OBS Business School

Ciberseguridad en pandemia: ¿Riesgo u oportunidad?

Óscar Quero Hijano
Business Information Manager en la multinacional Teladoc Health y Director del Máster en Ciberseguridad de OBS Business School.

Septiembre, 2021

Partners Académicos:

Universitat de Barcelona

ulc barcelona

obsbusiness.school

Autor

Óscar Quero Hijano

Colaborador de
OBS Business School

Óscar Quero Hijano, Business Information Manager, Certificado en Fundamentos de ITIL y con un Postgrado en Business Intelligence, y con más de 15 años de experiencia gestionando proyectos de Business Intelligence para diferentes empresas multinacionales, pertenecientes a multitud de sectores (Farma, Banca, Media, Seguros, Retail, Servicios). En la actualidad es Business Information Manager en la multinacional Teladoc Health, siendo responsable de los sistemas analíticos, dando soporte a los diferentes departamentos y a los clientes de EMEA, Asia y Pacífico. Tiene experiencia en una gran variedad de plataformas de Business Intelligence: Microstrategy, Business Objects, Microsoft BI y PowerPivot, Qlikview, Pentaho, entre otras.

Índice

Capítulo 1

Introducción

Qué es la ciberseguridad

La ciberseguridad, concepto muy actual en estos momentos por lo que ha generado la pandemia, es una noción genérica que cubre muchos aspectos. Si tuviéramos que dar una definición más concreta, podríamos quedarnos con la que Kaspersky incluye en su artículo "¿Qué es la ciberseguridad?" (2021): "La ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos".

Como puede verse, se trata de un concepto que, en toda su amplitud, cubre todos los elementos considerados como "tecnología", por lo que su impacto real en la sociedad actual es muy importante. Definamos algunas de las categorías más habituales en las que se suele trabajar en las compañías:

- **Seguridad en una red:** Es el conjunto de técnicas, desarrollos y procesos que ayudan a mantener la red protegida de accesos no autorizados por parte de personas (u organizaciones) ajenas a la compañía. También dentro de esta categoría se incluye el *malware* o programas "maliciosos", creados específicamente para provocar daños en las compañías, ya sea "secuestrando" equipos y/o información, o accediendo a datos de alto valor con los que obtener beneficios.
- **Seguridad de la información:** Es el conjunto de acciones y medidas que permiten proteger los datos de una empresa, salvaguardando tres aspectos críticos: Disponibilidad, confidencialidad e integridad.
- **Seguridad de las aplicaciones:** Todas las compañías y los usuarios domésticos tenemos aplicaciones, que deben cumplir con las medidas necesarias y suficientes para evitar ser vulneradas y afectar a los equipos que las contienen, poniendo en riesgo la información almacenada y, por extensión, a los propios usuarios.
- **Formación de los usuarios:** El usuario, ya sea profesional o doméstico, es la mayor amenaza de seguridad existente, ya que, por muchos procesos y medidas que instauremos, si estos procedimientos no se cumplen por parte del personal, difícilmente lograremos evitar y/o mitigar los riesgos. Es por esto por lo que es clave formar a las personas con planes adecuados a su perfil, con el fin último de reducir al mínimo los incidentes de seguridad que puedan ocurrir (el riesgo cero no existe).

Capítulo 2

La ciberseguridad en época de pandemia

1 El antes y el después

La ciberseguridad no ha sido una prioridad para muchas de las compañías hasta que llegó la pandemia. Antes de la pandemia más del 75 % de las compañías podían vivir sin planes de seguridad sobre los potenciales ataques y, en palabras de muchos de ellos, no estarían preparados para reaccionar de forma adecuada a un ataque.

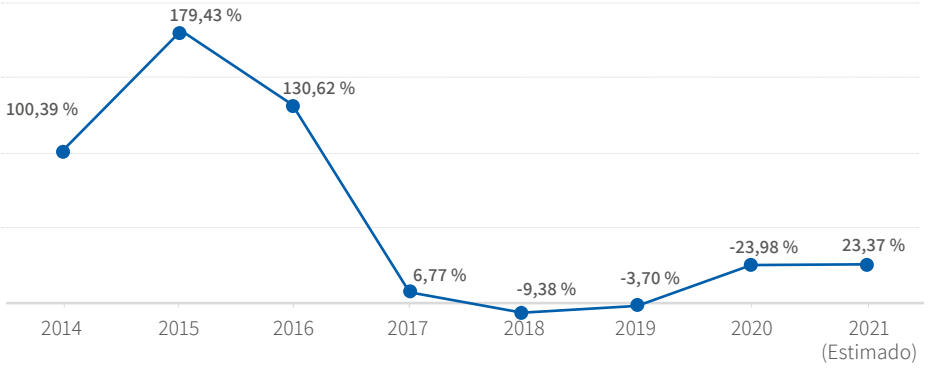
Este planteamiento es totalmente equivocado, máxime por la evolución del número de ciberataques que se está produciendo en los últimos años. Según datos del CNI-CERT (Centro Criptológico Nacional de España), ya desde 2018 se empezaba a ver un incremento preocupante en el número de ciberataques a empresas españolas (más de un 40 % en 2018).

Si nos basamos en los datos reportados por INCIBE, se puede ver que la pandemia ha generado un mayor número de incidentes de seguridad, al menos en base a lo que ha sido reportado a este organismo.

Si nos quedamos solo en el incremento relativo:

Figura 01 ⟶ INCIBE - ESPAÑA - INCIDENTES DE SEGURIDAD

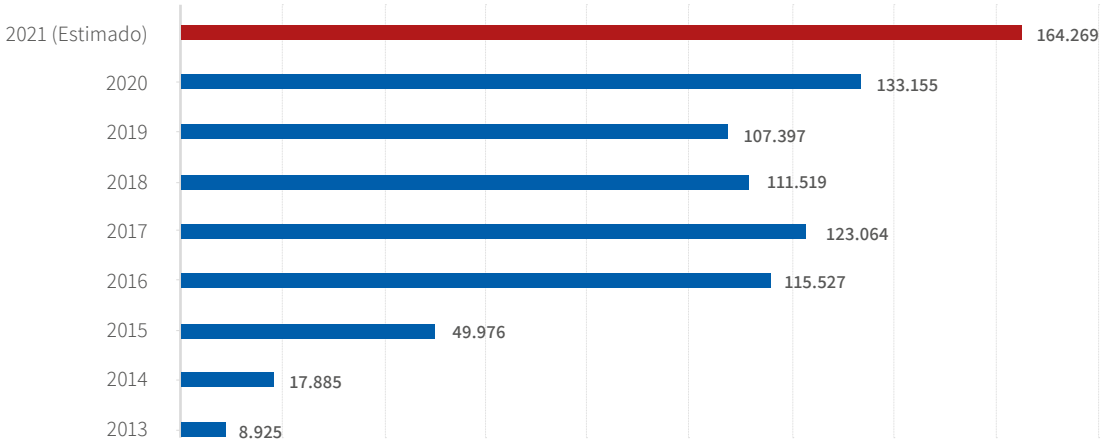
Fuente: INCIBE y estimación propia.



