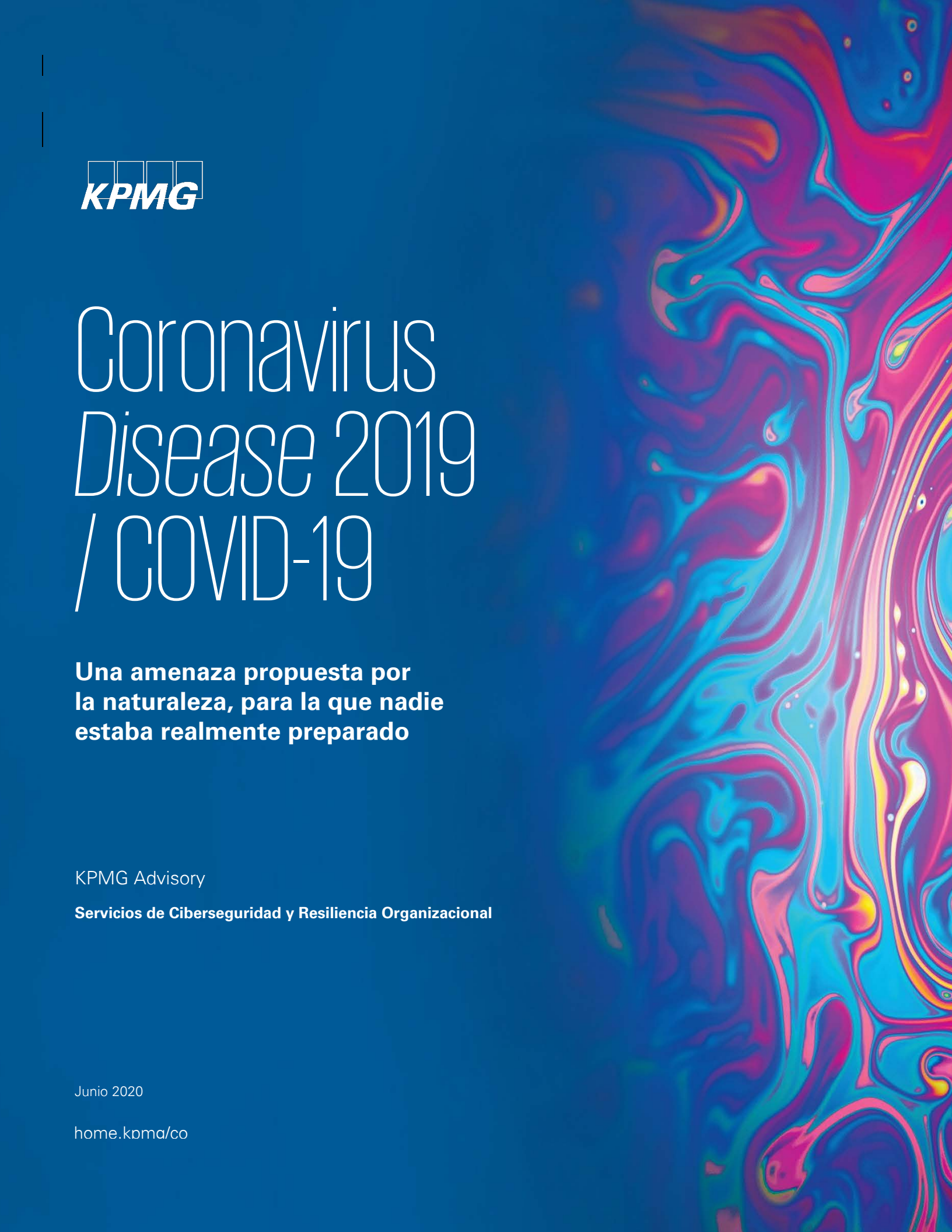
Coronavirus *Disease* 2019 / COVID-19

Una amenaza propuesta por la naturaleza, para la que nadie estaba realmente preparado



