datos del mundo. Por tanto, ya conoce bien los retos de la ciberseguridad.

En su sitio web (*Palantir Information Security*, s. d.) se pueden consultar todas las normativas y estándares que cumplen. Además, muestran sus numerosas acreditaciones.

Explican el objetivo de su estrategia de seguridad. En primer lugar, la empresa quiere garantizar la seguridad de la empresa, para que sus productos y sus clientes estén seguros y puedan contribuir a crear un mundo más seguro.

En la misma línea, sus productos son de código abierto para mejorar la seguridad de la información y permitir que todo el mundo mejore su propia seguridad. Además, dos veces al año realizan pruebas de penetración para poner a prueba su infraestructura y la de sus copias de seguridad. Por último, sus clientes también pueden realizar pruebas de penetración en sus productos si informan a la empresa con antelación. Esto ayuda a identificar puntos débiles en los productos que pueden haber pasado desapercibidos.

.

Virtusa también conoce bien la ciberseguridad. También desarrolla productos de ciberseguridad. Virtusa ofrece una plataforma completa de pruebas de seguridad: Virtusa Security Testing as a Service (vSTAAS).

La granja Wayne Sanderson no comparte información sobre su política de ciberseguridad.
Neiman Marcus Group y Room to go no comparten información sobre su seguridad. Aunque Neiman Marcus Group fue víctima de un ataque, no hubo nuevas comunicaciones tras la violación de datos.

Además, las empresas de esta clasificación se encuentran en una buena situación financiera. Como indica la metodología de la clasificación, las empresas tienen un nivel de ventas muy alto.
Si nos fijamos en las empresas líderes que obtienen mejores resultados en ciberseguridad, podemos distinguir varias características. Según el estudio de Mckinsey (madurez), "existe un vínculo entre la madurez en ciberseguridad y el margen.

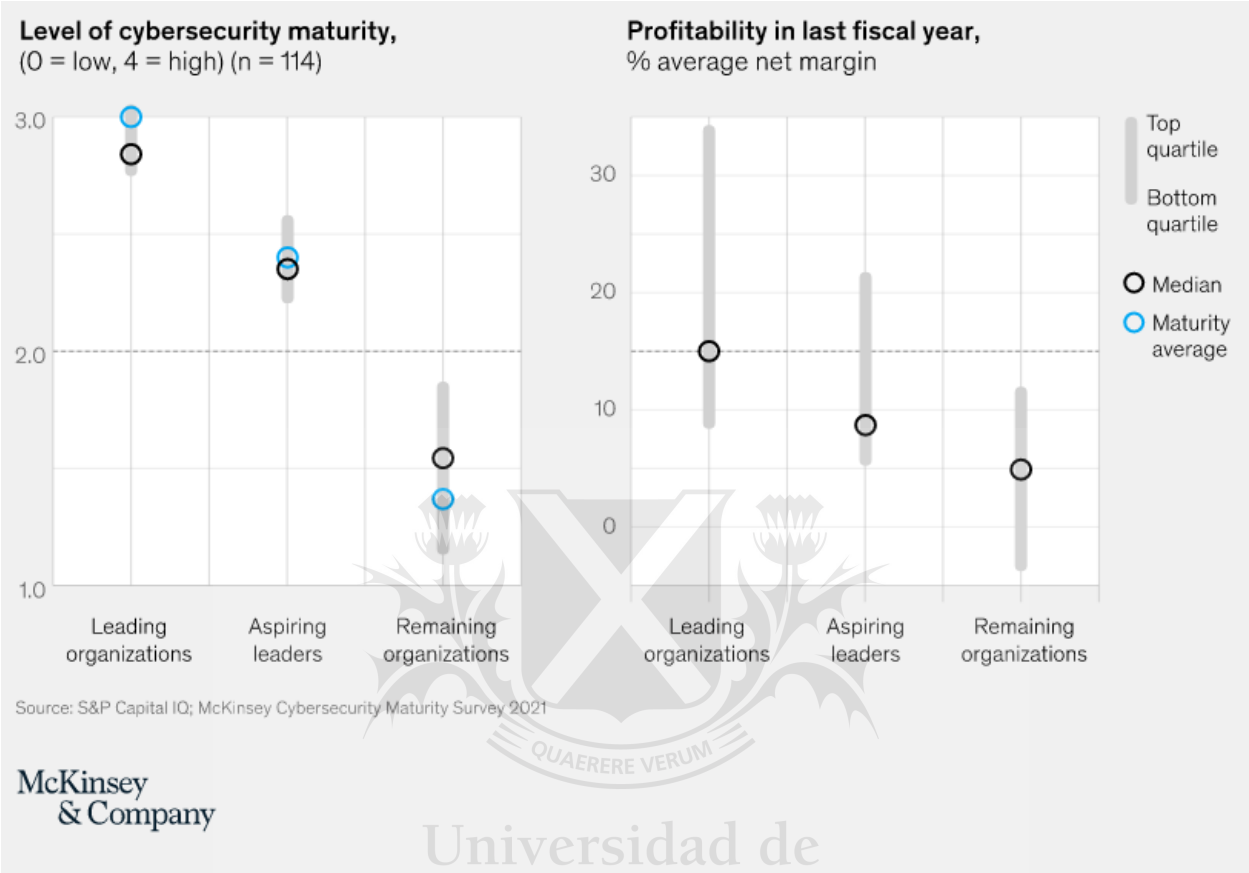


Figura 22. Madurez de la ciberseguridad y rentabilidad empresarial

Esto puede parecer coherente. Hemos visto que una buena rentabilidad permite un crecimiento exponencial. Por tanto, tener un margen atractivo estaría obviamente vinculado a los resultados en ciberseguridad.

El estudio también destaca las características clave de las empresas con mejores resultados. Destaca la importancia de mantener un inventario actualizado de los activos, informar sobre ciberseguridad al consejo de administración y aplicar la separación de privilegios (separar usuarios y procesos en función de distintos niveles de confianza, necesidades y requisitos de privilegios). Las dos primeras actividades fomentan claramente la concienciación sobre el estado actual de la ciberseguridad, lo que facilita a los directivos la identificación de lagunas y la medición del progreso. La

tercera actividad demuestra la sensibilidad operativa de los esfuerzos realizados para contener los riesgos cibernéticos.

Tras la evaluación comparativa de empresas que hemos podido realizar, podemos observar notables diferencias en las expectativas y requisitos de las empresas en función de su sector. A través de las diferentes empresas de los distintos sectores, pudimos comprobar que la comunicación y la estrategia de seguridad varían. Algunos sectores exigen más que otros, y algunas empresas buscan ante todo garantizar la confianza de sus clientes.

Benchmark de sectores

Como hemos visto, la ciberseguridad varía según las especificidades del sector. Depende de la normativa, la sensibilidad de las operaciones, los datos sensibles, la dependencia de la tecnología, las expectativas de los clientes y otros factores. Está claro que una empresa sanitaria no se enfrenta a los mismos problemas que una empresa de alimentación y bebidas. Así que hay muchas diferencias entre los sectores.

En primer lugar, debemos comparar qué sectores gastan más en ciberseguridad. Un estudio publicado en 2022 (*Cyber Security Market Share, Forecast | Growth Analysis [2030]*, s. d.) muestra la cuota de mercado de la ciberseguridad por sectores.

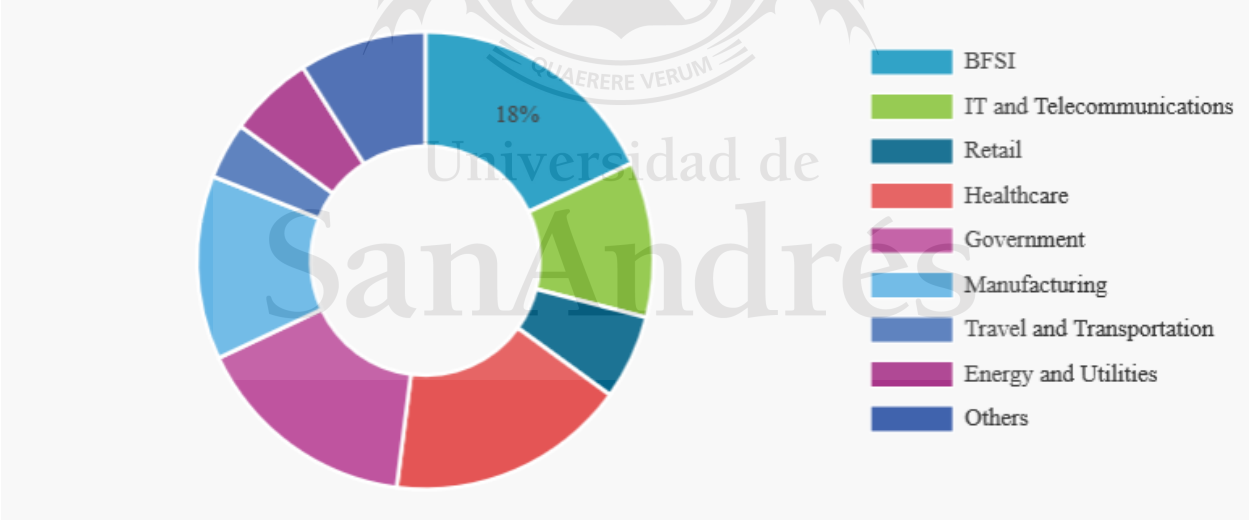


Figura 23. Mercado mundial de la ciberseguridad por sectores 2022

Las mayores cuotas de mercado corresponden a la banca, los servicios financieros y los seguros, seguidos de la sanidad, la administración pública, la informática y las telecomunicaciones, y la industria manufacturera.