Puede parecer que el incremento no es tan acusado, ya que se ve que los mayores porcentajes están en 2014, 2015 y 2016. Sin embargo, esta no es la realidad, tal y como muestran las estadísticas absolutas:

Figura 02 → INCIBE - ESPAÑA - INCIDENTES SEGURIDAD

Fuente: INCIBE y estimación propia.

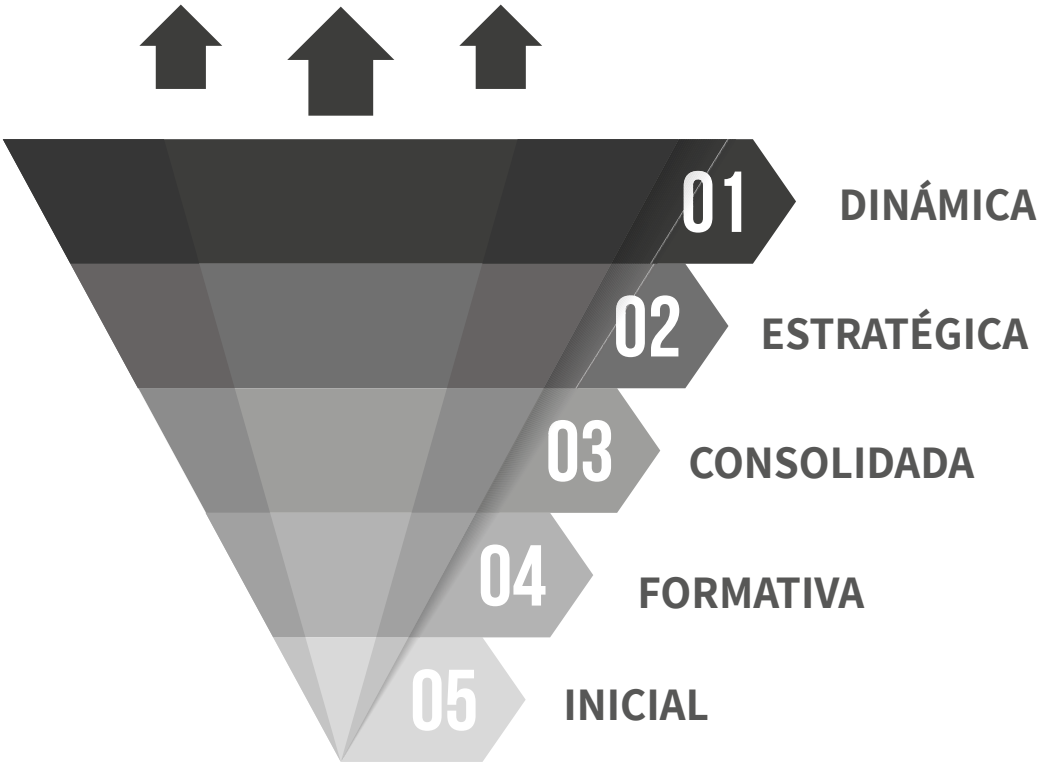


Como se puede ver de forma muy clara, hubo un gran incremento en 2016, situación que se estabilizó en los siguientes años, pero que ha experimentado un repunte importante en 2020, coincidiendo con la pandemia. Si, en base a los datos que tenemos, realizamos una estimación lineal de cómo acabaremos 2021, vemos que la tendencia natural nos lleva a otro crecimiento importante, similar al experimentado en 2020 en términos relativos, lo que trae un pensamiento a la cabeza: ¿Deberíamos empezar a preocuparnos? ¿Las empresas están realmente preparadas para protegerse de una posible avalancha de ataques cada vez más masivos y, posiblemente, ingeniosos?

Si ahora nos vamos a Latinoamérica, el panorama es, en apariencia, muy diferente. Según un informe presentado por Fortinet en Panamá (Marzo 2020), en 2019 hubo en América Latina 85 billones de ataques, mientras que en 2020 la cantidad se redujo a unos 41 billones, habiendo empezado el primer trimestre de 2021 con 7 000 millones (principalmente *malware* y uso de las redes sociales para difundir información de sitios web falsos). ¿A qué puede deberse esta tendencia tan contraria? En base a la información analizada, todo se debe al diferente nivel de madurez que existe tanto en empresas como en usuarios en cuanto a la digitalización y servicios tecnológicos.

Según un informe del Banco Interamericano de Desarrollo, titulado "Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe", las empresas y usuarios de América Latina tienen niveles de madurez bastante bajos, comparado con empresas y usuarios europeos, por ejemplo.

Antes de analizar la situación de los países, es importante explicar cómo funciona el modelo de madurez para ciberseguridad.



Este modelo de madurez se basa en cinco niveles, por los que se debe ir pasando secuencialmente:

- **Inicial:** No hay ningún tipo de madurez o se está empezando a trabajar la ciberseguridad.
- **Formativa:** Se realizan actividades, pero siempre son ad hoc y desorganizadas.
- **Consolidada:** Ya existen indicadores definidos para medirlo todo, pero no hay recursos humanos dedicados.
- **Estratégica:** Existe una estrategia clara en materia de ciberseguridad.
- **Dinámica:** La empresa es lo suficientemente capaz como para adaptar su estrategia en función del entorno y situaciones específicas.

