Documento de trabajo 13/2020
14 de julio de 2020

Ciberlecciones aprendidas del COVID-19

Javier Alonso Lecuit

Ciberlecciones aprendidas del COVID-19

Javier Alonso Lecuit | Investigador senior asociado, Real Instituto Elcano.

Índice

Introducción[1]

El COVID-19, entre muchos otros efectos principales analizados por el Real Instituto Elcano, ha puesto a prueba la resiliencia de las infraestructuras críticas y los redes y sistemas de comunicación del ciberespacio. Sus efectos han sido distintos de los incidentes y ataques para los que se preparan los responsables de la ciberseguridad; de ahí la utilidad de su análisis. Para ello, y contando con los colaboradores de los sectores público y privado de nuestro Grupo de Trabajo sobre Ciberpolítica, hemos llevado a cabo la reflexión colectiva que se presenta en este documento.

A partir de una primera valoración general, hemos agrupado las reflexiones en los apartados que se reflejan en el índice para diferenciar los impactos sistémicos, los previsibles, los novedosos y los intangibles, así como experiencias vividas durante la gestión de la crisis y recomendaciones para crisis similares en el futuro.

Impacto sistémico

La primera preocupación era la de evaluar si el COVID-19 había causado o había estado a punto de causar el colapso del ciberespacio, si bien según la información disponible en fuentes abiertas ni internet ni las redes y sistemas de información habían dejado de funcionar, aunque hayan experimentado problemas puntuales. Los colaboradores comparten esa misma percepción sobre la resiliencia global del sistema de TIC, pero muchos de ellos consideran sistémico el impacto que afecta al funcionamiento total de sus departamentos o a la continuidad de negocio de las empresas para las que trabajan. En cierta forma, la pandemia ha puesto a prueba los planes de contingencia y la gestión de crisis no por su impacto sobre la ciberseguridad, sino por su efecto sobre factores como la interrupción de suministros o la imposibilidad de acceso, por lo que "la crisis ha mostrado la necesidad de contar con un modelo de seguridad que integre seguridad física, ciberseguridad, inteligencia y resiliencia, en el marco de la continuidad del negocio y del servicio"[2].

Las empresas han activado en tiempo récord los procesos de continuidad de negocio, entre ellos el teletrabajo, junto con mecanismos de comunicación internos dirigidos a los empleados y externos dirigidos a clientes, entre otros, si bien es necesario reconocer que la activación ha funcionado mejor en empresas que habían simulado procesos de transición que en aquellas otras que han tenido que improvisar sobre la marcha. Por el contrario, la implantación de procedimientos de continuidad de negocio o resiliencia en pymes está poco extendida, por lo que muchas de ellas han tenido que reinventarse sobre la marcha sin planes claros para actuar. De cara a afrontar futuras pandemias y dada la gran afectación para el tejido empresarial, sería necesario fomentar estrategias de continuidad de negocio basadas en buenas prácticas, como normas UNE e ISO o CEN, y en organismos y asociaciones de apoyo. Dado que las pymes forman la mayoría del tejido industrial y de las cadenas de suministro, los poderes públicos no solo

[1] El autor quiere expresar su agradecimiento a todos los miembros del Grupo de Trabajo sobre Ciberpolítica que han participado en la elaboración de esta reflexión colectiva.

[2] Conclusiones del seminario virtual sobre "El papel de la seguridad (security) en la continuidad de negocio", Fundación ESYS, 25/VI/2020, p. 12.

deberían preocuparse por la continuidad en la prestación de los servicios esenciales y sus operadores designados, sino también por fomentar la planificación de su resiliencia ante escenarios de tipo disruptivo y no solo de futuras pandemias.

También han seguido funcionando las infraestructuras industriales sin que la pandemia haya provocado problemas especiales en el personal de operaciones y mantenimiento. Allí donde el teletrabajo no ha sido posible, y en previsión de contagios, se ha duplicado o triplicado el número de centros críticos de operaciones o establecido turnos de 15 días en condiciones de confinamiento de circunstancias (por ejemplo, en caravanas) del limitado personal de planta que realiza funciones críticas para evitar contagios. En los casos en que la infraestructura no estaba preparada para realizar el trabajo OT en remoto, se ha tenido que adaptar la infraestructura de red interna. El confinamiento por orden gubernativa no ha afectado al personal de operación y al mantenimiento de los servicios esenciales, que ha podido recibir salvoconductos de las autoridades de ciberseguridad (CNPIC[3]); de ahí que estas funciones hayan podido prestarse casi con normalidad.

Siguiendo con la continuidad de negocio, los expertos consultados resaltan que únicamente las grandes corporaciones que cuentan con una consolidada presencia internacional disponen de planes de continuidad plenamente operativos, es decir, establecidos, conocidos por la organización, auditados, ejercitados y actualizados. Al contrario, la gran mayoría de las pymes y de instalaciones de la Administración, como algunos hospitales, carecen habitualmente de planes de continuidad probados. Confían en la ciberprotección del Esquema de Seguridad Nacional o de los servicios de ciberseguridad con los que cuentan, pero, al carecer de planes de continuidad, corren el riesgo de colapsar y de provocar el colapso de otros sistemas[4].

A pesar de lo anterior, los responsables de empresas de ámbito multinacional dudan de que se puedan controlar en esos planes los incidentes de naturaleza global y disruptiva tales como la actual pandemia o plantear situaciones poco previsibles como, por ejemplo, la restricción internacional de movimiento de mercancías o el cierre de fronteras, entre otros. No obstante, si la empresa dispone de un plan de mínimos y determinada madurez en su implantación, es viable recuperar un cierto nivel de productividad. El tamaño de la empresa es determinante al menos en el proceso de implantación; las auditorías, pruebas y actualizaciones, además de necesarias, generan gran confianza en la alta dirección.

[3] El CNPIC ha emitido 269.737 acreditaciones a personal de operadores críticos y servicios esenciales durante el estado de alarma sanitaria. Datos proporcionados por su director, Fernando Sánchez, en el 12.º Encuentro Digital de Seguridad Integral, Seguritecnia, 23/VI/2020.

[4] A pesar de la preocupación por que se utilizaran contra hospitales españoles virus usados en otros países, como el NetWalker, no se ha podido confirmar su empleo, por lo que resulta difícil inferir si la continuidad de su servicio obedece a su capacidad de resiliencia o al azar de no ser atacados. Rodrigo Alonso, “Los cibercriminales utilizan el coronavirus para atacar a hospitales, gobiernos y usuarios”, ABC, 3/IV/2020.

Han contribuido a asegurar la resiliencia del sistema de TIC:

- el despliegue y capilaridad de la red de comunicaciones de banda ancha de acceso fijo por fibra e inalámbrica 4G con la que cuenta España;
- la previsión y gestión de las infraestructuras críticas en sus 12 sectores (regulaciones PIC y NIS, planes, medidas y consultas);
- el Esquema Nacional de Seguridad y las buenas prácticas de seguridad y de continuidad adoptadas con una visión integral por la mayoría de las grandes empresas y corporaciones públicas y privadas;
- disponer de planes de contingencia, continuidad y respuesta a emergencias, en ámbitos del sector público y privado, y
- las capacidades de protección al teletrabajo movilizadas por los medios públicos (como Incibe, CCN o CNPIC para la Administración) o los privados.

En resumen, a pesar de la resiliencia demostrada por el sistema global de TIC en esta pandemia o la confianza que se muestra en su redundancia de las redes de comunicación, no se debe descartar absolutamente la posibilidad de que se produzca un fallo sistémico de alcance global en internet o en las redes y sistemas de información[5]. Y no tanto por el lado de la ciberseguridad como por el lado de la seguridad física de sus responsables si el brote pandémico hubiera tenido mayor incidencia en el segmento del personal que atiende la operación de los sistemas o determinados servicios esenciales.