Banca y seguros

Las empresas del sector bancario y de seguros tienen grandes necesidades en materia de ciberseguridad debido a sus actividades y a los datos que tratan. Las empresas necesitan mantener la confianza de sus clientes y esforzarse por cumplir los objetivos de confidencialidad, integridad y accesibilidad. Según EY, (*La cybersécurité dans les services financiers*, s. d.) "la gestión integrada de los riesgos de ciberseguridad permite a las entidades financieras obtener resultados empresariales positivos, mejorar el cumplimiento de la normativa, aumentar la eficacia de la gestión de riesgos, preservar la imagen de marca y crear un mayor valor para los accionistas. Una estrategia de este tipo contribuye a crear y mantener la confianza en las instituciones financieras y en los mercados".

Salud

Luego está el sector sanitario. La ciberseguridad desempeña un papel fundamental en estas actividades, lo que debería motivar a todas las empresas a invertir masivamente en seguridad. Un ataque puede provocar un deterioro de las operaciones, con un impacto directo en la vida de los pacientes, y esto puede tener varias consecuencias (*Les enjeux de la cybersécurité dans le secteur de la santé*, s. d.) :

- Cierre del sistema de información
- Riesgo de pérdida o robo de datos de pacientes
- Reprogramación o aplazamiento de intervenciones quirúrgicas
- Desvío de pacientes de urgencias a otros hospitales
- Reducción de la calidad de los servicios asistenciales

Gobiernos

Los Estados y los gobiernos son objetivos de los piratas informáticos. Son objeto de un enorme número de ataques. En el artículo de Deloitte (William D. Eggers,

Government's cyber challenge, 2016), "Sea cual sea el motivo, está claro que los gobiernos son hoy los objetivos de mayor valor para los piratas informáticos".
Los gobiernos son objetivos muy atractivos para los hackers por varias razones. Tienen datos confidenciales muy delicados, controlan infraestructuras muy sensibles dentro del país y pueden ser el objetivo de hackers políticos militantes.

IT et telecomunicación

La ciberseguridad es necesaria porque las medidas de seguridad protegen todas las formas de datos de pérdidas, ciberriesgos y robos de identidad. Dado que las empresas de telecomunicaciones gestionan infraestructuras críticas, un ciberataque podría tener un efecto significativo y de gran alcance.
Los datos de los clientes son otro objetivo clásico de alto impacto. Las empresas de telecomunicaciones suelen guardar datos personales de todos sus clientes,

Manufacturing

La fabricación también representa una parte importante de los ingresos de la ciberseguridad. Las consecuencias de una violación para las empresas manufactureras son la interrupción de las operaciones, la pérdida de propiedad intelectual (PI) y la pérdida de vidas humanas, en los casos más graves(*Cybersecurity in Manufacturing*, s. d.). Más allá de la interrupción de las operaciones, los atacantes también intentan robar datos, ya que gran parte de la propiedad intelectual que poseen los fabricantes son datos sobre los productos que se fabrican, el proceso y los tratamientos aplicados a los productos.

En cuanto a los distintos sectores, el estudio Mckinsey (*Organizational cyber maturity : A survey of industries*, 2021) presenta la madurez de las empresas por sectores.

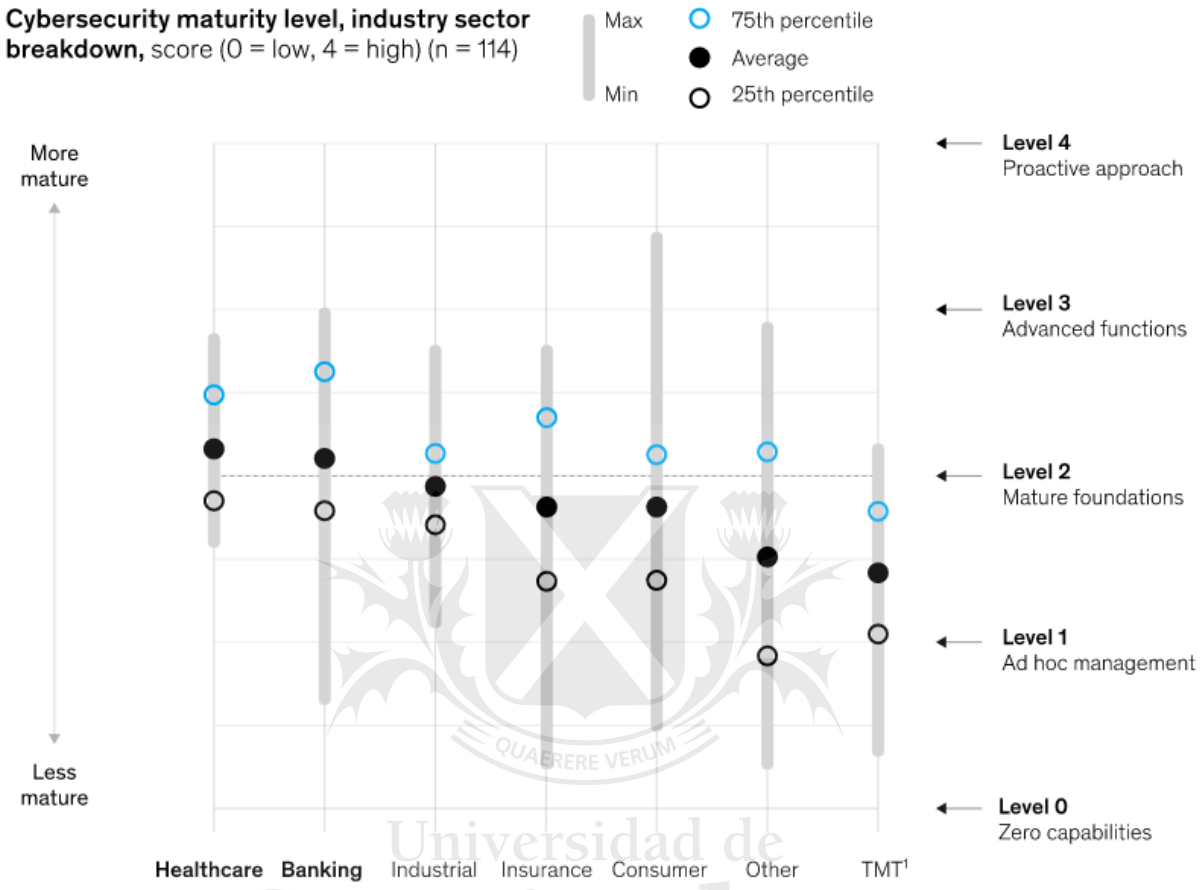


Figura 24. Madurez cibernética por sector

Podemos ver que la madurez media de las empresas también está relacionada con las cuotas de mercado que vimos antes. Están, por supuesto, los sectores sanitario y bancario. La madurez de estos sectores puede explicarse según tres criterios. En primer lugar, el entorno reglamentario específico del sector y la geografía. En segundo lugar, las expectativas de los clientes. En los sectores que están en contacto directo con los clientes, la ciberseguridad está más avanzada debido a las posibles violaciones de datos con consecuencias de largo alcance y a la creciente concienciación y exigencia de una mayor confidencialidad. Por último, existe la presión de los competidores y, por tanto, la pérdida de clientes si hay falta de confianza o confidencialidad.

Aunque la ciberseguridad responde a las expectativas específicas de un sector, también es necesario tener en cuenta las características específicas de las naciones en las que operan las empresas. La ciberseguridad es una preocupación global, y las empresas deben respetar tanto las prácticas del sector como el marco político, la normativa y los recursos disponibles.

Benchmark Nations

A escala internacional, existen desigualdades entre los países en términos de desarrollo de la ciberseguridad. Para entender qué países son los más avanzados, podemos comparar tres clasificaciones basadas en diferentes criterios.
Esta comparación de países nos permitirá después analizar las empresas de los distintos países y realizar un estudio comparativo para comprender globalmente cómo influye la ciberseguridad en la competitividad de las empresas.