Para evaluar estos niveles de madurez, se realiza un análisis en base a las siguientes dimensiones:

- Política y Estrategia de Ciberseguridad

Dimensión 1 **Política y Estrategia de Ciberseguridad** (Diseño de estrategia y resiliencia de ciberseguridad)	**D1.1** Estrategia Nacional de Ciberseguridad
	D1.2 Respuesta a Incidentes
	D1.3 Protección de Infraestructura Crítica (IC)
	D1.4 Gestión de Crisis
	D1.5 Defensa Cibernética
	D1.6 Redundancia de Comunicaciones

- Cultura Cibernética y Sociedad

Dimensión 2 **Cultura Cibernética y Sociedad** (Fomentar una cultura de ciberseguridad responsable en la sociedad)	**D2.1** Mentalidad de Ciberseguridad
	D2.2 Confianza y Seguridad en Internet
	D2.3 Comprensión del Usuario de la Protección de Información Personal en Línea
	D2.4 Mecanismos de Presentación de Informes
	D2.5 Medios y Redes Sociales

- Educación, Capacitación y Habilidades en Ciberseguridad

Dimensión 3 **Educación, Capacitación y Habilidades en Ciberseguridad** (Desarrollo del conocimiento de ciberseguridad)	**D3.1** Sensibilización
	D3.2 Marco para la Educación
	D3 .3 Marco para la Formación Profesional

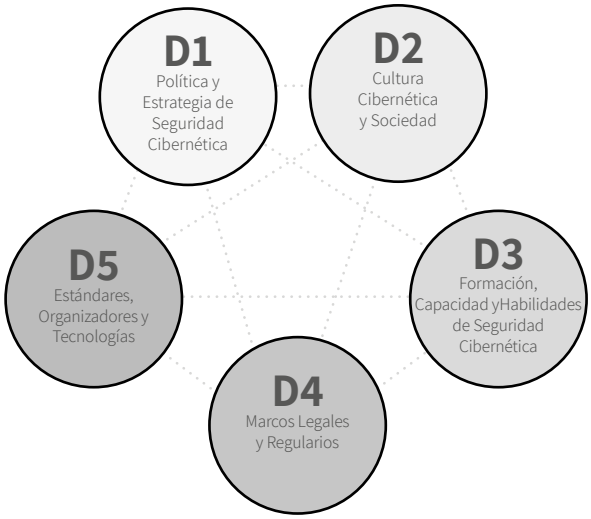
- Marcos Legales y Regulatorios

Dimensión 4 **Marcos Legales y Regulatorios** (Creación de marcos legales y regulatorios efectivos)	**D4.1** Marcos Legales
	D4.2 Sistema de Justicia Penal
	D4.3 Marcos de Cooperación Formal e Informal para el Delito Cibernético

- Estándares, Organizaciones y Tecnologías

Dimensión 5 **Estándares, Organizaciones y Tecnologías** (Control de riesgos a través de estándares, organizaciones y tecnologías)	**D5.1** Adhesión a los Estándares
	D5.2 Resiliencia de Infraestructura de Internet
	D5.3 Calidad del Software
	D5.4 Controles Técnicos de Seguridad
	D5.5 Controles Criptográficos
	D5.6 Mercado de Ciberseguridad
	D5.7 Divulgación Responsable

Naturalmente, las cinco dimensiones anteriores se hallan íntimamente relacionadas:



Aunque el informe citado contiene un análisis comparativo 2016-2020 de todos los países, es más importante hacer foco en dos de ellos, uno con un perfil más avanzado (México) y otro emergente (Perú):

México

Datos generales

Habitantes Ref: Banco Mundial*	Abonos a teléfonos celulares Ref: ITU**	Personas con acceso a Internet	Porcentaje de penetración de Internet Ref: ITU**
124.777.324	**114.329.353**	**79.673.128**	**64 %**
2017	2017	2017	2017

Dimensiones

D1	2016	2020
Política y Estrategia de Seguridad Cibernética		
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia		
Organización		
Contenido		
1-2 Respuesta a Incidentes		
Identificación de Incidentes		
Organización		
Coordinación		
Modo de Operación		
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación		
Organización		
Gestión de Riesgos y Respuesta		
1-4 Manejo de Crisis		
Manejo de Crisis		
1-5 Defensa Cibernética		
Estrategia		
Organización		
Coordinación		
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones		

D2	2016	2020
Cultura Cibernética y Sociedad		
2-1 Mentalidad de Seguridad Cibernética		
Gobierno		
Sector Privado		
Usuarios		
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario		
Confianza del Usuario en los Servicios de Gobierno Electrónico		
Confianza del Usuario en los Servicios de Comercio Electrónico		
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea		
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia		
2-5 Medios y Redes Sociales		
Medios y Redes Sociales		

Análisis

Aunque se ha continuado con la estrategia nacional en materia de ciberseguridad, potenciándola aún más, se ha trabajado mucho al usuario no profesional, logrando que entienda los riesgos que supone Internet y las redes sociales, además de proveer de mecanismos para canalizar las denuncias. Además, se ha fortalecido mucho el área legislativa, sobre todo en materias tan sensibles como la protección al menor.

Perú

Datos generales

Habitantes	Abonos a teléfonos celulares	Personas con acceso a Internet	Porcentaje de penetración de Internet
Ref: Banco Mundial*	Ref: ITU**		Ref: ITU**
31.444.297	**38.915.386**	**15.322.061**	**49 %**
2017	2017	2017	2017

Dimensiones

D1	2016	2020
Política y Estrategia de Seguridad Cibernética		
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia		
Organización		
Contenido		
1-2 Respuesta a Incidentes		
Identificación de Incidentes		
Organización		
Coordinación		
Modo de Operación		
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación		
Organización		
Gestión de Riesgos y Respuesta		
1-4 Manejo de Crisis		
Manejo de Crisis		
1-5 Defensa Cibernética		
Estrategia		
Organización		
Coordinación		
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones		

D2	2016	2020
Cultura Cibernética y Sociedad		
2-1 Mentalidad de Seguridad Cibernética		
Gobierno		
Sector Privado		
Usuarios		
2-2 Confianza y Seguridad en Internet		
Confianzay Seguridad en el Internet del Usuario		
Confianza del Usuario en los Servicios de Gobierno Electrónico		
Confianza del Usuario en los Servicios de Comercio Electrónico		
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea		
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia		
2-5 Medios y Redes Sociales		
Medios y Redes Sociales		

Análisis

Perú es un país menos digitalizado y eso tiene impacto en la madurez. Como puede verse en las tablas anteriores, si bien se ha avanzado en temas de legislación (donde no existía nada), se ha progresado muy poco en el resto de los apartados, con la única diferencia de la educación de la ciudadanía en aspectos de seguridad en entornos digitales.