Impactos sectoriales esperables

La desinformación es ya un clásico en todas las crisis y en la del COVID-19 no han tardado en aparecer noticias e informaciones asociadas a la pandemia con intención o resultado de daño para la salud pública (*infodemia*)[6] para las redes y sistemas de comunicaciones[7] o para los altos gestores de grandes compañías o servicios públicos[8]. La infodemia progresa propiciada por la inseguridad que generan la pandemia y la necesidad de conocer el estado de situación, lo que aumenta el recurso a las fuentes digitales de información. Al elevado nivel de uso de las redes sociales se une la escasa cultura sobre desinformación de sus usuarios, que presumen la veracidad de los contenidos digitales sin estar concienciados de los riesgos de las campañas de desinformación a través de bulos y el uso de bots por intereses políticos, económicos, desestabilizadores o de cualquier otro tipo. En este contexto de crisis global, la necesidad de información adquiere similar necesidad y relevancia a la que los ciudadanos pudieran tener de otros servicios básicos. Las autoridades y las grandes plataformas tratan de concienciar a los usuarios y filtrar los contenidos sin invadir los

[5] Fundación ESYS, 15/II/2018, La gestión de las cibercrisis globales ¿estamos preparados para un big one?

[6] Además de informaciones negacionistas de la pandemia o las conspirativas, otras atribuyen virtudes curativas a la leche¸ el vodka o la medicina tradicional y se las niegan a las vacunas y fármacos.

[7] ETNO, UNI Europa ICTS y GSMA han condenado más de 120 ataques contra los empleados y redes 5G porque se les atribuye la expansión del COVID (UK, NL, FR, DE, IR, BE, IT, SE, FI, CY).

[8] División de Comunicaciones Estratégicas y Análisis de la Información del SEAE, actualización del informe, 29/04/2020. Ryan Gallaher, "Hackers Target Top Officials at World Health Organization", Bloomberg, 21/IV/2020.

derechos y deberes fundamentales, pero en situaciones tales como la pandemia han tenido que emplear a fondo sus capacidades de vigilancia para evitar la propagación de informaciones falsas o contraproducentes para la salud. En España la vigilancia de las campañas durante el COVID-19 se ha centralizado en la Comisión de Desinformación y la respuesta ha correspondido a la Secretaría de Estado de Comunicación, dependiente de la Presidencia del Gobierno.

Las grandes plataformas también se han esforzado para verificar los contenidos de la información que trasladan, pero se han enfrentado a dos tipos de problemas. Por un lado, el incremento exponencial del tráfico (hasta más del 6.000% en abril[9]) y del *spam* (Google tuvo que filtrar y bloquear 18 millones de correos y otros 240 millones de *spam* diarios) y, por otro, la capacidad de los emisores para superar los filtros de detección[10]. El *spam* siempre ha sido uno de los principales problemas del servicio de correo electrónico al utilizarse como vía de ataque, por lo que los sistemas de filtrado han de estar sobredimensionados y tener cada vez mayor capacidad de inteligencia para poder descartar este tipo de tráfico malicioso, a ser posible en el punto más próximo a su origen. En consecuencia, será cada vez más necesario que los operadores de redes troncales IP (*carriers* internacionales), proveedores locales de servicios de acceso a internet (*Internet Service Providers*, ISP) y los proveedores mundiales de servicios de internet que gestionan los correos electrónicos (Gmail, Outlook, Hotmail. Yahoo y otros) potencien el uso de inteligencia artificial para multiplicar su capacidad de respuesta. Esta misma necesidad se ha comprobado en otros ámbitos de la ciberseguridad para los centros de operaciones de seguridad (*Security Operations Centre*s, SOC), que se mencionarán más adelante.

Los intercambios de información sobre los ciberdelitos percibidos por los responsables de seguridad coinciden en señalar las condiciones ideales que generan las pandemias para acometer estos delitos. El estado psicológico del usuario (ansiedad, miedo, desinformación, etc.), el aumento de las compras por internet como consecuencia del confinamiento y el entorno doméstico desde el que opera el usuario –mucho menos protegido que su puesto de trabajo corporativo habitual– aumentan significativamente la tasa de éxito del engaño. Los delincuentes aprovechan todas las técnicas de ingeniería social junto con la curiosidad y necesidad de información para cometer delitos masivos dirigidos a la población[11] y recurren a técnicas digitales para suplantar identidades, vender productos falsos o precarios o elaborar estafas o donaciones dinerarias bajo una supuesta solidaridad. También en este aspecto alguno de los expertos consultados ha resaltado la calidad de las técnicas de suplantación *ad hoc* dirigidas contra altos directivos de las organizaciones.

[9] IBM Security, "2020 Consumer Small Business Covid-19 Awareness Study", 7-8/V/2020.

[10] El vicepresidente de Google, Scott Spencer, denunció la capacidad de adaptación y el nivel de sofisticación de las tácticas para superar las medidas de control de su plataforma. Google Threats Analysis Group, "Findings on Covid-19 and online security threats", 1/V/2020

[11] Aprovechar el miedo, la curiosidad, la necesidad o la solicitud de ayudas para cometer delitos como los que revela Val Saengphaibut, "Latest Global COVID-19/Coronavirus Spearphising Campaign", Fortinet, 2/IV/2020.

La situación de incertidumbre ha propiciado un significativo aumento de ataques con programas dañinos (*malware*). Los portales de venta *online* minorista han experimentado un significativo incremento de ciberataques (principalmente *ransomware*) con numerosos afectados. Igualmente, se ha registrado un alarmante incremento de ciberdelitos de suplantación realizados mediante campañas muy elaboradas de *phishing* y *vishing* telefónico que buscan la vulnerabilidad del teletrabajador y el cliente final mediante técnicas de ingeniería social.

Según las opiniones consultadas, los delincuentes han alcanzado su máximo nivel de actuación en pocos días, después de realizar campañas de *phishing* dirigidas a usuarios finales y teletrabajadores, y han sido las pymes menos preparadas para el teletrabajo las más afectadas por los ataques. Las empresas han sido objeto de un notable incremento de fraude y de *malware* dirigido a la IT corporativa cuya vía de infiltración han sido las redes domésticas de los empleados. Las grandes empresas también han sido objeto de intensas campañas de suplantación de la marca corporativa dentro y fuera de España, lo que las ha obligado a una vigilancia continua de dominios y páginas web para asegurar la persecución y cierre de los casos detectados y prevenir su reaparición.

El sector privado manifiesta una notable preocupación por los grupos mafiosos que se infiltran en las redes corporativas (*Virtual Protection Networks*, VPN) y en la nube durante un prolongado tiempo para analizar la arquitectura, las aplicaciones y las transacciones antes de que puedan detectarse y activar *ransomware* para el robo de información o dinero en el momento más vulnerable (por ejemplo, el último viernes de mes, previo a los pagos de las nóminas) o el robo de información para hacerla pública antes que las juntas de accionistas. Por su parte, el sector público está preocupado por las amenazas persistentes avanzadas (*Advanced Persistent Threats*, APT) ligadas a Estados que dirigen sus ataques principalmente contra las infraestructuras críticas, a lo que habría que añadir, según los expertos, la importancia que cobra en situaciones de confinamiento general y prolongado de la población la resiliencia de los servicios esenciales prestados por las empresas de servicios públicos (*utilities*) de sectores tales como energía, banca, distribución de agua o alimentación.

La pandemia ha evidenciado la exposición a los ciberataques de las infraestructuras no declaradas como críticas debido a los servicios mínimos de personal para vigilancia o a los riesgos asumidos por el teletrabajo[12]. Otra conclusión compartida es que aquellas compañías que no tenían consolidados los medios técnicos, procedimientos y cultura del teletrabajo han tenido que anteponer la continuidad de negocio mediante el teletrabajo a su ciberseguridad, una exposición cuyas consecuencias para ellas o para las cadenas de suministro en las que funcionan pueden tardar tiempo en apreciarse, especialmente si no han hecho pública su situación. Y, aunque el alcance de los incidentes en estas circunstancias aún no se pueda evaluar, es previsible que en los próximos meses las corporaciones registren ciberincidentes a consecuencia de las intrusiones APT llevadas a cabo durante la pandemia debido a una mayor vulnerabilidad

[12] Los responsables han notado síntomas de agotamiento y síndrome de desconexión acumulado en el tiempo en las plantillas y tienen dudas de que la combinación de teletrabajo y trabajo presencial cuando la situación vuelva a la normalidad no reproduzca estos síntomas. También han tomado nota de la necesidad de tener prevista la rotación de personal crítico para evitar contagios.

por el aumento de la superficie de exposición vinculado al teletrabajo y la adopción de soluciones provisionales de IT.