El MIT ha publicado una clasificación de las 20 naciones digitales líderes en ciberseguridad. La clasificación ofrece una visión de la capacidad de respuesta a los ciberataques.
El estudio se basa en cuatro criterios

- infraestructura: se trata de evaluar la calidad de las telecomunicaciones, los servidores seguros y los centros de datos que sustentan la actividad económica del país
- recursos: se trata de evaluar diversos aspectos tecnológicos y jurídicos relacionados con el uso de los datos
- capacidad organizativa: se trata de evaluar la madurez de la ciberseguridad de las empresas y organizaciones del país

- compromiso político: se evalúa la comprensión, la calidad y la eficacia de la reglamentación de un país y la promoción de las prácticas de ciberseguridad.

The leaders	The 5 countries making the greatest progress and commitment toward creating a cyber defense environment.	1	Australia	7.83
		2	Netherlands	7.61
		3	South Korea	7.41
		4	United States	7.13
		5	Canada	6.94
The challengers	The 10 countries making progress or commitment toward creating a cyber defense enviroment.	6	Poland	6.91
		7	United Kingdom	6.79
		8	France	6.78
		9	Japan	6.71
		10	Switzerland	6.45
		11	Italy	6.37
		12	China	6.27
		13	Germany	6.24
		14	Spain	6.13
		15	Saudi Arabia	5.55
Strivers	The 5 countries making slow and uneven progress or commitment toward creating a cyber defense environment.	16	Mexico	5.31
		17	India	4.87
		18	Brazil	4.75
		19	Turkey	4.26
		20	Indonesia	3.46

Figura 25. Ranking MIT Technology review

El Índice de Ciberseguridad Global (GCI) es una referencia fiable que mide el compromiso de los países con la ciberseguridad a escala mundial, con el fin de concienciar sobre la importancia y las diferentes dimensiones de esta cuestión.

Los cinco pilares del GCI:

- Legal: Medido por la existencia de instituciones y marcos legales que se ocupan de la ciberseguridad y la ciberdelincuencia.
- Técnico: Medido en función de la existencia de instituciones y marcos técnicos que se ocupen de la ciberseguridad.
- Organizativo: Medido sobre la base de la existencia de instituciones de coordinación de políticas y estrategias para el desarrollo de la ciberseguridad a nivel nacional.
- Desarrollo de capacidades: Medido por la existencia de programas de investigación y desarrollo, educación y formación, profesionales certificados y organismos del sector público que apoyen el desarrollo de capacidades.
- Cooperación: Medida por la existencia de asociaciones, marcos de cooperación y redes de intercambio de información.

Characteristic	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
United States	100	20	20	20	20	20
United Kingdom	99.54	20	19.54	20	20	20
Saudi Arabia	99.54	20	19.54	20	20	20
Estonia	99.48	20	20	20	19.48	20
Korea (Rep. of)	98.52	20	19.54	18.98	20	20
Singapore	98.52	20	19.54	18.98	20	20
Spain	98.52	20	19.54	18.98	20	20
Russian Federation	98.06	20	19.08	18.98	20	20
United Arab Emirates	98.06	20	19.08	18.98	20	20
Malaysia	98.06	20	19.08	18.98	20	20

Figura 26. Ranking CGI

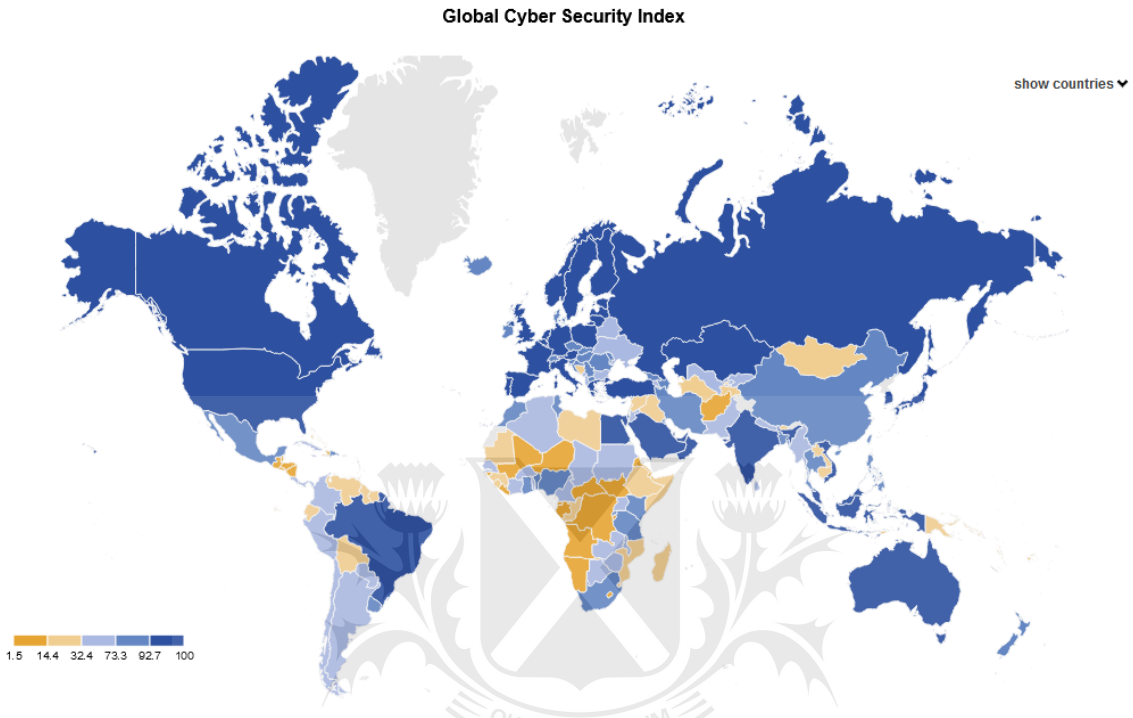


Figura 27. Mapa Global CyberSecurity Index

Últimamente, el national cyber security index (NCSI) mide el nivel de preparación para prevenir ciberamenazas e incidentes. Al igual que el GCI , el NCSI permite valorar los esfuerzos de las empresas en el ámbito digital y evaluar sus conocimientos.

El índice se ha desarrollado en 5 etapas:

- Identificación de las ciberamenazas a nivel nacional
- Identificación de las medidas y capacidades de ciberseguridad
- Selección de aspectos importantes y medibles
- Desarrollo de indicadores de ciberseguridad
- Consolidación de los indicadores de ciberseguridad

Rank	Country	National Cyber Security Index	Digital Development Level
1.	Belgium	94.81	74.07
2.	Lithuania	93.51	67.34
3.	Estonia	93.51	75.59
4.	Czech Republic	92.21	69.21
5.	Germany	90.91	80.01
6.	Romania	89.61	59.84
7.	Greece	89.61	64.02
8.	Portugal	89.61	68.46
9.	United Kingdom	89.61	79.96
10.	Spain	88.31	72.21

Figura 28. Ranking NCSI

Un benchmark de países nos permite identificar las naciones mejor preparadas en materia de ciberseguridad. Estudiando la metodología de las clasificaciones, podemos comprender qué mejores prácticas deben implantarse. Esto permite a las empresas establecerse en países donde se tendrá en cuenta la ciberseguridad. La colaboración entre países, gobiernos e industria ayuda a estimular toda esta innovación.
Además, la infraestructura del país será obviamente un factor positivo a la hora de desarrollar una estrategia eficaz de ciberseguridad.

Mientras los países ofrecen un marco preferente para el desarrollo de la ciberseguridad, ahora es crucial fijarse en las empresas que proporcionan soluciones de ciberseguridad.

Benchmark de las empresas de ciberseguridad

Para comprender el entorno en el que operan las empresas de ciberseguridad, podemos fijarnos en varias clasificaciones de empresas para entender cuáles son los principales actores del mercado. Si nos fijamos en los diversos artículos publicados en "Analytic insight", "Technology Magazine" y "Nomios", podemos ver que ciertas empresas aparecen una y otra vez. Entre ellas están Cisco, IBM security, Palo Alto Network, Crowd Strike y Fortinet.

En primer lugar, todas estas empresas tienen unos ingresos anuales superiores a los mil millones de euros. Por supuesto, la mayoría de estas empresas tienen su sede en California, que es el mayor caldo de cultivo tecnológico.

Para hacerse una idea clara del mercado, es esencial examinar más de cerca los negocios de estas empresas.

Palo Alto Network:

Palo Alto Networks Next-Generation Firewall, el NGFW, es una empresa famosa por su cortafuegos de última generación. Permite controlar el tráfico de red y comprobar quién entra y sale de la red. El firewall se considera la primera línea de defensa en la seguridad de la red.

Este firewall ha sido elegido 11 veces consecutivas mejor producto del mercado por el cuadrante mágico de Gartner (https://www.gartner.com/en/chat/magic-quadrant).