Aunque estos son solo dos ejemplos, la realidad de América Latina es que su nivel de madurez es bajo (hay pocos o nulos avances en dos tercios de los países), y esto impacta en un bajo uso de sistemas digitales, por lo que el riesgo de ciberataques es menor. No obstante, la pandemia ha provocado una aceleración de la adopción en estos países, por lo que la pregunta que surge es la siguiente: ¿Están preparadas las compañías latinoamericanas para un entorno digital?

2 Los ataques durante la pandemia

El hecho de que se estén usando de forma muy intensa todas las plataformas digitales ha generado que los ciberataques se focalicen aún más en determinados servicios, con el fin claro del robo de información para fines delictivos.

Según se comenta en un artículo de ESED, titulado "Los ciberataques más comunes durante la pandemia del Covid-19 y ejemplos", este sería un listado de los ataques más frecuentes durante la pandemia:

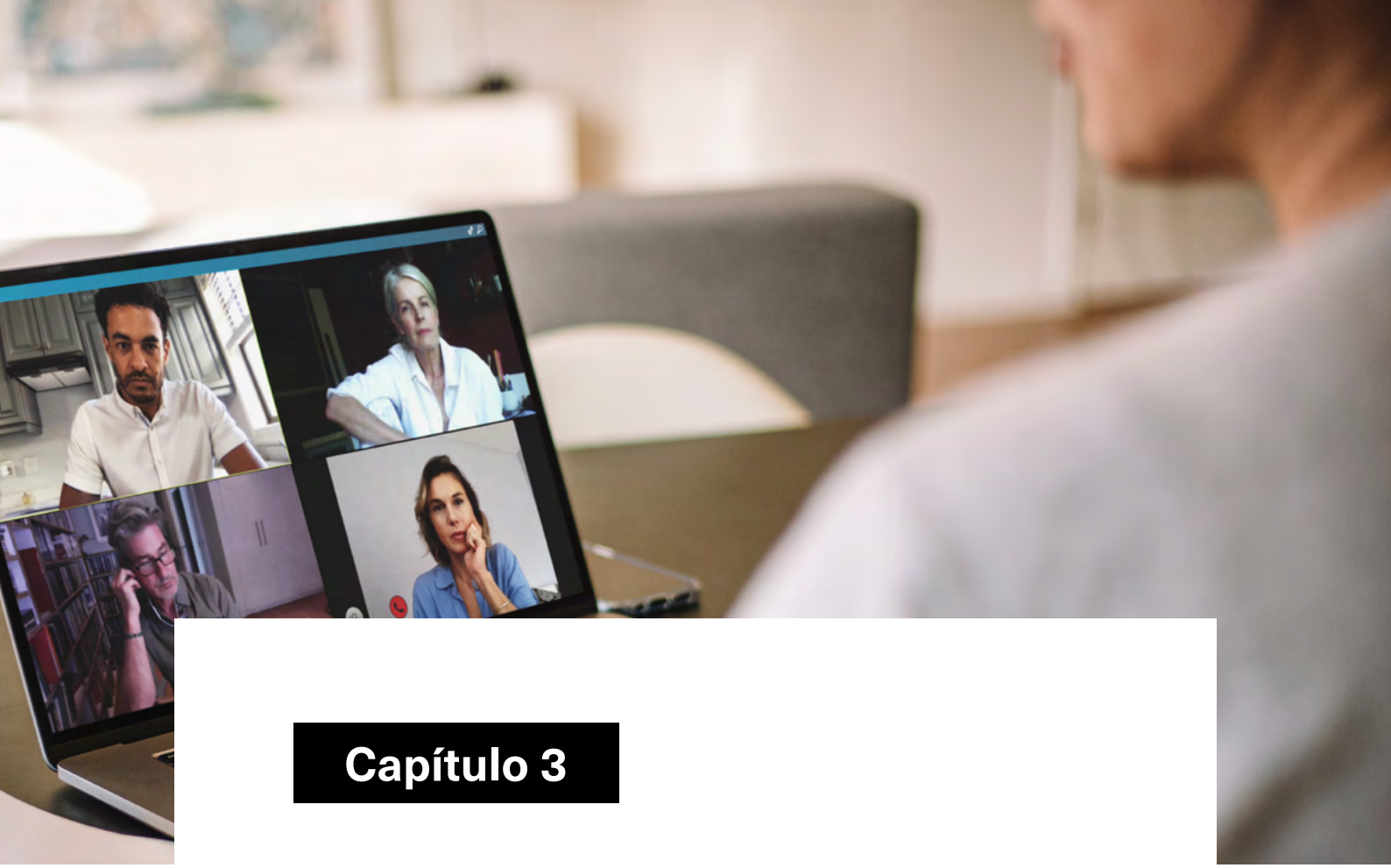
- **Phising**
  Este es el ataque más común, acrecentado por el uso intensivo que realizamos de las aplicaciones digitales por la pandemia. En este ataque, el objetivo recibe un correo electrónico que parece realmente del proveedor del servicio, requiriéndole que verifique ciertos datos y/o pinche en un enlace para realizar determinada acción. Un ejemplo podrían ser las comunicaciones sobre supuestos "problemas con subscripciones" en plataformas de contenidos. Suelen ser mails verdaderamente logrados y con pocos defectos, por lo que es probable que el usuario "pique". Otro ejemplo serían los correos en idiomas no comunes para el receptor o con traducciones parciales y/o erróneas, aunque estos son más fáciles de detectar, si bien es cierto que los usuarios menos habituados al uso de los medios digitales (normalmente de edad avanzada o niños) son muy proclives a caer.

- **Ciberataques contra centros sanitarios**
  Desde el inicio de la pandemia, ya por marzo 2020, se empezaron a recibir ataques de *malware* en centros de atención sanitaria, con el único objetivo de bloquear los sistemas y pedir un rescate.

- **Ofertas falsas de puestos de trabajo**
  Los ciberdelincuentes han detectado una oportunidad en la incertidumbre laboral generada por la pandemia, y han empezado a inundar Internet de ofertas falsas, con el único fin de recabar datos de carácter personal de los usuarios para utilizar en estafas de diferentes tipos, incluida la suplantación de identidad.

- **Páginas falsas para recaudar ayudas para afectados por el COVID-19**
  Esta es la estafa más deleznable, ya que se aprovecha del buen corazón de las personas. Los ciberdelincuentes diseñan y publican páginas web para recaudar fondos con la excusa del COVID-19, utilizando en muchos casos imágenes de empresas o asociaciones.