KPMG Advisory

Servicios de Ciberseguridad y Resiliencia Organizacional

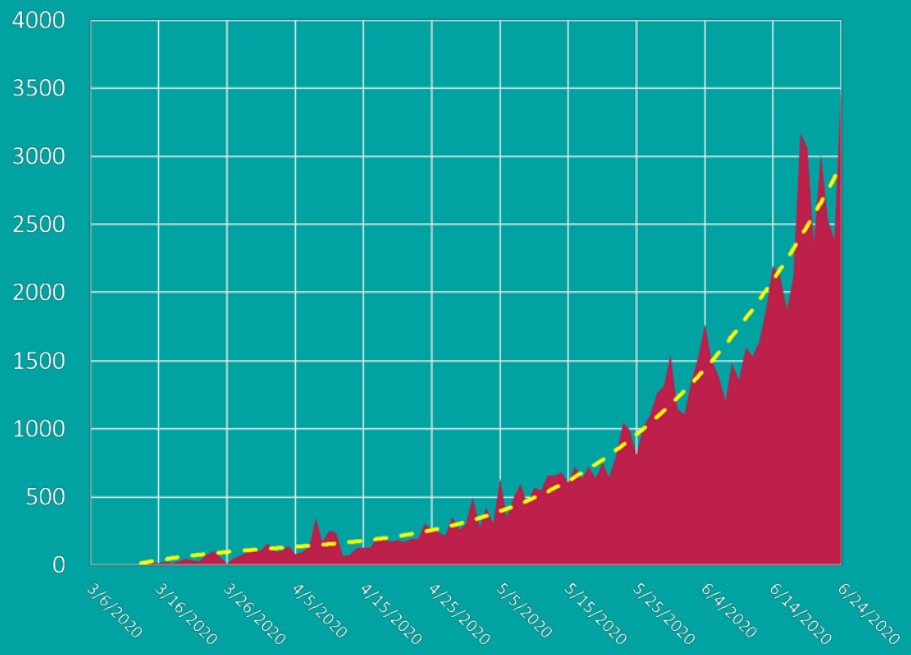
Junio 2020

home.kpmg/co

Introducción

El país se ha visto obligado a operar a su más mínima capacidad por un periodo de tiempo que se ha caracterizado por una creciente sensación de incertidumbre inimaginable. Durante la evolución temprana de la pandemia hubo sectores de la industria que tuvieron que mantener su operación, e inclusive consolidar y fortalecer su estructura para afrontar el evento y/o mantener a flote el suministro de servicios básicos necesarios para la comunidad en general. Las empresas que soportan los servicios públicos, las telecomunicaciones, el transporte terrestre, los servicios de salud, algunas entidades del gobierno, la agricultura, las grandes organizaciones del sector *oil & gas*, los cuerpos de seguridad, y el sector financiero tuvieron que responder y/o adaptarse a un evento que se podría catalogar como un "desastre de alcance nacional y mundial". Muchas de estas organizaciones de índole público y privado han tenido que improvisar planes de respuesta sin una planificación previa, con recursos y personal insuficiente y/o sin las competencias necesarias, así como sin una estrategia que les sirviera de guía y se coordinara con otros esfuerzos nacionales de índole institucional de mayor alcance. Tras los primeros 100 días de confinamiento, Colombia aún no ve la cúspide de la gráfica de comportamiento que esquematiza la evolución del proceso de contagio en el país (*Gráfica 1*).

¿Qué nos hizo falta?, ¿estábamos realmente preparados?, ¿cuáles han sido los factores de éxito en otras latitudes?, ¿qué deberíamos tener presente para esta nueva forma de operar?

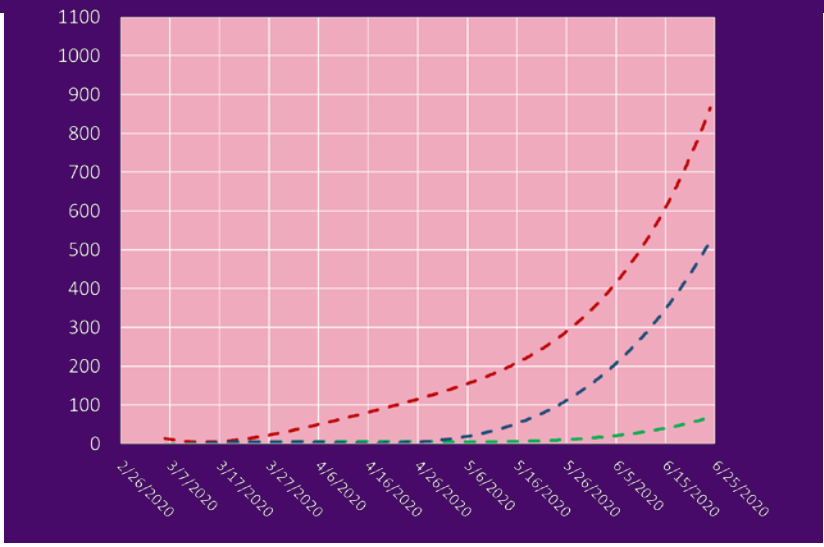


Grafica 1. Evolución del proceso de contagio en Colombia.