La empresa también ofrece otras funciones como VPN (red privada virtual), IPS (sistema de prevención de intrusiones) y UTM (gestión unificada de hilos).

Se dice que la empresa tiene un enfoque preventivo de la ciberseguridad, basado en la detección y filtrado de amenazas.

Ofrece sus servicios a pequeñas, medianas y grandes empresas.

Cisco Security:

Cisco security es una rama de Cisco Systems. La entidad de ciberseguridad se beneficia, por tanto, de la reputación y los recursos del gigante de las infraestructuras de red. La empresa también ofrece una amplia gama de soluciones, como IPS, firewall, cifrado de datos, seguridad en la nube y seguridad del correo electrónico.
Cisco es más antigua que Palo Alto Network y ofrece una gama de productos más variada. Además, Cisco Security desarrolla productos de seguridad directamente asociados a las tecnologías de nube que Cisco desarrolla y vende a sus clientes.

IBM Security:
Al igual que Cisco, IBM Security se beneficia de su reputación. La empresa también ofrece una gama completa de productos de seguridad. Proporciona sistemas de gestión de identidades para garantizar que se respetan los privilegios de los usuarios. Cada empresa podrá adaptar y elegir los productos de seguridad en función de sus necesidades y prioridades.

Crowd Strike:
Crowd Strike es una empresa estadounidense fundada en 2011. La empresa ofrece Falcon, una plataforma para asegurar los puntos finales en la nube. Proporciona protección contra el malware y las APT ("Advanced Persistent Threat"), así como protección de la identidad. Además de una gama de productos diversificada, la empresa ofrece servicios de gestión de incidentes y también es conocida por sus servicios de gestión de amenazas. (nombrada líder 2022 en inteligencia de amenazas por el cuadrante mágico de gartner)

Fortinet:
Fortinet también está especializada en firewalls de nueva generación. La empresa cuenta con una amplia gama de productos. La empresa ofrece una arquitectura que optimiza la interoperabilidad de productos de seguridad independientes, la Security

Fabric. Esta coordinación sería óptima para hacer frente a amenazas en constante evolución. Esta gestión centralizada sería una gran ventaja para la empresa.

Benchmark de formación

También hay una fuerte demanda de talentos en las profesiones relacionadas con la ciberseguridad. Para las empresas es crucial contar con los mejores talentos y expertos en ciberseguridad. Así que tenemos que mejorar la formación de los jóvenes en estas profesiones. Para contratar a los mejores, hay una serie de cursos, programas de formación y acreditaciones.

Existe una amplia gama de cursos de formación en ciberseguridad. En primer lugar, hay másters en las universidades de prestigio más conocidas. Según la clasificación de los 50 mejores másteres en seguridad de University HQ (*Top 50 Best Master's Cyber Security College and School Programs | UniversityHQ*, s. d.), no es de extrañar que los de Stanford ocupen el primer lugar. También están presentes los másteres de Berkley y Giorgiatech.

Estas universidades también ofrecen másteres en línea. Hay cursos recurrentes sobre redes, programación, criptografía y blockchain.

El máster de Harvard, que es un referente, tiene varios pilares. Entre ellos, cursos sobre seguridad en la nube, desarrollo de softwawre, cumplimiento y regulación, y optativas para especializarse en áreas como inteligencia artificial y seguridad, ética y la nube Azure de mircosoft.

También hay muchos cursos en línea. En Coursera, por ejemplo, encontrarás cursos muy valorados ofrecidos por IBM, Google y la Universidad de Nueva York.

También hay bootcamps de ciberseguridad, que combinan teoría y práctica. Entre ellos están Springboard Cybersecurity Bootcamp y Coding Dojo.

También existen certificaciones de ciberseguridad que acreditan un cierto nivel de conocimientos. Entre las más codiciadas están las certificaciones para iniciarse, como compTIA A+ y compTIA Security+.Para certificaciones de conocimiento de redes, están compTIA Network+ y Cisco CCNA.
Para penetración en redes, están compTIA PenTest+ y eJPT,Y por último, para certificar un nivel global completo de ciberseguridad, está la certificación Offencsive Security Certified Professional (OSCP).

Hemos podido analizar los distintos entornos, actores y productos del sector de la ciberseguridad desde distintos ángulos. Estos benchmarks nos permiten comprender mejor la complejidad del mercado y las fuerzas en juego. No todas las empresas tienen los mismos retos, el mismo framework o los mismos recursos. Ahora podemos construir una pauta a seguir para mejorar su estrategia de ciberseguridad.

VII. Roadmap

El objetivo del roadmap es dar a las empresas directrices para aprovechar las ventajas de la ciberseguridad. Hemos podido examinar la ciberseguridad desde distintos ángulos. Por lo tanto, vamos a considerar tantos parámetros como sea posible con el fin de proporcionar la mejor orientación a las empresas.

Diferentes exposiciones

Toda organización debe analizar su actividad y evaluar su dependencia de las tecnologías de la información y la comunicación. Como hemos visto, las expectativas de las distintas empresas, sectores y países son diferentes. No todas las empresas pueden seguir el mismo roadmap. No se adaptaría a las necesidades y riesgos de cada empresa. Así que hay que hacer una diferenciación inicial.

En el roadmap de (Bahuguna A et al. 2018), podemos distinguir cuatro tipos de dependencia.

El nivel 0 corresponde a operaciones totalmente independientes de las tecnologías de la información y la comunicación.

El nivel 1 corresponde a una dependencia limitada de las TIC. Las interrupciones de las TIC no tendrán un impacto importante en la organización.

En el nivel 2, las actividades de la organización dependen de las TIC. Sin embargo, las funciones críticas de la empresa no dependen de las TIC.

El nivel 3 corresponde a organizaciones que dependen totalmente
de las TIC. Las perturbaciones en la infraestructura de las TIC podrían provocar el fallo de todo el sistema.

Por tanto, toda empresa debe conocer su exposición a los riesgos asociados a las tecnologías de la información y la comunicación.

En cuanto al nivel 0, no es necesario desplegar muchos recursos para implantar un alto nivel de seguridad. La empresa no está expuesta a riesgos de ciberseguridad. Basta con que los usuarios y empleados sean conscientes de los riesgos de ciberseguridad. El factor humano es el más extendido en términos de riesgo en las empresas. Así que simplemente hay que concienciarlos.

Para el nivel 1, es aconsejable que las empresas poco dependientes de las tecnologías de la información y la comunicación adopten un nivel mínimo de seguridad. Así pues, los requisitos mínimos se dividen en cinco categorías:

- Inventario de hardware y software: debe conocer todos los terminales, equipos informáticos y software que utiliza. Debe ser capaz de catalogar todos sus recursos para identificar vulnerabilidades.
- Configuración segura de hardware y software: una configuración segura empieza por respetar protocolos de comunicación seguros como HTTPS. También implica aplicar actualizaciones y garantizar que los empleados siguen prácticas de ciberseguridad seguras.
- Análisis continuo de riesgos: debemos estar constantemente atentos a las vulnerabilidades y asegurarnos de que estamos al día en materia de ciberseguridad, ya que se trata de un campo que evoluciona rápidamente.
- Gestión de privilegios y control de acceso: como lo hemos visto, gestionar la identidad de los usuarios dentro de una empresa. Esto se aplica tanto a los empleados como a los clientes. Un sistema de gestión de identidades y accesos debe permitir controlar la identidad de todos.
- Soluciones antimalware: hay que detectar y proteger el malware. Hay muchas soluciones disponibles, sobre todo de los proveedores que hemos visto.

Para el nivel 2, es decir, empresas cuyas funciones críticas no dependen de las tecnologías de la información y la comunicación, recomendamos adoptar el framework del Center for Internet Security (CIS). Actualmente existen 18 controles:

-Inventario y control de los activos de la empresa
-Inventario y control de activos de software
-Protección de datos
-Configuración segura de activos empresariales y de software
-Gestión de cuentas
-Gestión del control de acceso
-Gestión continua de vulnerabilidades
-Gestión de registros de auditoría
-Protección del correo electrónico y del navegador web
-Defensa contra malware
-Recuperación de datos
-Gestión de infraestructuras de red
-Supervisión y defensa de la red
-Concienciación y formación en materia de seguridad
-Gestión de proveedores de servicios
-Seguridad del software de aplicación
-Gestión de respuesta a incidentes
-Pruebas de penetración

Este framework CIS puede corresponderse con el framework de ciberseguridad (CSF) publicado por el National Institute of Standards and Technology (NIST) (*CIS Controls v8 Mapping to NIST CSF*, s. d.), que veremos más adelantete. Por tanto, parece más prudente utilizar el equivalente del NIST, ya que es más completo. Así pues, las empresas pueden implantar el SIC basándose en el NIST. Una vez implantado, las empresas podrán ir más allá y alcanzar nuevos niveles de madurez sin tener que utilizar la metodología de otro framework.