Es importante remarcar que, según organismos oficiales en España como por ejemplo Incibe, más de la mitad de los incidentes de seguridad se deben a dos motivos: intrusiones y *malware*, siendo las familias de *malware* más utilizadas Emolet, Unholy Trinity y Magecart.



Capítulo 3

El teletrabajo y la ciberseguridad

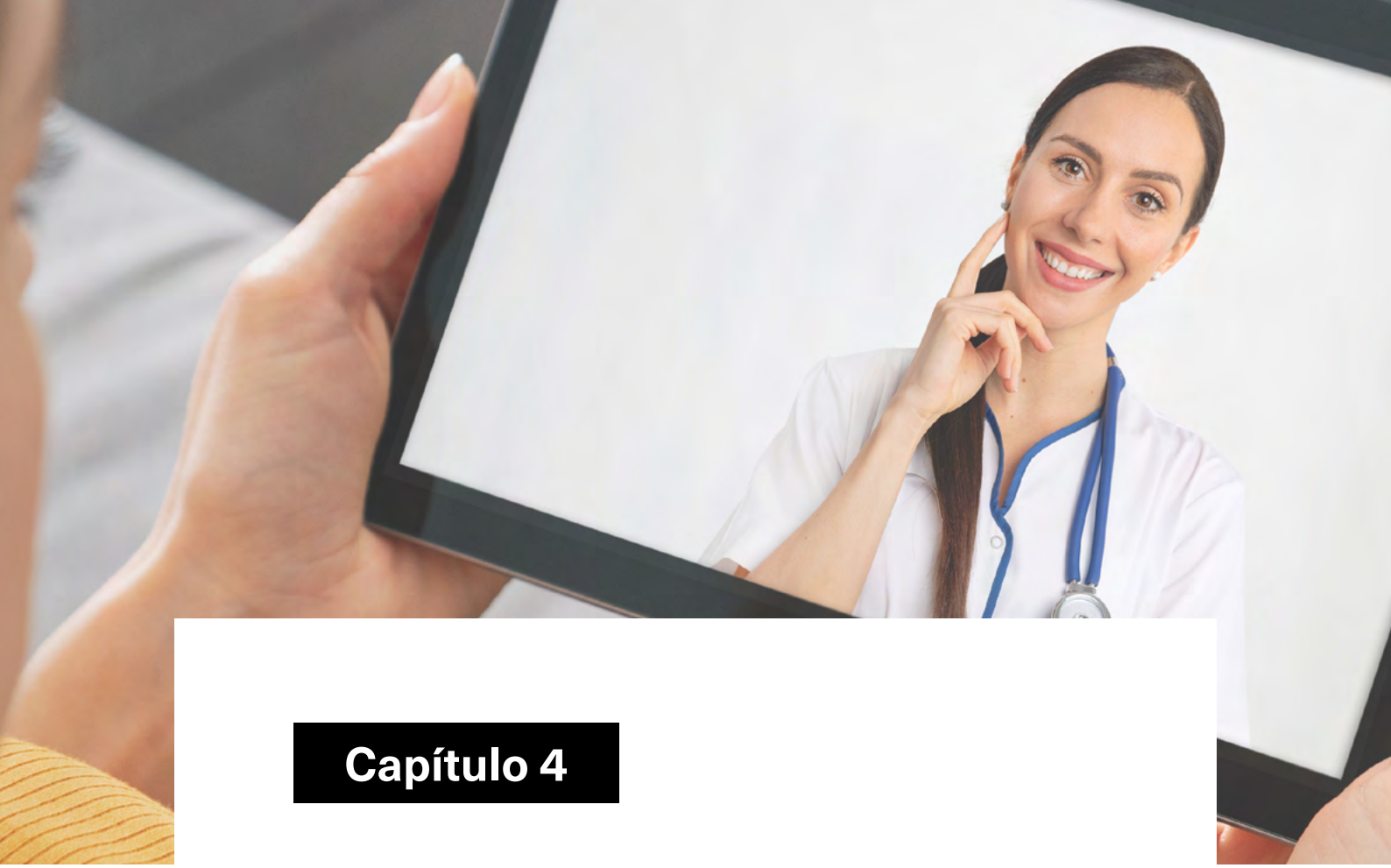
El teletrabajo ha pasado de ser una opción, utilizada por las empresas para captar capital humano, a ser una necesidad, ya que muchas compañías no habrían podido operar sin esta modalidad durante la pandemia. Según los datos de Adecco Group Institute, en España hay unos 3 millones de personas que teletrabajan, de las que poco más de 1 millón se generaron por la pandemia (un 33 %), lo que supone un incremento considerable del número de trabajadores que utilizan esta modalidad (en estos momentos forzosa en innumerables casos).

Este volumen, que puede parecer alto a priori, solo representa alrededor del 15 % de los ocupados, lo que, comparado con otros países de la UE, resulta muy bajo. Países vecinos como Portugal (20,7 %) o Francia (28,3 %) tienen tasas muy superiores a España, siendo los países del norte de Europa como Suecia (40,9 %) y Holanda (40,1 %) los que más lo fomentan. Pero ¿es el teletrabajo una herramienta coyuntural o se convertirá en la opción mayoritaria? La respuesta en estos momentos no está clara, ya que hay un factor que no estamos teniendo en cuenta e impacta en estas decisiones: la cultura empresarial de las empresas de los diferentes países.

Uno de los mayores frenos que muchas empresas tienen a la hora de instaurar o expandir el teletrabajo es la seguridad. Cuando un empleado trabaja desde casa, está utilizando sus propios recursos y no hay un control sobre el uso personal que hace de los mismos, por lo que hay un miedo inherente a que los activos de la empresa estén en riesgo por los propios empleados.

¿Cómo pueden protegerse las empresas? Lo primero, y más importante, es que los empleados no utilicen su ordenador personal para acceder a los recursos de la empresa, máxime cuando se trate de un dispositivo no controlado y/o gestionado (aquí habría que incluir los BYOD). Una vez el empleado dispone de un equipo gestionado por la empresa, hay que asegurar que dispone de un antivirus correctamente configurado, que no pueda ser deshabilitado, para evitar cualquier amenaza directa conocida. Por último, es obligado el uso de una VPN para conectar con la empresa, ya que de lo contrario la información fluirá por Internet sin ningún tipo de protección y cualquier persona que la capte podrá hacerse con información sensible (usuarios, contraseñas, IPs, nombres de equipos, datos…).