Respuesta y contención

Las fases de preparación, contención y mitigación en Colombia se han caracterizado por un reajuste en el destino de los recursos financieros del Gobierno Nacional con el fin de atender a la población vulnerable (*giros directos a los ciudadanos, subsidios en la tarifa de servicios públicos*), fortalecer el equipamiento del sistema nacional de salud (*adecuación y alistamiento de nuevas unidades de cuidado intensivo*), y disminuir la carga que pesa sobre las organizaciones y sus empleados (*garantías de crédito para las empresas privadas, subsidio para el pago de nóminas*). Estas medidas han requerido una actuación más audaz por parte de los entes de control para realizar un seguimiento sobre los procesos de contratación de última hora y su ejecución tras la alerta de malos manejos.

Los primeros dos meses tras el primer contagio, se han caracterizado por el desconcierto y la falta de coordinación entre diferentes entes de Gobierno, algo que inclusive fue reiterativo en la realidad de varios países, muchos de ellos altamente desarrollados. En Colombia, el 19 de marzo de 2020 se llevaron a cabo reuniones para la coordinación de esfuerzos con miras a enfrentar la pandemia. Por fortuna, Latinoamérica contó con la ventaja de las lecciones aprendidas en otras latitudes, pero aun así es posible notar el desconcierto por el comportamiento creciente de contagios que se ha venido dando a lo largo y ancho del país. No es difícil notar la diferencia en los resultados que arrojan las medidas de contención implementadas en las diferentes regiones (*Gráfica 2*); Medellín con una evolución creciente y casi marginal se destaca dentro de las ciudades que han sabido dar una respuesta más efectiva a la pandemia, Barranquilla con un proceso que inició más tardíamente pero que en el corto plazo ha aumentado su taza de contagios, y Bogotá, la primera ciudad



Gráfica 2. Comportamiento del contagio en: - - - Medellín, - - - Barranquilla, y - - - Bogotá

afectada y con un comportamiento creciente que aún no encuentra tope.

En contraposición, algunas medidas, o factores que han determinado el nivel de éxito para la contención de la pandemia que han implementado los Gobiernos de Corea del Sur, Singapur, Nueva Zelanda y Uruguay, incluyen:

- Suspensión de vuelos locales e internacionales.
- Cierre anticipado de fronteras.
- Suspensión de clases, servicios religiosos, y eventos públicos.
- Liderazgo coordinado de gobiernos transparentes.
- Tamizajes masivos y rápidos.
- Confinamiento de la población, incluso sin tener infectados.
- Implementación de mecanismos para la supervisión permanente de infectados.
- Aumento en el número de personas a cargo de rastrear infectados.
- Robustecimiento del sistema sanitario.
- Disponibilidad de planes de respuesta y contención previamente definidos.
- Disponibilidad de un inventario de soporte para el suministro de equipos y recursos requeridos por el sistema de salud.
- Disponibilidad de kits para la ejecución de pruebas.
- Implementación de una red masiva de laboratorios para el análisis de muestras.
- Implementación niveles alerta para las fases de preparación, contención, mitigación, y bloqueo.
- Avivar la transparencia en las comunicaciones que son dirigidas a la población.

"Eso es lo que nos muestra una epidemia: cuán vulnerables somos todos, cuánto dependemos del comportamiento considerado de otros, pero también cómo podemos protegernos y apoyarnos unos a otros actuando mancomunadamente".