Si ahora se trata de dependencias más importantes de las tecnologías de la información y la comunicación, recomendamos un enfoque diferente.

Para un nivel 3, ya habría que analizar la exposición al riesgo de forma más precisa y cuantificable.

Evaluar los riesgos de su empresa

Para las empresas que dependen de las tecnologías de la información y la comunicación, el primer paso esencial es evaluar sus riesgos y vulnerabilidades en materia de ciberseguridad. Un análisis de riesgos puede ayudar a una empresa a tomar decisiones de varias maneras (*Analyse des risques : quelle méthode pour les risques cyber ?*, s. d.):

- Alinee y asigne su presupuesto de seguridad de la información de forma más eficaz.
- Elija la solución de reducción de riesgos con el mejor rendimiento de la inversión.
- Comunicar los riesgos a la dirección y al consejo en términos financieros.
- Comprender los riesgos cibernéticos que plantean terceros a las empresas.
- Negociar el mejor seguro cibernético.
- Facilitar el cumplimiento normativo de su organización.

Esto plantea la cuestión de cómo pueden las empresas evaluar sus riesgos empresariales. Existen varios métodos, pero prácticamente todos se basan en una evaluación subjetiva de los riesgos de ciberseguridad. A menudo los llevan a cabo profesionales, pero el juicio de cada persona puede variar, por lo que puede ser difícil ponerse de acuerdo sobre todos los riesgos a los que se enfrenta una empresa. Lo hemos visto antes al evaluar la rentabilidad de una inversión en ciberseguridad. Las matrices de entrada se basan en la evaluación subjetiva de los expertos en ciberseguridad, que asocian un nivel de riesgo que luego se transforma en datos cuantitativos.

Existe un método de análisis de riesgos propuesto por la norma FAIR (Factor analysis of Information Risk). El modelo de análisis cuantitativo de riesgos FAIR define la gestión de riesgos como "la combinación de personal, políticas, procesos y tecnologías que permiten a una organización alcanzar y mantener de forma rentable un nivel aceptable

de exposición a pérdidas" (*The Importance and Effectiveness of Quantifying Cyber Risk*, s. d.). Este método está cada vez más extendido y es utilizado por las empresas. Adopta un enfoque matemático y se basa en factores como la probabilidad de que se produzca un suceso, el posible impacto financiero y las pérdidas potenciales.

FAIR propone una taxonomía del riesgo para ofrecer una visión completa, común y fija de las categorías de riesgo dentro de la organización. El riesgo asociado al escenario se desglosa en variables. El resultado es una estimación de la cantidad que la empresa podría perder. En este modelo hay dos tipos de pérdidas: primarias y secundarias. Las pérdidas primarias son los costes asociados a la productividad, la respuesta y la sustitución. Las pérdidas secundarias son los costes relacionados con la ventaja competitiva, la reputación y los costes relacionados con el marco jurídico.

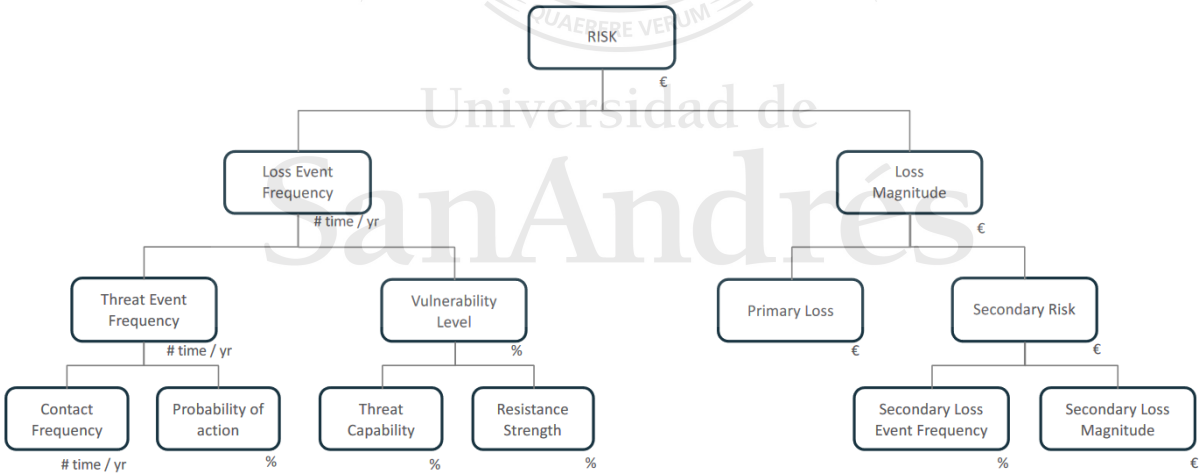


Figura 29. Taxonomía de los riesgos del método FAIR

Todo el método se basa en cuatro grandes etapas.

Alcance, para definir los activos, el ámbito de la organización y el objetivo del estudio. Recogida de datos y estimación de costes y probabilidades. La fase de cálculo,

utilizando funciones matemáticas y cadenas de Montecarlo en particular. Por último, los resultados y las respuestas a las preguntas sobre los niveles de riesgo, las principales amenazas, la reducción de riesgos, los ciberseguros y los beneficios y costes de un proyecto.

Este método permite cuantificar financieramente los riesgos a los que están expuestas las empresas. Este análisis de riesgos será un elemento clave para establecer una estrategia de ciberseguridad y aplicar un “Risk Based approach”.

Risk-based approach

La mayoría de las empresas que dependen de las tecnologías de la información y la comunicación se encuentran en una fase de “maturity based approach” (Boehm et al., 2019). Según el estudio de Mckinsey, el “maturity based approach” consiste en poner en marcha medidas para alcanzar un nivel de madurez objetivo. Este enfoque se centra en la creación de ciertas capacidades de ciberseguridad para alcanzar un nivel de madurez específico, en lugar de concentrarse en reducir los riesgos más críticos. Este enfoque presenta varios inconvenientes. En primer lugar, puede no ser suficiente para proteger a las empresas. En segundo lugar, es difícil medir el rendimiento de la inversión de las medidas implantadas. Por último, puede ser difícil de conseguir, porque los esfuerzos se reparten entre varios ámbitos y se acaba estancado en una situación que ya no avanza.

Para lograrlo, es aconsejable optar por una estrategia de “risk-based approach”. Esto implica identificar, evaluar y priorizar los riesgos de una organización, y después aplicar medidas de seguridad para reducir estos riesgos a un nivel aceptable. No es necesario implantar controles en toda la empresa, sino aumentar la seguridad donde sea necesario. Utilizar esta estrategia aumentará el nivel de seguridad y, al mismo tiempo, reducirá los costes de inversión.

Para aplicar un proceso de cambio hacia una estrategia de “risk-based approach”, se recomienda seguir estas ocho directrices:

1. Integrar plenamente la ciberseguridad en el framework de gestión de riesgos de la empresa.
2. Definir las fuentes de valor de la empresa en todos los equipos, procesos y tecnologías.
3. Comprender las vulnerabilidades de toda la empresa -en personas, procesos y tecnologías- a nivel interno y frente a terceros.
4. Comprender a los "actores de la amenaza", sus capacidades e intenciones.
5. Relacionar los controles de las actividades "en curso" y los programas de "cambio" con las vulnerabilidades que abordan, y determinar qué nuevos esfuerzos son necesarios.
6. Comparar los riesgos con el apetito de riesgo; informar sobre la reducción de riesgos.
7. Desarrollar una cultura de concienciación sobre los ciberriesgos.
8. Supervisar y mejorar continuamente el programa cibernético.

Si utilizamos el método FAIR descrito anteriormente, tendremos una buena visión general de los riesgos de la empresa. A continuación, podremos centrarnos en la respuesta a los riesgos que hayamos identificado y cuantificado. A continuación, nos corresponderá a cada uno de nosotros evaluar las distintas categorías del framework NIST para aplicar nuestra estrategia de ciberseguridad.

Roadmap NIST

Es importante tener en cuenta los frameworks más conocidos utilizados por las empresas. Entre ellos figura el cybersecurity framework (CSF) publicado por el Nacional Institute of Standards and Technology (NIST). Este framework consta de 50 páginas diseñadas para facilitar la gestión de riesgos. Hoy en día, es la principal autoridad en métodos de autoevaluación de los ciberriesgos y de aplicación de medidas preventivas y de protección. Constituye una metodología de gestión de la ciberseguridad. Es adecuado tanto para organizaciones privadas como públicas, y proporciona un framework para el proceso de identificación de riesgos, protección de los sistemas de información, detección y gestión de fallos de ciberseguridad y recuperación de los mismos.