Con estas medidas protegemos del lado del empleado, pero: ¿qué debemos hacer del lado de la empresa? Aquí la clave, aparte de implementar la infraestructura necesaria para dar cobertura a todo lo anterior, es establecer una política de copias de seguridad consistente, que proteja a la compañía de pérdidas de información. La recomendación es siempre que se realicen varias copias de seguridad, guardándose al menos una de ellas fuera de la empresa (la nube puede ser una buena ubicación).



Capítulo 4

La ciberseguridad y los nuevos servicios digitales

1 La telemedicina

La telemedicina, es decir, el uso de servicios médicos por medios digitales se está convirtiendo en la opción mayoritaria por parte de las empresas (finales y de seguros) para ofertar este tipo de servicios. Muchas compañías a nivel mundial están lanzando este nuevo modelo de atención, donde el usuario contacta con los facultativos de forma telemática (llamada o videoconsulta), pudiéndose realizar lo mismo que en una consulta presencial, pero sin moverte del lugar donde te encuentras.

Esto, en un momento como el actual de pandemia, con los servicios públicos colapsados y un miedo (lógico, por otro lado) a acudir a un centro médico y contagiarte, es una opción mayoritariamente elegida y que está ayudando a que los usuarios no se queden sin atención ante dolencias leves o moderadas, dolencias que en esta situación de *stress* sanitario podrían quedarse sin tratamiento y empeorar con el paso del tiempo.

Si ya antes podríamos estar preocupados por la seguridad de nuestros datos en los centros sanitarios, el hecho de que la información fluya desde multitud de dispositivos personales supone un riesgo importante, ya que la información de salud está catalogada como de muy alta protección según el Reglamento General de Protección de Datos. Por tanto, las compañías deben establecer métodos de comunicación seguros y no dejar en manos de los usuarios la implementación de estos.

La solución que se está aplicando con éxito actualmente es la creación de aplicaciones móviles específicas, tanto para dispositivos Android como iOS, que garanticen la seguridad de las comunicaciones entre usuario y proveedor del servicio, además de permitir un nivel alto de personalización y adaptación a lo que necesitan los propios usuarios. No obstante, los usuarios nunca deben olvidar que no es conveniente el uso de redes públicas para acceder a contenidos privados y que siempre se debe tener un antivirus.

2 La banca electrónica

Al igual que ha pasado con la atención sanitaria, la pandemia ha provocado que multitud de actividades que antes realizábamos de forma presencial en una sucursal bancaria las tengamos que realizar de forma digital. Esto ha supuesto el *boom* de las aplicaciones de banca electrónica.

Sin embargo, esta explosión ha supuesto un reto para las propias entidades bancarias, que han tenido que adaptar su infraestructura para poder ofrecer la disponibilidad del 99,9 % requerida, y han tenido que crear equipos específicos para la mejora continua de este nuevo canal con sus clientes.

Con todo, el mayor freno actual para la adopción de este canal por parte de los usuarios es la seguridad. Aunque desde las propias entidades se afirma que este canal es más seguro que el presencial, la realidad es que muchos usuarios, normalmente aquellos con menor conocimiento del medio digital, son reticentes al uso de estos y siguen prefiriendo el uso del canal presencial.

¿Cuáles son los métodos más habituales de estafa bancaria actualmente? El líder sigue siendo de largo el robo de datos sensibles, aunque los ciberdelincuentes han ampliado los métodos para lograr la información de los usuarios: correo electrónico (*phishing*), SMS (*Smishing*) y llamada telefónica (*Vishing*).

Otra de las estafas que se han popularizado en el último año es el duplicado de tarjetas SIM. Cuando un ciberdelincuente consigue tus datos básicos (nombre, apellidos, DNI, número de teléfono), se dirige a una sucursal del teleoperador y solicita un duplicado de tu tarjeta. Durante el tiempo en que la víctima no se da cuenta (le deja de funcionar todo), el ciberdelincuente puede acceder a todas las aplicaciones y correo electrónico.

Capítulo 5

Los ciberseguros

El auge de los servicios digitales y el riesgo inherente a los mismos ha provocado la aparición de una nueva modalidad de seguros, que protegen a usuarios y empresas ante situaciones ocasionadas en el entorno digital: los ciberseguros.

¿Qué es un ciberseguro? Es un tipo de seguro que pueden contratar las empresas para proteger cualquier tipo de incidente que ocurra en el entorno digital, ya sea en la infraestructura o debido a alguna actividad.

En el caso de una empresa, las aseguradoras, después de valorar el riesgo (como hacen para el resto de los seguros que comercializan), exigen a las empresas adoptar una serie de medidas de seguridad para poder contratar el servicio: medidas de protección, establecimiento de procedimientos de seguridad, aseguramiento del cumplimiento legal y formación a los usuarios en materia de ciberseguridad. Si todas estas medidas fallan, el seguro actúa como una medida de último recurso.

¿Qué cubre un ciberseguro? Las coberturas se concentran en los ámbitos siguientes (se citan los más comunes):

- Responsabilidad civil o de terceros.
- Responsabilidad por pérdida de datos de carácter personal.
- Cobertura a los datos alojados en la nube.
- Cobertura a reclamaciones.
- Asistencia técnica.
- Gastos de restauración de datos y reparación equipos.
- Cobertura ante pérdida de beneficios.
- Cobertura jurídica.

El precio, como en cualquier tipo de seguro, siempre dependerá del tamaño de la empresa y de la valoración de riesgos que realice la aseguradora, existiendo pólizas para PYMES desde los 300 € anuales hasta importes de 1000 €, ofertadas por alguna aseguradora.

Es importante remarcar que las diferentes aseguradoras que ofertan este tipo de producto no trabajan en todos los sectores, sino que excluyen algunos más complejos como el sector salud, dado el carácter altamente sensible de la información gestionada.

Capítulo 6

Los retos de la ciberseguridad

1 Seguridad en la nube

Las empresas cada vez optan más por la nube. El hecho de que los proveedores de este tipo de tecnologías sean más confiables está empujando a las empresas a embarcarse en proyectos de migración a este nuevo entorno, que ofrece capacidades de escalabilidad y disponibilidad sin límite, además de transferir el riesgo a un proveedor externo. Sin embargo, donde antes la empresa controlaba la seguridad de su infraestructura, en la nube (sobre todo las nubes públicas) esta seguridad es implementada por el proveedor del servicio, con lo que hay que establecer de forma clara las medidas de seguridad que la empresa necesita. Esto es la seguridad en la nube.