La valoración general es que el aumento de los delitos informáticos ha sido proporcional al aumento del uso de las comunicaciones y al riesgo de trabajar fuera del perímetro de las redes internas de las empresas y organismos de la Administración, lo que obviamente ha aumentado la exposición.

Impactos novedosos

La pandemia sí que ha traído algunos elementos de riesgo peculiares para el ciberespacio. Se han registrados cambios significativos en los niveles de tráfico y en su distribución horaria. Empresas como Nokia han detectado crecimientos de tráfico de hasta el 40%, WhatsApp duplicó su tráfico en las horas laborables y la demanda de Netflix se duplicó en las primeras mañanas y creció las primeras horas de la tarde (27-42%)[13].

Para hacer frente a los cambios bruscos de tráfico, la Comisión Europea y el regulador europeo de comunicaciones electrónicas BEREC solicitaron la cooperación de los operadores de telecomunicaciones y de los proveedores de servicios digitales en un comunicado conjunto para evitar la congestión y compañías como Netflix y YouTube redujeron la calidad de su *streaming* a petición del comisario Breton, lo que ha permitido mantener una calidad adecuada en la prestación de otros servicios (Zoom, Hangouts o WhatsApp, entre otros).

Los expertos coinciden en que el desempeño de las *utilities* en general y de los operadores de telecomunicaciones en particular ha sido excepcional y clave para el mantenimiento de la tranquilidad y paz social durante el confinamiento. La calidad percibida por los usuarios de los servicios finales de Zoom, WhatsApp, la navegación web o las llamadas telefónicas, entre otros, es la suma de las aportaciones en las distintas capas inferiores de dicho servicio. Pero en ocasiones los usuarios achacan erróneamente una mala calidad del servicio final a los servicios de telecomunicaciones. Los operadores disponen de sistemas de gestión del tráfico que permiten mantener la calidad de los servicios dentro de los acuerdos de nivel de servicio (ANS) contratados mediante la gestión del ancho de banda, el encaminamiento, la priorización de protocolos u otros instrumentos similares.

A este respecto, y añadido a los sistemas de gestión de red, otro aspecto estructural de la resiliencia de las redes de telecomunicaciones de particular importancia en periodos de crisis radica en la arquitectura y diseño topológico de la red, donde adquieren cada vez más relevancia componentes tan diversos como son las aplicaciones de IA, la cadena de suministro, las nuevas tecnologías virtualizadas (*Software Defined Networks*, SDN) y funciones de virtualización de redes (*Networks Virtual Functions*, NVF) y, más

[13] Observatorio Nacional 5G, "Networks respond favorably to traffic growth due to Covid-19", 6/IV/2020.

recientemente, la hiperconvergencia de infraestructuras (HCI [14]). Resulta extremadamente importante que en el diseño de la red y en su evolución no se pierdan conceptos básicos para su resiliencia como son la seguridad por diseño, el mallado, el respaldo y la diversidad. La presión del mercado y una regulación errónea podrían desincentivar al operador y conducirnos en un futuro cercano al espejismo de redes resilientes cuando en realidad no lo son.

Por otra parte, los hogares han incrementado su demanda de servicios digitales para teletrabajo, teleenseñanza y ocio hasta niveles de tráfico y calidad de servicio equivalentes a una pequeña empresa. Los proveedores de contenidos y servicios de telecomunicaciones han respondido a un reto importante y no conocido anteriormente: el uso masivo y simultáneo de millones de conexiones y videollamadas, el incremento de WhatsApp y similares y la distribución masiva de contenidos. En este sentido, la consulta resalta que los hogares, en el futuro, deberán disponer de una red interna configurada y dimensionada para dar cabida simultánea a los diversos usos en el ámbito del ocio, la educación a distancia y teletrabajo con unos niveles mínimos de disponibilidad, calidad de servicio y seguridad y, en particular, contar con varias vías de acceso, ya que los hogares con un solo acceso son un potencial punto crítico para la conectividad.

En efecto, las fuentes abiertas revelan la disparidad de los efectos sobre los usuarios según sea la ubicación (rural o urbana), el tipo de redes utilizadas (cable, fibra, satélite…), la calidad del servicio de acceso a internet (estándar o elevada), la infraestructura doméstica de TIC (capacidad, configuración *router*/*fireware*, contraseñas, segmentación u otras medidas de seguridad, diversificación del acceso fijo/4G/wifi a internet, actualización de sistemas operativos y de aplicaciones en los dispositivos del usuario o franjas horarias de mayor uso), etc.

Los expertos consultados señalan que la conectividad de los teletrabajadores confinados en sus domicilios no ha presentado problemas en la mayor parte del territorio español gracias a la excepcional conectividad de banda ancha, mayoritariamente provista de accesos a red fija por fibra. En algunos casos, como altos directivos o puestos técnicos de alta criticidad, las empresas solo han tenido que configurar conexiones con medidas de seguridad especiales para las redes corporativas, aunque todas ellas han intensificado la monitorización del uso de la red corporativa para readaptar la capacidad de conexiones a esta (VPN) y/o aumentar el número de licencias concurrentes de Office 365 u otros servicios virtualizados en la nube.

Los operadores destacan que la pandemia ha cuestionado la disparidad que ofrecen a los ciudadanos las zonas rurales respecto a los grandes núcleos urbanos porque no

[14] La infraestructura hiperconvergente (*Hyper-Converged Infrastructures*, HCI) es el próximo paso en la evolución de las arquitecturas de centros de datos. Combina equipos *hardware* de uso común del centro de datos con *software* inteligente para crear bloques flexibles que reemplacen las infraestructuras tradicionales a base de servidores, redes de almacenamiento y matrices de almacenamiento separado. En un entorno HCI, los recursos convergen de forma física en servidores estándar que forman un potente entorno convergente definido por *software*. Simplifica las operaciones de TI permitiendo que el mismo servidor *hardware* gestione el almacenamiento y procesamiento, lo que elimina las ineficiencias y acelera el procesamiento.

cuentan con la conectividad adecuada a unas necesidades de digitalización que afectan a derechos esenciales como la seguridad, la salud o la educación, situación estrechamente vinculada en los próximos años al despliegue de tecnologías habilitadoras para la digitalización tales como el 5G. Lo mismo puede decirse respecto de los colectivos sociales más desfavorecidos, que se ven excluidos de los beneficios de la sociedad digital. Aunque la falta de ordenadores o la obsolescencia de los sistemas operativos no es responsabilidad de los operadores, sí que lo es prever su acceso a una internet con la adecuada calidad. Por consiguiente, es previsible que se reactive el debate sobre políticas para la universalización de la banda ancha y otras vinculadas a la disponibilidad de terminales.

La pandemia ha dado a conocer el potencial del teletrabajo para la sociedad digital y es previsible que la vuelta al puesto presencial en oficinas tarde meses e incluso que algunas compañías evalúen el teletrabajo como opción principal. Por encima de sus aspectos sociales y laborales, el teletrabajo desencadenó también una oleada de ciberataques como los llevados a cabo sobre los protocolos de Microsoft para acceder al control remoto de los ordenadores de trabajo (*Remote Desktop Protocol*, RDP)[15]. Las plataformas ofimáticas virtualizadas, como Outlook 365[16], han facilitado el trabajo durante la pandemia para mantener la continuidad de las funciones corporativas. El acceso remoto a la red corporativa (VPN) ha permitido seguir utilizando los programas y herramientas corporativos (aplicaciones para la administración de los recursos humanos, financieros-contables, productivos, logísticos, etc., de la empresa) y la utilización de algunos se ha visto notablemente incrementada (videollamadas, chat…). Algunas corporaciones han tenido que hacer frente a retos singulares; por ejemplo, las retransmisiones de las juntas de accionistas a empleados e inversores mediante *streaming.* Sin embargo, salvo excepciones, no ha sido posible controlar a distancia el trabajo de empleados que operan en entornos de alta seguridad desempeñando funciones críticas, ya que no suele preverse para ellos el control remoto.