Angela Merkel
Canciller de Alemania

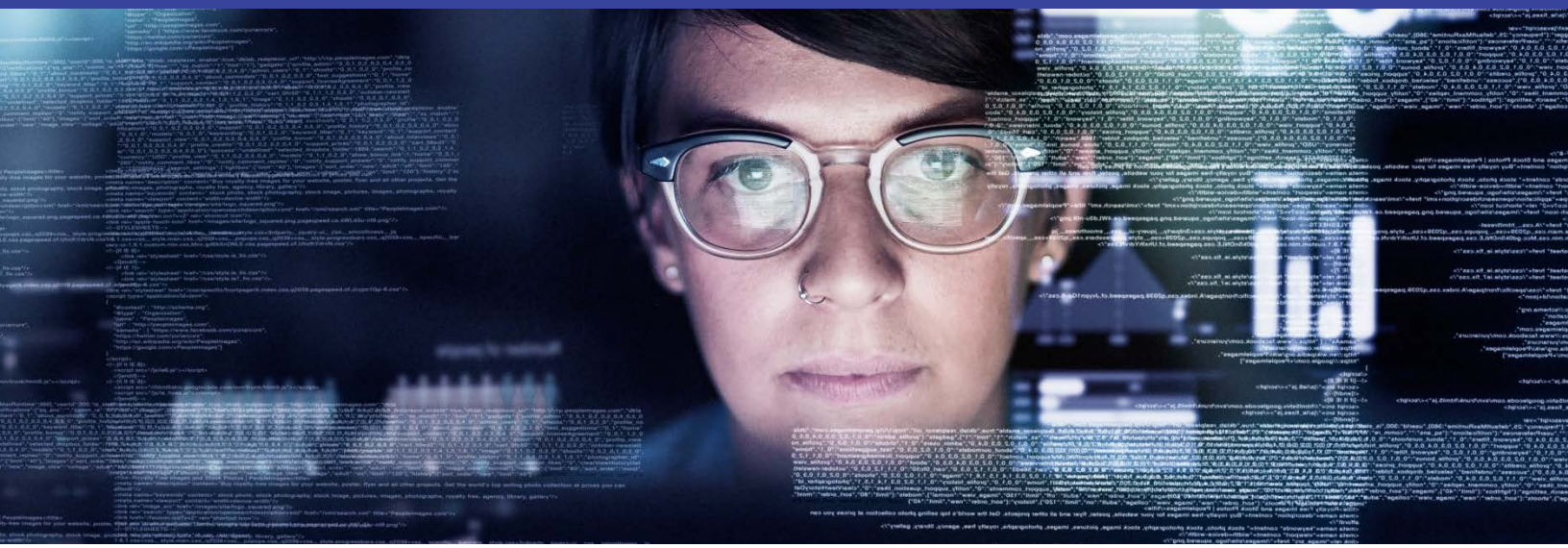
El "Evento 201"

En el mes de octubre del año 2019, el trabajo mancomunado entre el Centro Johns Hopkins, el Foro Económico Mundial y la Fundación Bill & Melinda Gates, permitió que se realizara en la ciudad de Nueva York el "Evento 201"; con el fin de desarrollar un simulacro para verificar el efecto de una pandemia global y determinar el grado de preparación que se tenía para brindar una respuesta apropiada por parte de los gobiernos y las organizaciones afectadas. La documentación existente evidencia de la ejecución y los resultados del simulacro ofrece una perspectiva de la que se deduce fácilmente que las actividades similares desarrolladas hasta la fecha fueron insuficientes por lo que, pese a que este ejercicio arrojó importantes conclusiones, muchas de las recomendaciones no tuvieron el tiempo suficiente para prosperar en la materialización de controles y/o planes de respuesta adecuados.

El 'Evento 201' destacó que los gobiernos y las empresas deben mantener fondos de capital suficiente para afrontar eventos de muy alto impacto y con ello mitigar sus efectos. A pesar de que, por separado cada país cuenta con recursos reservados para ciertos eventos catastróficos, la pandemia actual demuestra el poco o nulo nivel de preparación real con este tipo de eventos.

Otra gran conclusión a la que se llegó durante el evento y que hoy tiene en vilo al mundo establece que: "*los Gobiernos deberían haber proporcionado más recursos y apoyo para el desarrollo y la fabricación de vacunas, terapias y diagnósticos que serían necesarios durante la materialización de una pandemia*". También se exaltó la necesidad de aumentar el grado de cooperación de los países que a hoy cuentan con una gran capacidad de producción en torno al desarrollo de insumos médicos que podrían llegar a ser requeridos para su distribución a nivel mundial. Paradójicamente a esta recomendación dada en el 'Evento 201', en la respuesta a la pandemia actual se evidenció el desequilibrio existente y las medidas implementadas para acaparar los suministros médicos disponibles, hecho identificado como probable en los resultados obtenidos a través del simulacro reciente.