Existen 4 niveles de madurez del framework.
El nivel 1 implica una gestión parcial del riesgo. Es más una cuestión de reacción que de prevención de riesgos.
El nivel 2 representa un marco de riesgo mejor. Existen procesos y herramientas, pero faltan medios de comunicación seguros.
El nivel 3 corresponde a una estrategia bien formalizada y priorizada. La empresa dispone de herramientas seguras y los empleados son conscientes de los riesgos.
El nivel 4 es el más alto. La empresa es capaz de protegerse y anticiparse a los riesgos.

El framework se basa en cinco funciones principales:

- Identificar: La Función Identificar ayuda a desarrollar una comprensión organizativa para gestionar el riesgo de ciberseguridad para sistemas, personas, activos, datos y capacidades. Comprender el contexto empresarial, los recursos que respaldan las funciones críticas y los riesgos de ciberseguridad relacionados permite a una organización centrar y priorizar sus esfuerzos, en consonancia con su estrategia de gestión de riesgos y sus necesidades empresariales.

- Proteger: La función de protección describe las salvaguardias adecuadas para garantizar la prestación de servicios de infraestructuras críticas. La función de protección apoya la capacidad de limitar o contener el impacto de un posible evento de ciberseguridad.
- Detectar: La Función de Detección define las actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad. La función de detección permite descubrir a tiempo los sucesos de ciberseguridad.
- Responder: la función Responder incluye las actividades apropiadas para tomar medidas en relación con un incidente de ciberseguridad detectado. La función Responder permite contener el impacto de un posible incidente de ciberseguridad.
- Recuperar: La función de recuperación identifica las actividades apropiadas para mantener los planes de resistencia y restaurar las capacidades o servicios que se hayan visto afectados por un incidente de ciberseguridad. La función de recuperación apoya la recuperación oportuna de las operaciones normales para reducir el impacto de un incidente de ciberseguridad.

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Figura 30. Función y categoría del NIST

Aplicar el CSF puede ser complicado porque depende de un proceso de evaluación que nadie puede validar. También existen otros métodos, como la ISO27001, pero esta dificultad persiste. Es difícil evaluar los riesgos y, en general, se trata de una evaluación subjetiva y cualitativa.

Con el método FAIR, estos riesgos pueden identificarse y cuantificarse. Ahora las empresas pueden orientar su estrategia en función de los riesgos.

VIII. Visión de la evolución de la ciberseguridad

Sensibilización

Creo que seguimos viviendo en un periodo de complacencia y que las empresas hacen la vista gorda ante la ciberseguridad y los riesgos y beneficios que puede aportar. Si tuviera que establecer una comparación entre la ciberseguridad y un médico, utilizaría la analogía de un médico y un paciente. La mayoría de las empresas esperan a ser atacadas para tomarse en serio la ciberseguridad, igual que un paciente esperaría a estar enfermo para preocuparse por su salud e ir al médico. Sin embargo, es mucho más eficaz, sostenible y saludable prevenir la enfermedad. Por lo tanto, las empresas con una actitud proactiva en materia de ciberseguridad ya tienen una ventaja sobre sus competidores.

En los próximos años, cada vez más empresas van a tener que adoptar la ciberseguridad en sus prácticas. Hoy en día, no se habla lo suficiente de ciberseguridad, de los riesgos y consecuencias que puede tener en una empresa o en la vida de las personas. En los últimos años, hemos asistido al auge del Big Data, de las capacidades de almacenamiento de datos y de la inteligencia artificial. Sin embargo, estas tecnologías han aparecido en nuestra vida cotidiana muy rápidamente, y el público en general ha podido disfrutar de sus beneficios sin comprender las desventajas.

La importancia de los datos personales, la privacidad y la confidencialidad se han convertido en nuevas cuestiones que debemos integrar en nuestra vida cotidiana.

Por ejemplo, hemos visto lo que empresas como Cambridge Analytica son capaces de hacer con nuestros datos personales. La empresa ha sido capaz de influir en elecciones en Estados Unidos, Europa y África. El uso malintencionado de nuestros datos personales puede incluso mermar nuestras libertades.

Por tanto, creo que la concienciación sobre los retos y objetivos de la ciberseguridad aumentará en un futuro próximo. Esta concienciación podría aumentarse suavemente a

través de la comunicación, la información y la educación. También podría adoptarse una línea más dura, con importantes consecuencias financieras y personales que obligaran a las empresas a adoptar la ciberseguridad.

Evolución de las amenazas y las defensas

Es difícil que las empresas y los empleados comprendan la ciberseguridad y se interesen por ella. Las tecnologías son demasiado avanzadas y los conceptos no se han popularizado lo suficiente como para que la gente quiera implicarse. Tenemos que dotar a la ciberseguridad de cierto encanto y atractivo para atraer el interés del gran público. Así que va a haber un gran trabajo de aprendizaje, enseñanza y educación de las empresas. Vamos a tener que hacer que los conceptos básicos de la ciberseguridad sean accesibles a todo el mundo.

Al mismo tiempo, las tecnologías evolucionan muy rápidamente y los ataques son cada vez más sofisticados. Así que es difícil mantenerse al día con la innovación y la tecnología. Así que va a ser aún más complejo apropiarse de tecnologías y conceptos cada vez más inventivos e innovadores.

Por un lado, creo que vamos a reducir enormemente las vulnerabilidades que hoy parecen básicas. Vamos a reducir el riesgo de ingeniería social, que actualmente es demasiado alto. También vamos a reducir el número de técnicas "sencillas" como el phising. Para ello habrá que aumentar la concienciación.
Por otra parte, las nuevas tecnologías de comunicación, almacenamiento y análisis aumentarán considerablemente las vulnerabilidades. Aumentarán las pérdidas financieras, lo que impulsará aún más la demanda de soluciones de ciberseguridad. Toda esta fase consistirá, como indica el estudio McKinsey, en ponerse a la altura del mercado actual y del mercado potencial.

Carrera tecnológica

Creo que hay tres tecnologías principales que influirán en la ciberseguridad en los próximos años.

Inteligencia Artificial

El desarrollo de la inteligencia artificial abre nuevas posibilidades en materia de ciberseguridad. Por un lado, permitirá desarrollar nuevos métodos de protección de las organizaciones. Podremos adoptar un enfoque más inteligente, rápido y adecuado para gestionar las amenazas, como detectar y clasificar el malware utilizando métodos tradicionales de aprendizaje automático o métodos de Deep Learning (Li 2018). Por otro lado, esto también abrirá la puerta a nuevas amenazas aún más desarrolladas. Por lo tanto, sigue siendo difícil confiar en la inteligencia artificial para desarrollar una estrategia de defensa. Así, el desarrollo de ciertos modelos debe llevarse a cabo con precaución, especialmente en lo que respecta a la forma en que se entrenan estos modelos de inteligencia artificial (Taddeo, McCutcheon y Floridi 2019). Por lo tanto, es aconsejable utilizar datos internos y seguros para alimentar los modelos. En cuanto aumentamos el riesgo proporcionando datos que alimentarán nuestro sistema, nos exponemos a fallos en el diseño y el rendimiento del sistema. También es necesario optimizar los modelos utilizando técnicas de aprendizaje adversarial, que se adaptarían bien a la ciberseguridad. Esto mejoraría la robustez de los modelos y daría buenos resultados en la detección de anomalías.

Además de estos métodos de detección y análisis del peligro, la inteligencia artificial sería útil para activar una respuesta adecuada en caso de peligro. Esto permitiría gestionar el problema lo antes posible y minimizar la duración de la exposición al riesgo.

Blockchain

Las tecnologías blockchain son evidentemente tecnologías que pueden ser útiles para la seguridad de las empresas. Ya sea por sus características de descentralización, no

modificación o cifrado, las ventajas de blockchain son recursos que las empresas pueden explotar. Aunque el uso de Ethereum y la tecnología de contratos inteligentes resuelve problemas de seguridad, el uso único de blockchain no resolverá todos los problemas de seguridad informática (Taylor et al. 2020). Además, por los tiempos de computación que requiere, todavía puede haber tiempos de latencia lentos para las máquinas que se comunican y utilizan las tecnologías blockchain.

Quantum computing

Microsoft afirma que podrá ofrecer un ordenador cuántico en menos de diez años. Argumentan que ya han hecho grandes avances en computación cuántica (*Accelerating scientific discovery with Azure Quantum - The Official Microsoft Blog*, s. d). "Científicos y empresas revolucionarán los componentes básicos de los productos cotidianos para dar paso a una nueva era de innovación y crecimiento económico. Juntos, podemos comprimir los próximos 250 años de química y ciencia de materiales en los próximos 25".

El ordenador cuántico supondría una potencia de cálculo exponencial. Esto volvería a poner en el punto de mira toda la ciberseguridad y, en particular, la criptografía. También repercutiría en la inteligencia artificial y el blockchain. Esta tecnología sería tan disruptiva que es difícil imaginar el futuro de la ciberseguridad.