Aquellas compañías en las que el teletrabajo estaba ya implantado o en fase avanzada de implantación no han experimentado grandes dificultades en esta rápida transición al teletrabajo generalizado. Los expertos han descrito cómo esas compañías han preparado y probado la infraestructura de comunicaciones e IT, elaborado los procedimientos internos y actualizado la configuración y la seguridad de los dispositivos en movilidad (terminales móviles y ordenadores adecuadamente plataformados) implantando el acceso seguro mediante doble factor de autenticación o una política de uso de firma electrónica biométrica a través del terminal móvil y firma cualificada. En algunas corporaciones, la red corporativa VPN no estaba dimensionada para acoger a la mayor parte de la plantilla en teletrabajo de un día para otro, por lo que ha sido necesario redimensionar la capacidad de la red corporativa e instalar más pasarelas. El gran aumento de videollamadas ha obligado en ocasiones a redimensionar el ancho de banda de la red corporativa. La entrega a los empleados de terminales seguros ha

[15] Dmitry Galov, "Remote spring: the rise of bruteforce attacks", Kaspersky, 29/VI/2020.

[16] La sobrecarga de actividad durante la pandemia ha obligado a Microsoft en ocasiones a reubicar los servicios que presta a sus clientes, con su consentimiento, a centros de datos redundantes en otros países, como Italia, Noruega, Finlandia y Méjico, para mantener la calidad y disponibilidad del servicio.

planteado ocasionales dificultades logísticas. Algunos prestadores de servicio han tenido que utilizar medios particulares como solución de contingencia inmediata.

En conclusión, y en esto coinciden los participantes en la reflexión conjunta, no todas las empresas grandes y mucho menos las pequeñas han estado preparadas para tener a toda su plantilla en teletrabajo en tan breve plazo de tiempo, una coincidencia que podría aplicarse también al sector público, aunque en ambos casos la convicción carece de los necesarios elementos de prueba. Las Administraciones Públicas presentan un balance similar al sector privado, ya que muestran disparidad en sus niveles de preparación para el teletrabajo y accesos no presenciales telemáticos que permitan mantener la continuidad de los servicios prestados a los ciudadanos. La digitalización de la Administración española goza de una posición de privilegio entre las de la UE (el segundo lugar en el Índice DESI relativo a 2019), pero habrá que esperar a la edición de 2020 para conocer el impacto de la pandemia en la Administración digital[17]. La Administración ha funcionado mejor en los sectores digitalizados de TIC que en los demás, donde carece de interfaces web con los usuarios a pesar de que la plantilla siga trabajando. Las Administraciones locales y de menor tamaño han tenido mayores dificultades para ofrecer atención al ciudadano y, en algunos casos, a las empresas de ciberseguridad en trámites normales como licencias o la congelación de las contrataciones.

La pandemia ha permitido a los CISO conocer mejor los riesgos y necesidades de seguridad del teletrabajo. El comportamiento de los atacantes se ha adaptado al nuevo terreno y a las nuevas circunstancias de sus víctimas. Ha cambiado la superficie de ataque incluyendo el domicilio de los usuarios que teletrabajan y las nuevas plataformas de colaboración utilizadas; cambian igualmente los vectores de ataque y el *modus operandi* de los delincuentes. La experiencia debe permitir adoptar las medidas procedimentales, técnicas y organizativas que equiparen la seguridad del entorno de teletrabajo con la que lleva aparejado el puesto de trabajo corporativo, de manera que represente un coste similar para el atacante (principal barrera de entrada). En este sentido, las empresas han elaborado planes específicos para la segurización y disponibilidad del puesto de teletrabajo, estableciendo un estado de vigilancia especial en formato emergencia, intensificando el control y la defensa del terminal (*endpoint*), incluyendo controles adicionales –en particular sobre la navegación web del usuario y el empleo exclusivo de aplicaciones corporativas, por ejemplo la adopción de Teams– o bloqueando el uso de programas no autorizados (algunas han limitado el creciente uso de la aplicación de videollamadas Zoom debido a las vulnerabilidades reportadas[18]).

En una segunda fase, se han reforzado los controles en la red corporativa y la seguridad de la nube. Las medidas de seguridad del *endpoint* se han adaptado a la criticidad del puesto de trabajo: alta (equipo bastionado, HDD cifrado, conexión a VPN cifrada, acceso a red dedicado), media (equipo bastionado) o baja (equipo doméstico, protección de la red del hogar), y en ocasiones se ha instalado un segundo *router* para no verse expuestos a la gestión remota del operador de acceso. Las Administraciones Públicas y algunas corporaciones han utilizado herramientas del CCN-CERT como MicroClaudia

[17] Comisión Europea, Índice de la Economía y la Sociedad Digitales (DESI 2020), España.

[18] Véase, por ejemplo, el aviso AV 22/20 Vulnerabilidad en Zoom, publicado por el CCN-CERT, 5/IV/2020.

y Claudia[19] para llevar a cabo acciones de detección y respuesta (vacuna informática) ante *malware* complejo de tipo *ransomware*[20], así como Carmen, especializada en la detección de movimiento lateral en la red administrada, propio de ataques persistentes avanzados (APT).

La reflexión ha aflorado el esfuerzo acelerado de empresas y Administraciones para hacer frente a las necesidades sobrevenidas de formación, lo que agrava la escasez de personal cualificado. Un indicador del esfuerzo de formación debido a la pandemia se encuentra en el incremento del número de cursos impartidos por el CCN durante el confinamiento, que se ha disparado con el COVID-19[21].

Las tecnologías y aplicaciones (*apps*) para la pandemia han generado un amplio debate sobre su viabilidad, eficacia y ética[22]. La reflexión colectiva no se ha centrado en su utilidad en la lucha contra la pandemia, sino en la cuestión de la privacidad porque preocupa su impacto sobre el derecho fundamental a la privacidad al tratarse de tecnologías y *apps* que procesan datos sensibles (salud y geolocalización) o de proximidad a otras personas y contacto con ellas (la defensa de la privacidad ha retrocedido frente el miedo a la pandemia). Igualmente, la pandemia ha avivado el debate sobre el uso de los datos sanitarios, combinando las necesidades de gestión sanitaria con la debida protección de derechos y datos sensibles, usados únicamente con la finalidad clara, transparente y debidamente informada a los ciudadanos de combatir y prevenir los contagios.

Impactos tangibles

Otro objeto de la investigación era detectar impactos poco apreciables desde fuera del sector de la ciberseguridad, pero que representaran algún cambio cualitativo sobre los patrones de comportamiento previos a la pandemia. Algunas empresas han establecido actuaciones a corto plazo centradas en reforzar la disponibilidad y seguridad del teletrabajo mediante la entrega de portátiles plataformados, el uso de Office 365 y el

[19] MicroClaudia es un centro de vacunación de sistemas informáticos del CCN-CERT que, mediante el despliegue de "vacunas", permite prevenir la infección de equipos informáticos. Esta solución está orientada a completar y ampliar las funciones de los antivirus para evitar que el código más dañino, como el *ransomware*, se ejecute en sus entornos. La solución Claudia permite tener una visión más completa de lo que ocurre en los ordenadores de una organización, ya que su objetivo principal es la detección del código dañino complejo y de las APT. Datos del curso sobre "Experiencia del CCN-CERT durante el Covid-19", 2/IV/2020.

[20] Entre el 27 de abril y el 1 de junio, la herramienta MicroClaudia del CCN-CERT había desplegado 34 vacunas a partir de nuevas muestras de *ransomware* (Snake Fresenius, Hydra, Robinhood, Xorsit, MorrsbatchCrypto, Cryptolocker, etc.) en 10.589 equipos de 141 organismos públicos, generado 1.120 alertas y detenido alrededor de 100 ataques. Curso sobre "Experiencia del CCN-CERT durante el Covid-19", 2/IV/2020.