Nuevo entorno, nuevas amenazas



Para muchas organizaciones la situación actual se ha convertido en un momento de precariedad que se percibe como el resultado palpable de la poca orientación y empuje que han tenido los entes reguladores al intentar instaurar buenas prácticas en los sectores que les corresponde y que hoy en día ya son una regla general para el desarrollo de actividades de negocio en los países desarrollados.

Un estudio de la empresa Comparitech publicado en el año 2018, analizó a 60 países en materia de ciberseguridad, contemplando siete criterios de análisis, en el que Dinamarca aparece como el país mejor preparado y Colombia es ubicado por debajo del nivel medio aceptable en el puesto 39.

El COVID-19 se ha convertido en la cuna propicia para el aumento significativo en los ataques cibernéticos, con un incremento de al menos el 40% en el nivel de exposición a ciberataques, lo que potencialmente significará comprometer información sensible de índole personal y/o de las organizaciones.

Esta situación entonces debe ser percibida como un cambio en el panorama de riesgos ya que la puesta en marcha de nuevos esquemas de operación, como: el teletrabajo, cambios de horario, turnos, jornadas flexibles, vacaciones anticipadas y permisos no remunerados, aumentarán el interés de los ciberdelincuentes para establecer nuevos mecanismos que les permitan sacar provecho de la situación de manera ilegal.

No se puede desconocer, sin embargo, el esfuerzo que han venido desarrollando progresivamente sectores de la industria como el financiero, que al encontrarse mejor preparado ha sabido sortear los cambios impuestos por la coyuntura actual; adaptándose con mayor velocidad, al contar con una cultura instaurada asociada a la gestión del riesgo sobre su operación.

Será entonces foco de atención para las entidades de regulación dar mayor celeridad a las iniciativas que se tenían en curso y trabajar en la definición y promulgación de nuevos preceptos como las circulares expedidas por la Superintendencia Nacional de Salud en el año 2018 en las que se fomenta la definición, implementación, prueba y mantenimiento de un proceso para administrar y asegurar la continuidad del negocio, incluyendo elementos como: prevención, atención de emergencias, administración de situaciones de crisis, y definición de planes de contingencia en las instituciones del sector, medida que sería bienvenida en este preciso instante.

La información como factor determinante

Como si fuese una respuesta intuitiva, los Gobiernos, las empresas, los medios de comunicación, la publicidad y la comunidad en general están fomentando el uso informal de términos como: resiliencia, recuperación, reconfiguración, crisis, reinvención e innovación para referirse indistintamente al momento coyuntural por el que la sociedad está pasando, o para puntualizar una idea esperanzadora relacionada con la incertidumbre y la desorientación reinante. Un desafío que muy pocas organizaciones han logrado dirimir, es el de la homologación de términos para referirse a conceptos que son claves en la Continuidad del Negocio y, que en la práctica aunque de forma casi imperceptible, se convierten en la base que soporta el grado de éxito de las actividades de respuesta y recuperación, porque determinan el método de comunicación y entendimiento que es necesario definir y trabajar para unificar y coordinar el esfuerzo de múltiples grupos e integrantes de respuesta; estos términos ayudan a tener una percepción uniforme de una situación por demás desconcertante y su impacto relacionado.

En paralelo al avance del coronavirus, la sociedad se ha visto acorralada con el fenómeno de la "infodemia"; manifestación heredada del proceso de evolución acelerado que estamos viviendo hoy en día. La infodemia a la que se refiere la OMS, ha consistido en la masificación de información a través de: anuncios, noticias, mensajes e inclusive, publicidad que en muchos casos es falsa o malintencionada, sobre los hechos que han acontecido o caracterizado al evento de la pandemia y que finalmente han aumentado el grado de pánico, incertidumbre y angustia en las personas, organizaciones y gobiernos en general.