Conclusión

Este estudio analiza el tema principal de la ciberseguridad para las empresas. Empezamos por identificar los principales objetivos de la ciberseguridad y el entorno mundial de la ciberseguridad. Respondemos a las primeras preguntas generales, es decir, qué es la ciberseguridad y cuáles son sus objetivos.

1) Analizamos el mercado y su potencial futuro. Analizamos el ecosistema de la ciberseguridad, presentando los riesgos, los productos disponibles y los principales actores de la ciberseguridad. A continuación, integramos la ciberseguridad en las estrategias de crecimiento exponencial. Para que la ciberseguridad mejore la competitividad de las empresas. A continuación, pudimos hacer una evaluación comparativa general de la ciberseguridad estudiando diferentes enfoques. Esto nos permitió comprender la realidad de la ciberseguridad en nuestra sociedad y elaborar una hoja de ruta realista y coherente para integrar la ciberseguridad en las empresas.

2) En el transcurso de este estudio, hemos podido extraer una serie de conclusiones que podrían contribuir a facilitar la integración de la ciberseguridad para las empresas.
    - Dado el gran número de ataques y los daños causados, debería haber una demanda mucho mayor por parte de las empresas en el mercado de la ciberseguridad. Hay una falta de inversión en este sector. Es necesario que las empresas tomen conciencia de la importancia de la ciberseguridad. Las empresas necesitan invertir más recursos para hacer frente a las vulnerabilidades.
    - Los ataques y las defensas en materia de ciberseguridad son muy complejos. Es una batalla técnica, estratégica y de gestión. Es difícil

encontrar razones que animen a las empresas a invertir en estas tecnologías.

3) Para que la ciberseguridad mejore la competitividad de una empresa, podemos identificar tres palancas principales de actuación:
    - la propuesta de valor,
    - el impulso del cambio hacia una cultura de ciberseguridad
    - la gestión de la rentabilidad.

4) Por último, tras realizar una serie de evaluaciones comparativas para comprender cómo se integra la ciberseguridad en su entorno, pudimos trazar una hoja de ruta a seguir. Todas estas conclusiones deberían ayudar a las empresas a darse cuenta de la importancia de la ciberseguridad. También hemos dado argumentos que justifican la inversión en ciberseguridad. Los beneficios son innegables y deben tenerse en cuenta para aumentar el interés de las empresas por la seguridad. Además, la hoja de ruta presentada puede inspirar a otras empresas a elaborar su propia hoja de ruta. Las empresas pueden inspirarse en los razonamientos y utilizar los distintos marcos que hemos estudiado. Esta estrategia también deberá combinarse con una gestión adecuada del cambio hacia la innovación y la ciberseguridad.

5) Durante este estudio, también constatamos las limitaciones que debe superar la ciberseguridad. Cada vez surgen más métodos para cuantificar los beneficios de la ciberseguridad. Sin embargo, sigue siendo difícil y a veces demasiado subjetivo evaluar claramente el impacto de la ciberseguridad para las empresas. Además, la percepción de la ciberseguridad debe cambiar para que se integre más fácilmente. Los ciudadanos siguen estando poco sensibilizados y tienen una mala imagen de la ciberseguridad. Por último, el desarrollo de la ciberseguridad debe estar en consonancia con el marco geopolítico y con el

sector empresarial específico. La ciberseguridad sigue siendo un campo muy complejo y en constante evolución. El panorama tecnológico cambia muy rápidamente y las tecnologías de ciberseguridad deben adaptarse al desarrollo de las nuevas tecnologías. Está claro que la ciberseguridad será cada vez más importante en los próximos años, y que las empresas tendrán que adaptarse a ella les guste o no.

Dentro de 5 o 10 años, creo que las tecnologías de la información y la comunicación habrán evolucionado considerablemente y serán adoptadas más ampliamente por la gente. El 5G estará ampliamente desarrollado en nuestras redes y tendremos acceso a internet en todo el mundo gracias a los satélites Starlink. Por tanto, todos los intercambios de datos se producirán muy rápidamente y la mayoría de las zonas desarrolladas y urbanas estarán ultraconectadas. La hiperconexión será, por tanto, una evolución de lo que ya conocemos con el Big Data y la inteligencia artificial, pero esta vez será omnipresente, más precisa y más útil en nuestra vida cotidiana. Todas estas tecnologías más avanzadas significan más almacenamiento, más datos y un procesamiento de datos más rápido y eficiente. Sin embargo, como hemos visto en este estudio, con las nuevas oportunidades vienen nuevas vulnerabilidades.

Empecemos por fijarnos en nuestra vida cotidiana como usuarios e imaginemos todas las vulnerabilidades de ciberseguridad que existen. Entendemos que hay mucho en juego, tanto a nivel individual como organizativo. Ahora tenemos que imaginar que lo que está en juego va a ser mucho mayor a medida que evolucione la tecnología. La ciberseguridad también seguirá esta tendencia e imagino que formará parte de nuestra vida cotidiana.

Creo que vamos a asistir a la aparición de sistemas de puntuación, como estamos viendo actualmente en el mercado de la alimentación y las bebidas. En Europa existen hoy aplicaciones y puntuaciones obligatorias en los productos alimentarios que evalúan la calidad nutricional de un producto (nutri score en Francia). También existe Yuka, que combina la calidad nutricional y la calidad del producto con la procedencia. Ahora están

apareciendo nuevos sistemas de puntuación para evaluar el impacto ecológico de lo que consumimos.

Todavía es difícil de imaginar, pero creo que evaluaremos nuestros productos para ver hasta qué punto son seguros. Seremos conscientes de los riesgos de comprar productos que no tengan seguridad integrada. Este fenómeno se acentuará aún más con la cadena de productos conectados de los que dependeremos.

Hoy dependemos sobre todo del teléfono y del ordenador, ambos conectables. Hemos visto la aparición de otros objetos como relojes, tabletas y coches. Así que estamos empezando a crear una malla conectada con todos estos objetos. Cada vez tenemos más objetos domóticos conectados al hogar, con asistencia por voz, altavoces conectados, lámparas, persianas aspiradoras y mucho más. Todas estas conexiones van a aumentar, por lo que esta cadena de objetos será vulnerable en todos los puntos de entrada. Así que habrá empresas que se harán con los nuevos objetos conectados, y las empresas que produzcan estos objetos tendrán que incorporar la seguridad en el corazón de su producto. De lo contrario, crearán vulnerabilidades que se revelarán al público en general, reduciendo así las ventas.

Al mismo tiempo, las empresas proveedoras de software de seguridad tendrán que hacer frente a nuevos retos. Tendrán que desarrollar soluciones para analizar, detectar, proteger y limpiar todos los canales conectados utilizados por los usuarios. Del mismo modo que podemos pagar por licencias de antivirus, podremos pagar por un software de seguridad que cubra todos nuestros terminales.

Sin embargo, esta hiperconexión también encontrará una fuerte oposición por parte del público. Habrá una forma de molestia y pérdida de libertad ante esta forma del Gran Hermano de 1984 escrito por George Orwell. Está bastante claro que los usuarios ya no desean ser analizados y espiados a lo largo de su día. Tendremos que crear cada vez más momentos alejados de todas estas tecnologías. Por tanto, la ciberseguridad tendrá un papel que desempeñar para proteger a los usuarios y desconectarlos de estas tecnologías.

Espero que este trabajo contribuya a llamar la atención sobre la importancia de la ciberseguridad. Este estudio trata de combinar varios enfoques y varias teorías empresariales que se adaptan a la ciberseguridad. Los consejos y conclusiones que pueden extraerse están abiertos a la interpretación y a la mejora. Las empresas tienen muchas formas de integrar la ciberseguridad y no existe una estrategia única. Al contrario, las empresas necesitan adquirir un cierto nivel de concienciación y madurez en innovación para ser ágiles y adaptarse a los retos que se avecinan.