[21] En relación con la iniciativa #CiberCOVID19, el CCN-CERT ha mantenido hasta el 28 de mayo 25 de un total de 36 webinarios programados sobre ciberseguridad con 10.760 inscritos y una asistencia de 6.356 personas hasta finales de mayo. El CCN-CERT ha impartido 193 horas de formación a más de 10.900 alumnos en el mes de abril. Datos del curso sobre "Experiencia del CCN-CERT durante el Covid-19", mencionado anteriormente.

[22] Andrés Ortega, "La búsqueda de inmunidad digital frente a la pandemia: eficacia, privacidad y vigilancia", Real Instituto Elcano, mayo de 2020.

acceso a las aplicaciones corporativas por el personal previamente autorizado a través de la VPN.

El creciente uso de servicios en la nube (*cloud*) ha suscitado una polémica artificial que ha querido ver en esta pandemia la excusa ideal para atacar el uso de los sistemas *in house* y las VPN haciéndolos parecer obsoletos para forzar una emigración generalizada de las corporaciones hacia la nube. En este sentido, algunos expertos en ciberseguridad afirman que la nube no es lo segura que afirman los grandes proveedores y que es necesario estructurar un debate en profundidad sobre la ciberseguridad aplicable a cada tipo de nube según el tipo de empresa, necesidad, criticidad y regulación sectorial, ya que no es válido un diagnóstico general. Por otro lado, el cifrado en la nube que preserve la confidencialidad del dato es un tema aún no resuelto. En el futuro, tendrán que convivir las plataformas en la nube con soluciones flexibles para grupos de teletrabajo corporativos basadas en la virtualización de redes y las redes definidas por *software*.

En el marco del aseguramiento de las soluciones en la nube, es esencial la protección de los servicios y de la información corporativa alojada mediante redundancia con centros de datos distantes para garantizar la continuidad de servicio en su configuración y bastionado, así como la monitorización y vigilancia de ataques (incluyendo los de denegación de servicio). Los administradores de los servicios en la nube han de garantizar un uso particularmente seguro en modo remoto de los usuarios privilegiados. La pandemia también ha reafirmado los temas sobre la gestión segura de la identidad *online*, haciéndose necesario el uso de una cadena de identidad global y robusta aplicada a las redes corporativas que se interconectan y a los dispositivos, sistemas, aplicaciones y el propio usuario, todo ello integrado en un sistema de gestión de identidades (*Master Data Management*, MDM). Estos sistemas proporcionan listas de los datos compartidos y utilizados por las diversas aplicaciones que permiten, además, combinar mecanismos adicionales de identificación para el acceso a la red, la identificación y autenticación multimodal robusta y la gestión del mínimo privilegio, todo ello bajo un sistema dinámico de control y análisis de riesgo y de cifrado de la información combinado con sistemas de monitorización y detección temprana de amenazas y una gestión proactiva de vulnerabilidades y configuraciones.

En relación con las nuevas necesidades de comunicación de las plantillas y el teletrabajo, surge una magnífica oportunidad de negocio para los operadores de comunicaciones electrónicas y dirigida al mercado de empresas consistente en desarrollar servicios basados en redes NFV y SDN sobre grupos cerrados de usuarios seguros establecidos mediante conexiones o circuitos virtuales (por ejemplo, *Multiprotocol Label Switching*, MPLS[23]) que conecten las casas de los empleados, las empresas o los participantes en una reunión.

Los servicios de ciberseguridad son más necesarios que nunca para hacer frente a ciberataques que se apalancan en el miedo, los problemas económicos y la rápida

[23] El MPLS es una técnica o protocolo para la transferencia de datos con el que podemos enviar en una red de un área geográfica extensa datos de diferente tipo —incluyendo servicios de voz y transmitidos por IP, como los servicios de videoconferencia e internet— gestionando la calidad del servicio.

adopción de nuevos modelos de negocio derivados de una crisis profunda. Durante la pandemia, debido al incremento de los ciberataques, los centros operativos de seguridad (SOC) se han visto desbordados y, por lo tanto, los expertos prevén que los SOC pos-COVID requieran de mayor orquestación y automatización auxiliada por IA. Es igualmente necesario que las empresas inviertan en tecnología y herramientas preventivas, como la mencionada Claudia del CCN-CERT. El uso de herramientas para la clasificación, tipificación y notificación en cadena y escalada de los incidentes es otro efecto intangible de la pandemia. Por otra parte, es importante indicar la necesidad de establecer procedimientos y capacidades de acceso remoto en tiempo normal y su habilitación, autorización y uso desde terminales y ubicaciones que no cumplan determinados estándares de seguridad. Los SOC han de poder trabajar en modo de teletrabajo o distribuido para garantizar sus servicios. Deben aunar la seguridad de todos y cada uno de los componentes y del propio personal crítico, que ha de establecer turnos y retenes para garantizar servicios mínimos ante enfermedades y bajas.

El impacto de la pandemia sobre las cadenas de suministro y los procesos de digitalización era otro de los objetos de consulta. Las opiniones apuntan a que la resiliencia de las primeras debe ser una de las prioridades de la ciberseguridad pos-COVID-19[24]. Las empresas han tenido dificultades para que algunos de sus contratistas pudieran teletrabajar e interactuar con las debidas medidas de seguridad, por lo que han recurrido a exigir certificaciones. Algunos proveedores han establecido planes de gestión de crisis, pero no todos disponen de ellos ni han realizado ejercicios de simulación. Expertos del sector de la ciberseguridad señalan que, en general, las cadenas de suministro no disponen de medios ni preparación en ciberseguridad o en gestión de crisis, a pesar de contar con buenas infraestructuras y sistemas de comunicación. Afortunadamente, no se han registrado incidencias graves en el sector de las TIC por incumplimientos de acuerdos de nivel de servicio (ANS). Es probable que la pandemia no haya puesto a prueba las cadenas de suministro, pero sigue preocupando la existencia de bastantes empresas sin una estrategia clara de transformación digital para prestar servicios y operar procesos, una preocupación que se debería subsanar regulando la obligación de certificación para formar parte de las cadenas.

Esta consulta ha incluido cuestiones sobre los ciberincidentes y la resiliencia registrada en situaciones de pandemia en servicios esenciales (públicos y privados), como los de comunicaciones (electrónicas, de servicios de emergencia, telefonía móvil y fija y acceso a internet) o las infraestructuras de TIC y SSII de los sistemas sanitario y energético Se trataba de valorar si esos servicios e infraestructuras han registrado algún efecto peculiar; por ejemplo, conocer si las personas confinadas en sus domicilios habían seguido recibiendo servicios de comunicaciones y otras *utilities* como la electricidad, el gas y el agua.

[24] ISMS Forum presentó el 18 de mayo de 2020 la "Guía para la gestión de crisis por ciberincidente en la cadena de suministro". El documento ofrece recomendaciones y buenas prácticas sobre cómo deben abordar las empresas una estrategia de protección y respuesta a incidentes de ciberseguridad con origen en el proveedor que puedan llegar a suponer una amenaza grave para la propia empresa, así como las convenientes medidas de monitorización, contención y vuelta a la normalidad de la entidad.

Las respuestas valoran positivamente la resiliencia de las redes de comunicaciones españolas, ya que se han dimensionado con márgenes de seguridad en capacidad y redundancia más que suficientes para permitir el tráfico del teletrabajo y los sistemas que gestionan la red han podido redistribuir las cargas. Y, cuando se han producido aumentos de tráfico como el mencionado 75% de WhatsApp (debido al vídeo, fundamentalmente), los retardos o caídas obedecen más a los servidores que a la saturación de la red.