La seguridad en la nube es un área de la ciberseguridad que garantiza que todos los sistemas y datos que residen en la nube estén seguros, implicando esfuerzos tanto por parte del proveedor de servicios en la nube como de la empresa. A modo de definición más formal, la siguiente Kaspersky lo detalla de forma concisa: "**La seguridad en la nube es toda la tecnología, los protocolos y las buenas prácticas que protegen los entornos informáticos en la nube, las aplicaciones que se ejecutan en la nube y los datos almacenados en ella**".

Esta seguridad está dividida en una serie de componentes:

- **Seguridad de los datos.** Gracias a herramientas que se ponen entre el acceso y la posibilidad de acceder a los datos, proveedor de servicios y cliente pueden proteger los datos ante accesos no autorizados. Las herramientas más utilizadas son las VPNs y el cifrado de datos.
- **IAM (gestión de las identidades y accesos).** Se debe tener un control total sobre las cuentas que tienen acceso a los diferentes servicios y los privilegios que tienen, con el fin de garantizar que solo pueden acceder a lo que realmente necesitan y que las acciones que pueden realizar están ajustadas a su posición. Las herramientas más utilizadas son la gestión de las contraseñas y métodos de autenticación como el doble factor.
- **Políticas para evitar, detectar y mitigar las posibles amenazas.** Implementar programas de formación, para preparar a los usuarios ante las posibles amenazas de la red, es una inversión clave, ya que el primer y menos controlable punto de acceso de los ciberdelincuentes a información sensible es el ser humano.
- **Establecimiento de políticas de retención de datos y creación de un plan de continuidad del negocio.** En las compañías tenemos que asegurar una redundancia óptima de los datos, además de establecer unas políticas de retención de los datos ajustadas a la ley (cada tipo de datos tiene un tiempo diferente de retención). Por otra parte, es preciso tener un plan que asegure la continuidad del negocio ante cualquier tipo de desastre, plan que debe ser probado y que debe mantenerse siempre actualizado (con el paso del tiempo, los sistemas y los procesos cambian).
- **Cumplir con los requerimientos legales.** Todas las empresas están obligadas a cumplir con una serie de requerimientos legales, siendo comunes a todas lo que tiene que ver con la protección de datos (aunque lo que sí varía es el nivel de protección de estos en base a su naturaleza). Políticas como el enmascaramiento de datos (con códigos hash) o su cifrado son muy útiles para cumplir con determinados requerimientos legales.

No obstante, la nube no está exenta de riesgos, donde los más importantes

son los siguientes:

- Riesgos inherentes a tener la infraestructura fuera de nuestras oficinas (no tenemos control, por ejemplo, de las medidas de seguridad que se utilizan para prevenir el acceso físico).
- El error humano (el proveedor de servicios puede realizar configuraciones erróneas y otorgar privilegios a usuarios incorrectos).
- Amenazas de tipo externo, comunes a infraestructuras on-premise.

Un punto sensible en cualquier implantación *cloud* son las comunicaciones. Se realizan multitud de transferencias de datos de usuarios a servidores, que en muchos casos contienen información sensible, y debemos proteger esas transmisiones. ¿Cómo lo hacemos? Utilizando una herramienta muy útil: el cifrado de datos. Este cifrado puede ser global, específico (solo ciertos datos) o punto a punto.

2 Confianza cero (Zero trust)

Esta tendencia, considerada por grandes corporaciones como Microsoft, Google o Cisco como ***"el futuro de la ciberseguridad empresarial***", se basa en algo muy sencillo: monitorización y autenticación continua de los usuarios que acceden a la red privada de la compañía.

Esta tecnología, que compite con otras soluciones como las VPNs, se basa en poner "vigilantes" en cualquier puerta y lugar de nuestra red, asegurando que si alguien entra de forma fraudulenta tengamos unas mayores probabilidades de detección (en la VPN el vigilante solo está en la puerta principal y, si alguien traspasa esa barrera de seguridad, puede moverse por dentro sin que lo controlen). Por tanto, al utilizar Zero Trust, el volumen de datos comprometidos por una intrusión se reduce drásticamente.

Otro beneficio de Zero Trust es la mejor experiencia del usuario. La saturación de conexiones VPN durante la pandemia ha provocado que las comunicaciones se resientan, por lo que muchas de ellas se han realizado sin una VPN activa. Al implementar este tipo de sistema de seguridad en la nube, evitamos estos problemas de saturación y no dependemos de que los usuarios se comuniquen siempre con la VPN activada.

Pero no todo son ventajas. Este aumento en los controles necesita de una mayor inversión en recursos y supone una mayor complejidad en la implantación, lo que se traduce en una necesidad mayor de recursos económicos, tanto para su implantación como para su mantenimiento (costes recurrentes).

Capítulo 7

Conclusiones

Es evidente que la ciberseguridad es un elemento que ha pasado de ser "colateral" en las compañías a ser un elemento crítico donde focalizar proyectos e inversiones. Si bien muchas empresas ya lo tenían claro desde hace unos años, en los que han estado invirtiendo mucho dinero en partidas relacionadas con la seguridad, la pandemia mundial y la digitalización acelerada provocada por esta ha forzado a todas las compañías a cambiar su estrategia, poniendo en el centro la seguridad.

Al analizar las cifras de eventos de seguridad reportados por organismos públicos de prestigio, se puede ver claramente que la aceleración de la digitalización ha comportado un aumento del cibercrimen. En base a los datos reportados por INCIBE en España y a la estimación propia realizada, desde 2013 los casos reportados se han incrementado en un 2 000 %, experimentándose en los dos últimos años un incremento del 50 % (acumulado). Todo esto está íntimamente relacionado con el avance de la digitalización.

Esta relación entre cibercrimen y madurez digital se advierte con claridad cuando analizamos los datos de América Latina. En una región con niveles más bajos de digitalización y una evolución por países muy dispar, la tendencia en cuanto a incidentes de seguridad es contraria a la de Europa,

lo que nos indica de forma clara que estos ciberdelincuentes buscan lugares con un nivel de digitalización más extenso para perpetrar sus acciones.