Bibliografía

6 étapes pour créer une proposition de valeur [en ligne], (2021). Blog HubSpot : marketing, vente, relation client et site web. [Consulté le 7 août 2023]. Disponible sur : https://blog.hubspot.fr/marketing/proposition-de-valeur

Accelerating scientific discovery with Azure Quantum - The Official Microsoft Blog. (s. d.). The Official Microsoft Blog. https://blogs.microsoft.com/blog/2023/06/21/accelerating-scientific-discovery-with-azure-quantum/

Aiyer, B., Caso, J., Russell, P. et Sorel, M., (2022). New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers [en ligne]. McKinsey & ; Company. Disponible en: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers

Analyse des risques : quelle méthode pour les risques cyber ? (s. d.). Expert in Cyber Risk Quantification | C-Risk. https://www.c-risk.com/fr/blog/analyse-des-risques/

Baghai, M., Smit, S. et Viguerie, S. P., (2007). The granularity of growth [en ligne]. McKinsey & ; Company. [Consulté le 7 août 2023]. Disponible sur : https://www.mckinsey.com/featured-insights/employment-and-growth/the-granularity-of-growth

Bahuguna A, Bisht RK, Pande J (2018) Roadmap amid chaos: cyber security management for organisations. In: Proceedings of the ninth international conference on computing communication and networking technologies (ICCCNT), pp 1–6

Boehm, J., Curcio, N., Merrath, P., Shenton, L., & Tobias StÃ¤hle. (2019, 8 octobre). The risk-based approach to cybersecurity. McKinsey & ; Company. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-risk-based-approach-to-cybersecurity

Caso, J., Cole, Z., Patel, M. et Zhu, W., (2023). Cybersecurity for the IoT : how trust can unlock value [en ligne]. McKinsey & ; Company. [Consulté le 7 août 2023]. Disponible sur : https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/cybersecurity-for-the-iot-how-trust-can-unlock-value#/

CIS Controls v8 Mapping to NIST CSF. (s. d.). CIS. https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mapping-to-nist-csf

Cisco Secure Products and Solutions Cisco. Disponible en: https://www.cisco.com/site/us/en/products/security/index.html

Cybersecurity in Manufacturing. (s. d.). Databricks. https://www.databricks.com/blog/2023/03/01/cybersecurity-manufacturing.html

Cyber Security Market Share, Forecast | Growth Analysis [2030]. (s. d.). Fortune Business Insights™ | Global Market Research Reports & ; Consulting. https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165

Enterprise Security Solutions IBM - Deutschland | IBM.. Disponible en: https://www.ibm.com/security

Frambach, R. T. et Schillewaert, N., (2002). Organizational innovation adoption : a multi-level framework of determinants and opportunities for future research. Journal of Business Research [en ligne]. 55(2), 163–176. [Consulté le 8 août 2023]. Disponible sur : doi : 10.1016/s0148-2963(00)00152-1

Garvey, P. R., Moynihan, R. A. et Servi, L., (2012). A macro method for measuring economic-benefit returns on cybersecurity investments : The table top approach. Systems Engineering [en ligne]. 16(3), 313–328. [Consulté le 8 août 2023]. Disponible sur : doi : 10.1002/sys.21236

Global Leader of Cybersecurity Solutions and Services | Fortinet Fortinet. Disponible en: https://www.fortinet.com

Grube, J. W., Mayton, D. M. et Ball-Rokeach, S. J., (1994). Inducing Change in Values, Attitudes, and Behaviors : Belief System Theory and the Method of Value Self-Confrontation. Journal of Social Issues [en ligne]. 50(4), 153–173. [Consulté le 8 août 2023]. Disponible sur : doi : 10.1111/j.1540-4560.1994.tb01202.x

Hoffmann, R., Napiórkowski, J., Protasowicki, T. et Stanik, J., (2020). Risk based approach in scope of cybersecurity threats and requirements. Procedia Manufacturing.

Ishaq Azhar Mohammed. (2019). CLOUD IDENTITY AND ACCESS MANAGEMENT – A MODEL PROPOSAL. International Journal of Innovations in Engineering Research and Technology, 6(10), 1–8.

Joseph, S., (2022). Cybersecurity for Dummies. Wiley & Sons, Incorporated, John.

La cybersécurité dans les services financiers. (s. d.). EY Deutschland - Home | Building a better working world.
https://www.ey.com/fr_fr/innovation-financial-services/cybersecurity

La cybersécurité, un nouvel avantage concurrentiel pour les e-commerces ? [en ligne], (sans date). El Tigre – Software Solutions. [Consulté le 7 août 2023]. Disponible sur : https://el-tigre.net/blog/la-cybersecurite-un-nouvel-avantage-concurrentiel-pour-les-e-commerces/

Lee, I., (2021). Cybersecurity : risk management framework and investment cost analysis. Business Horizons [en ligne]. 64(5), 659–671. [Consulté le 8 août 2023]. Disponible sur : doi : 10.1016/j.bushor.2021.02.022

Les enjeux de la cybersécurité dans le secteur de la santé. (s. d.). IPAC Traductions. https://www.ipac-traductions.com/blog/la-cybersecurite-dans-le-secteur-de-la-sante-quels-sont-les-enjeux/

Les meilleures entreprises de cybersécurité à suivre en 2023 [en ligne], Nomios Belgique]. Disponible en : https://www.nomios.be/fr/actualite/meilleures-entreprises-cybersecurite-2023-2/

Li, J.-h., (2018). Cyber security meets artificial intelligence : a survey. Frontiers of Information Technology & ; Electronic Engineering . 19(12), 1462–1474.. Disponible en: doi : 10.1631/fitee.1800573

Mays N, Pope C. Qualitative research: rigour and qualitative research. BMJ 1995;311:109-12

Mercado de la ciberseguridad - Crecimiento, tendencias, impacto de COVID-19 y previsiones (2023-2028) disponible en https://www.mordorintelligence.com/fr/industry-reports/cyber-security-market

Network Security [en ligne], Palo Alto Networks. Disponible en: https://www.paloaltonetworks.com/network-security

Onwubiko, C. et Onwubiko, A., (2019). Cyber KPI for return on security investment. Dans : 2019 international conference on cyber situational awareness, data analytics and assessment (cyber SA), 3–4 juin 2019, Oxford, United Kingdom [en ligne]. IEEE. [Consulté le 8 août 2023]. Disponible sur : doi : 10.1109/cybersa.2019.8899375

Organizational cyber maturity : A survey of industries. (2021, 4 août). McKinsey & ; Company. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/organizational-cyber-maturity-a-survey-of-industries

Pearlson, K. et Huang, K., (2020). A Culture of Cybersecurity Can Be Your Competitive Advantage. MIT Sloan (CAMS) Research Consortium.

Penman and Nissim (2003) Ratio Analysis and Equity Valuation: From research to practice Review of Accounting Studies
6, pp. 109-154

Qu'est-ce qu'un avantage concurrentiel ? (+ exemples) [en ligne], (2022). Blog HubSpot : marketing, vente, relation client et site web. [Consulté le 7 août 2023]. Disponible sur : https://blog.hubspot.fr/marketing/avantage-concurrentiel

Renaud, K., Zimmermann, V., Schürmann, T. et Böhm, C., (2021). Exploring cybersecurity-related emotions and finding that they are challenging to measure. Humanities and Social Sciences Communications [en ligne]. 8(1). [Consulté le 7 août 2023]. Disponible sur : doi : 10.1057/s41599-021-00746-5

The Importance and Effectiveness of Quantifying Cyber Risk. (s. d.). Quantitative Information Risk Management | The FAIR Institute. https://www.fairinstitute.org/fair-risk-management

Thomson, D. G., (2005). Blueprint to a billion : 7 essentials to achieve exponential growth. Wiley.

Top 50 Best Master's Cyber Security College and School Programs | UniversityHQ. (s. d.). University HQ : Helping You Find The Best Ranked Online Colleges, Degrees & ; Programs. https://universityhq.org/degrees/online-masters-cybersecurity-programs/best-schools/

Taddeo, M., McCutcheon, T., & Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. Nature Machine Intelligence, 1(12), 557–560. doi:10.1038/s42256-019-0109-1

Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M. et Choo, K.-K. R., (2020). A systematic literature review of blockchain cyber security. Digital Communications and Networks . 6(2), 147–156. Disponible en: doi : 10.1016/j.dcan.2019.01.005

The CrowdStrike FalconÂ® platform crowdstrike.com.Disponible en: https://www.crowdstrike.com/falcon-platform/

Dejan Kosutic 2021, The Impact of Cybersecurity on Competitive Advantage

Top 10 Leading Cybersecurity Companies in the World You Should Know. Analytics Insight. Disponible en: https://www.analyticsinsight.net/top-10-leading-cybersecurity-companies-in-the-world-you-should-know/

Top 10 cybersecurity companies in the world in 2022 [en ligne], Home | Technology Magazine. Disponible en: https://technologymagazine.com/articles/top-10-cybersecurity-companies-in-the-world-in-2022

Western Alliance Bank Cyber Security. (s. d.). Business Banking | Western Alliance Bank. https://www.westernalliancebancorporation.com/insights/western-alliance-bank-cyber-security

Western Alliance Bank launches new technology hub. (s. d.). Retail Banker International. https://www.retailbankerinternational.com/news/western-alliance-bank-technology-hub/

What is Cloud Security ? Cloud Security Defined | IBM Disponible en: https://www.ibm.com/topics/cloud-security

What is Network Security ? Forcepoint. Disponible en: https://www.forcepoint.com/fr/cyber-edu/network-security

William D. Eggers, Government’s cyber challenge, 2016 disponible en https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/risk/DR19-governments-cyber-challenge.pdf