Una valoración similar reciben la ciberseguridad y resiliencia de las infraestructuras críticas, así como la colaboración público-privada a través de los canales formales establecidos con el CNPIC[25]. Sus compañías han consolidado su cultura de seguridad integral (física y cíber) y no ha sido necesario acometer cambios estructurales. Éstas mantienen un elevado nivel de exigencia, preparación y control para minimizar los impactos de ciberincidentes, por lo que tampoco se han visto obligadas a implantar cambios cualitativos significativos salvo adaptaciones puntuales a la magnitud de la situación. No obstante, consideran que deben progresar en su preparación ante la eventualidad de ciberataques a la red OT, acelerar la integración de la seguridad y las comunicaciones IT-OT, contar con sistemas y operaciones bastionados[26] y con una operación centralizada junto con un modelo de explotación segregada dependiente de la unidad de negocio.

Las compañías consultadas con infraestructuras críticas que ofrecen servicios esenciales manifiestan no haber detectado campañas de ciberataques graves fuera de lo habitual en la red corporativa de IT ni en la operación de OT. Han continuado aplicando sus planes de operación y autoprotección, diseñados para prevenir los ataques más graves de las APT, lo que les ha permitido afrontar el COVID-19 con solvencia. Su prioridad ha sido garantizar la continuidad de negocio mediante la seguridad industrial OT y, en menor medida, la confidencialidad, ya que algunas corporaciones no tienen clientes finales.

La consulta no ha podido valorar debidamente el impacto de la pandemia sobre la continuidad de negocio del tejido industrial, las pymes, *start-ups* o los programas de I+D+i, entre otros, por lo que las conclusiones al respecto son especulativas. Se estima, sin evidencias conocidas, que aquellas empresas que habían adoptado la gestión de información y sistemas basada en la nube han tenido más sencilla la adopción del

[25] El CNPIC informa de haber atendido un total de 6.763 consultas (2.262 vía telefónica, 4.501 vía correo electrónico). La plataforma CNPIC-PI3 (578 usuarios) sirve de apoyo para el intercambio de información entre todos los agentes implicados en la protección de las infraestructuras críticas, incluidos los cuerpos policiales. Además de la anterior, la aplicación AlertPIC facilita la comunicación de las emergencias entre el CNPIC y los operadores críticos y de servicios esenciales, estando habilitados tanto los responsables de seguridad y enlace como los responsables de seguridad de la información. Datos extraídos del 12.º Encuentro Digital de Seguridad Integral, Seguritecnia, 23/VI/2020.

[26] El bastionado de los sistemas de información permite preparar los sistemas informáticos, servidores y aplicaciones para resistir ataques conocidos y aquellos que aprovechan vulnerabilidades de día cero. Durante el proceso de definición de una línea básica de seguridad (hardening), se analiza el software utilizado en el sistema, tanto interno de la empresa como externo, y el perfil de los usuarios para que las protecciones se adecúen al uso del sistema. Estas medidas de seguridad incluyen, por ejemplo, las acciones permitidas en los paquetes ofimáticos del usuario final o el rol que desempeñan los distintos servidores en la red corporativa (directorio activo, servidor web, servidor de bases de datos…).

teletrabajo y la puesta en marcha de los planes de contingencia requeridos para afrontar la situación de confinamiento forzoso. Sin embargo, a pesar de su dificultad, sería importante conocer el impacto sobre esas empresas, que forman la mayor parte del tejido industrial y empresarial del país. Un conocimiento, pues, imprescindible para determinar, incluso regulatoriamente, las especificaciones que exigir a los actores ya identificados en la trasposición de la Directiva NIS (Decreto Ley 12/2018), incorporar sus conclusiones al reglamento que desarrolle esta ley, aún pendiente de publicarse, o la próxima revisión de la Directiva NIS a finales de 2020.

En relación con la soberanía tecnológica y de los datos –dos líneas rojas establecidas por la CE–, se observa una progresiva concentración y desaparición de los intermediarios tecnológicos y proveedores locales de *cloud*. La integración vertical en servicios virtualizados –aplicaciones corporativas (SaaS), alojamiento, ciberseguridad– ofrecidos por los tres principales proveedores multinacionales de *cloud* aumenta su posición de dominio en el mercado de empresas al ritmo de la digitalización. En consecuencia, se reduce el espacio de supervivencia de las empresas nacionales de IT, proveedores locales de *cloud*, empresas de ciberseguridad o integradores, entre otras. Esta tendencia puede acarrear graves consecuencias en el empleo y supervivencia del tejido empresarial, además del impacto negativo de la concentración del riesgo y la dependencia para la ciberseguridad en multinacionales no europeas.

En las consultas también ha aparecido un último impacto intangible relativo a la importancia que adquieren los datos y las tecnologías para explotarlos en la prevención y gestión de crisis, en este caso sanitaria. Los medios de comunicación se han hecho eco de la desestructuración de los datos sanitarios y de su limitada utilidad para mejorar la resiliencia. Esta misma carencia se da en sectores cíber, donde los departamentos de sistemas de información funcionan en silos que se resisten a perder autonomía de gestión. Dado el buen resultado que algunas empresas consultadas están experimentando en la operación y mantenimiento de las infraestructuras y los procesos industriales gracias a los datos, los responsables de seguridad plantean la posibilidad de aplicar las mismas técnicas a la gestión de la seguridad. Se han recibido varias sugerencias como usar plataformas y criterios de gestión de la información (categorización de datos) homogéneos e interoperables entre los agentes de cada sector, ampliar la centralización de datos anonimizados a un modelo de conocimiento e inteligencia y compartir datos abiertos (*open data sharing*) mediante tecnología IA (algo semejable a la armonización de datos a nivel sectorial, regional o estatal que propone la UE en su estrategia de datos).

Gestión de la crisis.

Cada responsable y sector consultado ha gestionado la crisis de una manera distinta, aunque todos han tenido ocasión de poner a prueba sus procedimientos. Los comités de crisis tienen por objeto asegurar la integridad y continuidad de negocio de las operaciones (el funcionamiento de la planta de producción y centros críticos de operación, los turnos de personal, la ciberseguridad OT, el mantenimiento, etc.) y de las funciones corporativas (teletrabajo de los empleados, sistemas de información y redes corporativas, ciberseguridad IT y otras). La pandemia ha obligado al seguimiento diario de la crisis para adaptar las respuestas a la situación cambiante.

Desde el inicio de la pandemia se han activado con rapidez los procedimientos de gestión de crisis preparados y probados y se han puesto a prueba las capacidades de las organizaciones en términos de resiliencia; los gestores coinciden en señalar que la alta dirección de las empresas ha tenido ocasión de apreciar el valor que añaden esos procedimientos a la continuidad de negocio. Los colaboradores de esta consulta concuerdan en el apoyo de la alta dirección a los responsables de la gestión y su implicación en los procedimientos establecidos, lo que justifica el esfuerzo económico invertido en las medidas de prevención que habían solicitado.

La colaboración público-privada no tiene problemas, pero sí límites (está centrada en los ciberincidentes). Los expertos privados se han visto apoyados por algunos análisis y recomendaciones de la Administración en relación con la ciberseguridad[27], aunque echan en falta una mejor coordinación, por ejemplo, entre la Agencia Española de Protección de Datos y los ministerios de Interior y Sanidad en relación con las medidas de prevención laboral, como las recomendaciones de uso de las cámaras termográficas para la medición de fiebre en los controles de acceso.

La asociación Continuam España ha promovido la creación, entre asociaciones, fundaciones, colectivos y profesionales, del Foro Resilium España, desde donde ha emitido boletines a organizaciones para la mejor gestión de la continuidad, decálogos de resiliencia organizativa y social, la creación de un espacio de compartición de noticias, ayudas, buenas prácticas e infografías que las diferentes asociaciones generaban para sus asociados y eventos virtuales y ha invitado a sumarse a otras asociaciones y profesionales de Latinoamérica. A raíz de ello, se ha elaborado un "Manifiesto conjunto sobre Resiliencia Organizativa y Social Sostenible"[28]. Hay que señalar entre los mecanismos *ad hoc* para la gestión de crisis el mencionado foro, iniciativa de la sociedad civil y el asociacionismo junto con iniciativas llevadas a cabo desde otros ámbitos (UNE, ISACA, Alastria) encaminadas a la divulgación o puesta en marcha de iniciativas cíber a través de una exhaustiva recopilación de enlaces sobre guías, artículos, noticias, conferencias, seminarios, webinarios y aplicaciones.