Otro punto importante para las empresas actualmente es garantizar la seguridad de sus sistemas para poder seguir operando, y aquí el teletrabajo ha sido una variable nueva que ha entrado en la ecuación. Cuando antes era una opción residual por la que algunas empresas optaban, se ha convertido en mayoritaria por necesidad. Pero ¿están las empresas preparadas para securizar todos los accesos a sus sistemas, independientemente desde donde se realicen? Actualmente existen muchos sistemas para lograrlo y las compañías, a la vista de la necesidad, están invirtiendo cada vez más en seguridad.

Teniendo en cuenta este incremento de las amenazas por el avance de la digitalización, surge una pregunta: ¿son los servicios digitales seguros? La respuesta es, en base al escenario actual, un rotundo sí. Si analizamos dos servicios que actualmente se utilizan y que gestionan datos de alto nivel de protección, la telemedicina y la banca electrónica, se han implementado muchas medidas de seguridad para garantizar que no acceden personas ajenas al servicio. Si bien es cierto que el riesgo cero no existe, la creación de aplicaciones móviles propias, que eviten el uso de las webs, y la implementación de medidas de seguridad como las autenticaciones biométricas, está logrando que los servicios sean cada vez más confiables y el nivel de adopción se vaya incrementando día a día.

Ante los problemas ocasionados por los ciberdelincuentes, las empresas de seguros han visto la oportunidad y algunas de ellas están trabajando en un nuevo producto enfocado en dar cobertura a las empresas ante los efectos de cualquier incidente de seguridad: los ciberseguros. Estos seguros tienen unos requerimientos previos a la contratación, pero dan la tranquilidad (sobre todo a pequeñas y medianas empresas) de tener a una compañía detrás que les puede asesorar, guiar y apoyar ante situaciones dañinas generadas por un ciberataque.

Por último, se identifican dos grandes retos para la ciberseguridad en los próximos años: la seguridad en la nube, dado que muchas empresas están migrando sistemas y servicios a este nuevo entorno, y el sistema de autenticación “Zero Trust”, que permitirá no depender de que los propios usuarios activen las diferentes medidas de seguridad. Ambos retos incrementarán los costes, pero el retorno de la inversión (ROI) será muy positivo.

A modo de conclusión, la ciberseguridad ha pasado en poco más de un año de ser un elemento coyuntural a estar en el centro de la estrategia empresarial, ya que es necesaria para asegurar operaciones. Por lo tanto, si las empresas quieren asegurar su supervivencia en los próximos años, es fundamental que inviertan en ciberseguridad de forma continua. Aquellos que no lo hagan, estarán en situación de riesgo.

Referencias bibliográficas

1 Bardají, E. (s. f.). Los ciberataques más comunes durante la pandemia del Covid-19 y ejemplos. ESEDSL. Recuperado el 11 de agosto de 2021. https://www.esedsl.com/blog/ciberataques-mas-comunes-durante-pandemia-covid-19-y-ejemplos

2 Castillo, N. (2020, 30 de junio). Los ciberseguros, otra manera de protegerse frente a los ciberriesgos. Interbel. https://www.interbel.es/ciberseguros-otra-manera-de-protegerse-frente-a-los-ciberriegsos/

3 CCN-CERT IA-13/20 Ciberamenazas y Tendencias. Edición 2020. (2020, 29 septiembre). CCN-CERT. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5377-ccn-cert-ia-13-20-ciberamenazas-y-tendencias-edicion-2020/

4 elmundo.es (2021, 1 marzo). Banca online: Blindaje contra los ciberdelincuentes. https://www.elmundo.es/economia/actualidad-economica/2021/03/01/60379566fc6c83f22d8b4615.html

5 Financiero (2020, 10 de marzo). América Latina fue blanco de 85 billones de intentos de ciberataques en 2019. https://financierolatam.com/tecnologia/america-latina-fue-blanco-de-85-billones-de-intentos-de-ciberataques-en-2019/

6 Fortinet (s. f.). América Latina sufrió más de 41 billones de intentos de ciberataques en 2020. Recuperado el 11 de agosto de 2021. https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2021/latin-america-suffered-more-than-41-billion-cyberattack-attempts-in-2020

7 Fortinet (s. f.). La nueva plataforma Fortinet Threat Intelligence Insider Latin America ofrece información local sobre ciberseguridad para varios países de la región. Recuperado el 11 de agosto de 2021. https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2019/new-fortinet-threat-intelligence-insider-latin-america-platform-offers-local-cybersecurity

8 Google (2019). Panorama actual de la Ciberseguridad en España. https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf

9 Grupo Adecco (2020, 9 de junio). The Adecco Group España. https://www.adeccogroup.es/

10 IADB (2020, 28 de julio). 2020 Cybersecurity Report: Risks, Progress, and the Way Forward in Latin America and the Caribbean. https://publications.iadb.org/en/2020-cybersecurity-report-risks-progress-and-the-way-forward-in-latin-america-and-the-caribbean

11 INCIBE (2020, 23 de julio). Ciberseguridad en el teletrabajo: una guía de aproximación para el empresario. https://www.incibe.es/protege-tu-empresa/guias/ciberseguridad-el-teletrabajo-guia-aproximacion-el-empresario

12 INCIBE (s. f.). INCIBE. Recuperado 11 de agosto de 2021. https://www.incibe.es/

13 Kaspersky (2021, 9 de agosto). ¿Qué es la ciberseguridad? latam.kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

14 Kaspersky (2021, marzo de 16). ¿Qué es la seguridad en la nube? https://www.kaspersky.es/resource-center/definitions/what-is-cloud-security

15 Mesa Editorial (2020, 20 de noviembre). Telemedicina y Ciberseguridad, un binomio perfecto. Saludiario. https://www.saludiario.com/telemedicina-y-ciberseguridad-un-binomio-perfecto/

16 Rodríguez, P. (2021, 5 de febrero). Qué es el sistema 'zero trust' y por qué Microsoft, Google y Cisco lo consideran el futuro de la ciberseguridad empresarial. Xataka. https://www.xataka.com/pro/que-sistema-zero-trust-que-microsoft-google-cisco-consideran-futuro-ciberseguridad-empresarial

17 Staff, F. (2020, 14 de julio). La ciberseguridad antes, durante y después de la pandemia. Forbes Centroamérica. https://forbescentroamerica.com/2020/07/14/la-ciberseguridad-antes-durante-y-despues-de-la-pandemia/

OBS Business School

School of **Business Administration & Leadership**

School of **Innovation, & Technology Management**

School of **Health Management**

De:

Planeta Formación y Universidades