Algunos sectores, como el financiero, han activado medidas especiales[29], pero los procedimientos de gestión de crisis implantados en las empresas y sectores consultados se han mostrado resilientes y, tras evaluar su funcionamiento durante la pandemia, es de esperar que apliquen las lecciones aprendidas para mejorar los procedimientos vigentes[30]. En este contexto se ha constatado la preocupación por los riesgos para la

[27] Incibe, "Cómo detectar y prevenirse ante los fraudes y bulos que circulan en relación al COVID-19", 27/III/2020; CCN-CERT, "Repunte de las campañas de phishing relacionadas con la pandemia COVID-19", 19/III/2020; "CERT-EU Cyber Security Guidance to Survive the COVID-19 Crisis", 24/III/2020; "EC-Echo white paper. The COVID-19 Hackers Mind-set", 8 de abril de 2020.

[28] La asociación Continuam promueve la resiliencia basada en cuatro pilares junto con el análisis y mejora de lecciones aprendidas y diseño de escenarios *what if*: prevención y gestión de riesgos 360º, seguridad integral de todas las disciplinas, gestión de crisis y emergencias (respuesta) y gestión de la continuidad operativa (plan de planes).

[29] El Banco Central Europeo alertó al sistema financiero sobre los riesgos para la ciberseguridad y las medidas de contingencia que adoptar frente al COVID-19.

[30] Los planes de contingencia deben prever situaciones como la vivida, con una disminución fuera de lo normal de la actividad, y evaluar el impacto de los distintos escenarios de duración temporal posible sobre sus servicios, su personal, sus cadenas de suministro y otras interdependencias críticas.

seguridad de la información de las organizaciones que implican las reuniones virtuales, realizadas a través de plataformas en la nube en las que se intercambia información corporativa sensible y se adoptan decisiones relevantes de toda índole. Las dudas sobre la seguridad de Zoom alertaron al sector de la necesidad de ampliar el perímetro de protección, especialmente las empresas que deben prevenir las actuaciones de los servicios de inteligencia extranjeros.

Por su parte, la Administración no ha adoptado mecanismos de gestión espaciales para la pandemia[31] y la gestión se ha conducido bajo los procedimientos normales. El Departamento de Seguridad Nacional ha recabado la información del Sistema de Ciberseguridad Nacional y la ha trasladado diariamente al presidente del Gobierno. El CNPIC también ha elaborado informes diarios para el Ministerio del Interior. Entre los organismos que han intervenido en los niveles operacional y técnico cabe mencionar al Centro Criptológico Nacional del CNI (CCN, Ministerio de Defensa), centro de alerta y respuesta nacional del sector público con responsabilidad en ciberataques sobre sistemas clasificados, sistemas del sector público[32] y empresas y organizaciones de sectores estratégicos para el país, en coordinación con el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC, Ministerio de Interior), cuya misión es la protección de infraestructuras críticas y servicios esenciales[33], así como el Instituto Nacional de Ciberseguridad de España (Incibe, Ministerio de Asuntos Económicos y Transformación Digital) para la salvaguarda de la ciberseguridad de empresas, profesionales y ciudadanos. Asimismo, el CCN y la Secretaría General de Administración Digital han activado el Grupo de trabajo de Seguridad Ampliado, compuesto por 125 representantes de departamentos de seguridad de Comunidades y Ciudades Autónomas, servicios de salud de CC. AA. y el Ministerio de Sanidad, con el objetivo de reforzar la seguridad del sector sanitario.

No podían dejar de abordarse las relaciones público-privadas durante la gestión de la crisis. Al no tratarse de una gestión de ciberincidentes, no ha sido necesario seguir el procedimiento reglado para ellos, pero las opiniones muestran que todavía es necesario reducir distancias entre lo público y lo privado para potenciar y sistematizar la

[31] El Departamento de Defensa de los EE. UU. creó una COVID-19 Telework Readiness Task Force para prevenir las vulnerabilidades creadas por el trabajo a distancia

[32] Las líneas de actuación realizadas y previstas del CCN en la crisis del COVID-19 incluyen acciones de concienciación, formación y colaboración (creación del *hashtag* #CiberCOVID19 para informar de campañas de *ransomware*, 36 actividades de formación *online* con la participación de 6.356 asistentes, más de 10.900 alumnos en formaciones realizadas en abril, 35 infografías…), acciones de vigilancia (180 dominios con 2.100 subdominios de hospitales, agencias, empresas relacionadas con la salud y empresas públicas, 16 informes ejecutivos y 45 informes técnicos a servicios y departamentos de salud, 23 organismos analizados, análisis de la superficie de exposición de servicios de salud y universidades…), acciones de detección y respuesta (14 informes de análisis de código dañino, 18 alertas sobre riesgos y vulnerabilidades, tres listas negras con indicadores de compromiso, más de 100 ataques parados y 1.000 alertas de *ransomware* con la herramienta MicroClaudia…) y acciones de monitorización de vulnerabilidades. Datos del curso sobre "Experiencia del CCN-CERT durante el Covid-19", 2/IV/2020.

[33] El CNPIC ha emitido durante el estado de alarma 171 notas, 264 informes y 791 comunicaciones en relación con el sistema PIC junto con 152 incidentes de seguridad durante el mes de abril de 2020. Asimismo, ha gestionado 339 sucesos de desinformación, entre los cuales destacan, segmentados por temática, 80 referidos al estado de alarma (23,6%), 42 sobre instituciones del Estado (12,39%), 36 sobre material sanitario (10,6%) y 34 sobre teorías alternativas y conspiratorias (10%). Datos del 12.º Encuentro Digital de Seguridad Integral, Seguritecnia, 23/VI/2020.

colaboración y compartir inteligencia entre los sistemas de gestión de crisis públicos y privados. Los intercambios informales en el sector privado han funcionado con normalidad, pero las corporaciones echan en falta mecanismos de relación preestablecidos que permitan una gestión ágil ante crisis no ocasionadas por un ciberincidente. Las consultas reconocen que la Administración ha tenido que dar prioridad a los planes del Esquema Nacional de Ciberseguridad frente a las necesidades del sector privado. A pesar de que la colaboración público-privada en coordinación e inteligencia sigue progresando, algunas empresas han visto a la Administración desbordada y echan de menos la colaboración "informal" de la Administración antes de la pandemia, si bien la mayoría de la inteligencia que reciben las (grandes) empresas consultadas procede habitualmente de servicios privados. La gestión de crisis con el COVID-19 ha vuelto a suscitar la preocupación latente en el sector privado por su papel y preparación para una gestión público-privada de situaciones de gravedad, ya sea la reglada de grandes incidentes o situaciones como la vivida con la pandemia.

El último punto consultado a propósito de la gestión de crisis era si, debido al incremento, adaptación y sofisticación de los ciberataques, seguían siendo de utilidad los modelos de análisis de riesgos actuales (SOC, analistas) o si era necesario aplicar nuevas metodologías, como CCE (*Consequence-driven Cyber-informed Engineering*) [34] o inteligencia artificial. Los expertos en gestión han resaltado la necesidad de que la gestión se adapte a los impactos reales y no tanto en su probabilidad basada en series estadísticas de ocurrencias (resaltan la dificultad de contar con modelos que analicen, por ejemplo, el impacto de la geopolitización actual). Por ello, siguen sosteniendo la validez del analista de inteligencia, aunque apoyándolo con las tecnologías necesarias para desarrollar su función y, se hace hincapié en esto, asegurando su familiarización y formación para emplearlas.

Conclusiones y recomendaciones

Terminamos este ejercicio de reflexión con las principales conclusiones y recomendaciones que nos han trasladado los expertos en ciberseguridad consultados en función de su experiencia particular. Son provisionales, porque dependen de una verificación más objetiva que la recabada en las consultas y mayor perspectiva temporal, pero pueden servir como orientaciones de tendencias provisionales.

Resiliencia

El COVID-19 no ha causado un impacto sistémico en el ciberespacio y la resiliencia de éste ha contribuido significativamente a mantener la de los servicios esenciales. La pandemia ha impulsado en tiempo récord la digitalización de los ciudadanos, empresas y Administraciones y la puesta en valor de los servicios de telecomunicaciones y aplicaciones de internet, apuntando igualmente carencias tales como la formación en materia digital, la conectividad de zonas rurales o la disponibilidad de terminales en estratos sociales más desfavorecidos, con impacto directo en la enseñanza (es decir, los efectos del dividendo digital).

[34] Idaho National Lab (INL), "Consequence-driven Cyber-informed Engineering", 18/X/2016.

La pandemia ha subrayado la importancia de preservar la resiliencia de las infraestructuras básicas y los servicios esenciales relacionados en situaciones de confinamiento generalizado y prolongado de la población. A los anteriores se unen ahora los relacionados con la salud y la educación, por lo que habría que asegurar que ambas participan del adecuado nivel de resiliencia.

La resiliencia añade valor a las empresas y Administraciones y se ha abierto un debate sobre la continuidad de negocio como una función específica de la alta dirección y su relación con la seguridad integral o la gestión de crisis. Las corporaciones, infraestructuras industriales e infraestructuras críticas han activado los procesos de continuidad de negocio, entre ellos el teletrabajo. Su implantación ha sido rápida y efectiva en aquellas empresas que ya estaban preparadas, pero las que no lo estaban han puesto en riesgo la continuidad de su negocio o la de las cadenas de suministro a las que pertenecen.

- Se recomienda a los gestores públicos y privados de ciberseguridad valorar las lecciones aprendidas en todos los niveles de responsabilidad para hacer frente en el futuro a situaciones similares a la pandemia o de mayor virulencia con efectos colaterales en materia de ciberseguridad y valorar la necesidad de elaborar estrategias que aseguren su resiliencia o la continuidad de negocio.
- Se recomienda sopesar si la regulación existente, además de abordar la fase de protección, debería incluir también la formación y los simulacros de gestión de situaciones de crisis para mejorar la resiliencia de las empresas.
- Se recomienda que se valore la resiliencia de los servicios que se prestan desde la nube y que madure el debate sobre su seguridad y su contribución a la resiliencia.

Infraestructuras

Las infraestructuras de TIC críticas han soportado el elevado y rápido incremento en las cargas de tráfico y los cambios en patrones de uso de las redes de acceso e internet desconocidos hasta la fecha sin comprometer la disponibilidad y la calidad del servicio gracias a la arquitectura y diseño de las redes, sus sistemas de gestión y las medidas puntales adoptadas para responder a la pandemia. Esta valoración no puede generalizarse para las infraestructuras no declaradas como críticas, que no tenían la obligación de contar con capacidades de resiliencia elevadas o planes de contingencia, por lo que han sufrido una mayor exposición a los ciberataques cuyos efectos están aún por conocer.

La resiliencia de unas y otras no puede darse por garantizada para el futuro porque depende cada vez más de tecnologías habilitadoras emergentes tales como la inteligencia artificial, las tecnologías virtualizadas de red e información y arquitecturas de datos hiperconvergentes, por lo que resulta básico potenciar determinados principios de diseño conservadores, en particular la seguridad desde el diseño, el mallado de redes, la redundancia y la diversidad de sistemas, para evitar el deterioro efectivo de la resiliencia. Por otro lado, la disponibilidad y gestión de los datos sanitarios y la disrupción de las cadenas de suministro han reabierto el debate sobre la relocalización de datos e

industrias, su explotación a efectos empresariales e industriales y el grado de autonomía necesario para preservar los intereses críticos nacionales.

- Se recomienda preservar la resiliencia de las infraestructuras básicas y los servicios esenciales, incluyendo ahora los relacionados con la salud y la educación, en situaciones de confinamiento generalizado y prolongado de la población.
- Se recomienda progresar en la resiliencia de las infraestructuras industriales de las redes OT, acelerar la integración de la seguridad y las comunicaciones IT-OT, contar con sistemas y operaciones bastionadas y con una operación centralizada compatible con un modelo de explotación segregada dependiente de la unidad de negocio.
- Se recomienda incorporar los aspectos industriales y de oportunidades de negocio de las nuevas redes, sistemas y protocolos de teletrabajo a la valoración actual de los aspectos tecnológicos y de seguridad de las infraestructuras de comunicaciones electrónicas (5G) y TIC.

El teletrabajo

El teletrabajo ha aumentado el perímetro de exposición a los ciberataques tanto en el sector público como en el privado. El esfuerzo adicional de organismos como el CCN, CNPIC, Incibe o AEPD ha limitado el impacto en la Administración Digital y el sector privado; los planes de transición de algunas grandes compañías han hecho lo propio en el sector privado. Quedan por valorar los efectos sobre los sectores públicos y privados menos preparados, que se han visto forzados a realizar la transición de forma precipitada, anteponiendo la continuidad de negocio a la seguridad.

- Se recomienda reglar las condiciones de acceso remoto a entornos críticos desde ubicaciones y equipos externos a las instituciones públicas y las empresas privadas.
- Se recomienda reglar los procesos de transición hacia el teletrabajo en los sectores no críticos para asegurar el funcionamiento de los servicios esenciales públicos y privados a los que apoyan.

Gestión de crisis

Las experiencias analizadas muestran que la existencia de procedimientos y sistemas de gestión de crisis ha sido útil para gestionar la pandemia, aunque no estuvieran pensados para ella. Tampoco se han utilizado los procedimientos de gestión de crisis diseñados para ciberincidentes de mayor gravedad, sino procedimientos pensados para la resiliencia y la continuidad de negocio de las empresas y Administraciones.

Los procedimientos de gestión de incidentes se han mostrado resilientes para afrontar el incremento de ciberataques, ciberdelitos y desinformación, especialmente los diseñados para hacer frente a las APT en infraestructuras críticas y servicios esenciales (Esquema Nacional de Seguridad y grandes empresas). Las experiencias confirman la persistencia de algunos lugares comunes, como el limitado intercambio de inteligencia entre los sectores público y privado, su desbordamiento en situaciones de gravedad y

la prevalencia de los canales informales. En sentido contrario, se han identificado intercambios de buenas prácticas en ambos sectores, así como múltiples iniciativas, webinarios y guías *ad hoc* para solucionar problemas prácticos.

- Se recomienda adoptar medidas para proteger la seguridad de la información corporativa compartida en la nube.
- Se recomienda realizar simulaciones de grandes incidentes para reducir la desconfianza hacia la gestión de crisis en situaciones extremas.
- Se recomienda implantar sistemas de inteligencia artificial para apoyar a los analistas y centros de gestión de crisis en esas situaciones.
- Se recomienda potenciar la estrategia europea de datos (EC Data Strategy) mediante estructuras de datos armonizadas y plataformas interoperables que faciliten el análisis e intercambio de información en situaciones de crisis con las adecuadas garantías jurídicas.

Regulación

A lo largo de la reflexión colectiva se ha mencionado la conveniencia de regular algunos aspectos, siempre tras la debida valoración de las lecciones aprendidas y cuidando de no provocar distorsiones en las condiciones competitivas del mercado. Entre otros, figuran los siguientes:

- Ampliar la exigencia de controles y certificaciones de ciberseguridad en la seguridad de la nube, la cadena de suministro, la resiliencia de la red y la seguridad industrial, en particular de los elementos IIoT.
- Exigir a la cadena de suministro (*vendors*) certificaciones de ciberseguridad que homologuen los equipos en concordancia con la criticidad de la función que desempeñen.
- Revisar y, en determinados casos, acotar dentro del marco de la Ley de Protección de Infraestructuras Críticas (LPIC) el número de controles que certificar por cada infraestructura crítica (actualmente, unos 780 controles por instalación).
- Acelerar la actualización y aprobación de la LPIC y el Reglamento NIS[35] junto con los esquemas de certificación de infraestructuras.

[35] Desarrollo reglamentario del Real Decreto Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información que traspone la Directiva UE 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (Directiva NIS).