Sin desconocer la virtud que se requiere a la hora de seleccionar la información, lo más común hoy en día es el consumo desproporcionado de información sin contexto y sin el uso del pensamiento racional que nos caracteriza. Esto se empeora con las denominadas "Fake News". Siendo estas noticias falsas y peligrosas, un grave problema que desvirtúa la intención del mensaje original, una práctica que se aprovecha de la situación para sacar algún tipo de beneficio y al final aumentar el grado de confusión y desconcierto. Los motivos a la hora de desinformar son muchos e influyen: factores políticos, intereses personales (autopromoción)

e inclusive los nuevos modelos de negocio con campañas de publicidad enfocadas a ganar la atención de nuevos potenciales clientes. Quienes lo hacen juegan con las emociones, los miedos, los prejuicios y la ignorancia afirmando que brindan un aporte de significado y confianza en una realidad que es especialmente compleja, desafiante y altamente cambiante.

Todas las empresas que en este momento afrontan la pandemia bajo la declaración de una situación de crisis organizacional, han confiado ciegamente en las fuentes de información que tenían a la mano y que frecuentemente no son confrontadas para evidenciar su veracidad y oportunidad en el fulgor de las medidas apresuradas que se vieron obligadas a implementar. En este panorama cobran mayor relevancia las actividades de: recolección, centralización, análisis y decantación de la información para la toma efectiva de decisiones a través de un Centro de Comando y Control instaurado para el debido Manejo de Situaciones de Crisis y Emergencias, que a través de protocolos y procedimientos previamente documentados se permita estar en contacto constante antes, durante y después de un evento con líderes representantes de entidades de gobierno, proveedores financieros, entes de control, reguladores, aseguradoras y organismos de respuesta que a la final podrían hacer la diferencia a la hora de generar una respuesta efectiva y coherente con el avance y evolución del escenario inicial. La mejor estrategia a la hora de combatir la infodemia y con ella las noticias falsas, es la identificación y el acercamiento previo, así como el uso frecuente de fuentes confiables de información. También están disponibles los "servicios de verificación de hechos" o *fact-checking*, a través de los cuales inclusive el periodismo de investigación realiza una comprobación de la información relacionada a uno o varios eventos; hoy en día muy focalizado a las noticias o rumores en Internet. Algunos de los proveedores que ofrecen este tipo de servicios a través de Internet son:

Fact Check Explorer: Barra de búsqueda que permite ingresar palabras claves, así como también citas o párrafos completos para desplegar historias relacionadas que ya han sido verificadas.

ImgOps: Motor de búsqueda de imágenes para detectar anomalías que indiquen manipulación o falsedad**.**

Fake News Detector: Sistema que identifica y marca todas las noticias falsas en una página web, incluso dentro de las redes sociales más populares**.**

NewsCracker: Sistema basado en tecnología *Machine Learning* que permite clasificar la calidad de cualquier publicación en una escala del 0 a 10 en función de su veracidad.

La pandemia como escenario

La versión 14 del informe de riesgos global del año 2019 ubica en la décima posición del Top 10 de eventos con mayor impacto la denominada "propagación de enfermedades infecciosas" por detrás de eventos como: "desastres ambientales causados por el hombre", "ciberataques" y "eventos climáticos extremos", entre otros. Si la identificación y planteamiento de escenarios es una práctica recurrente a la hora de prever los hechos que pueden llegar a requerir un comportamiento resiliente en una organización, ¿por qué los gobiernos y empresas subestimaron la pandemia como escenario a la hora de planificar sus planes de respuesta y recuperación?

En el mes de septiembre del año 2007, más de 2.700 empresas de servicios del sector financiero de los Estados Unidos participaron en un ejercicio simulado para evaluar el escenario de una pandemia global. El ejercicio denominado "FBIIC/FSSCC Pandemic Flu Exercise of 2007", fue el resultado del trabajo realizado por la asociación SIFMA - "Securities Industry and Financial Markets Association", con el fin último de medir la capacidad de mantener la continuidad de las actividades de negocio en un escenario de pandemia. Era la primera vez que esta asociación cambiaba el enfoque de sus pruebas anuales, focalizadas principalmente en verificar temas netamente técnicos. El escenario planteado fue el de un brote global de influenza originado por una cepa de gripe que se transmitía de persona a persona y podía causar una enfermedad grave con bajo nivel de inmunidad natural y una cantidad limitada de vacuna disponible. Los hospitales y en particular, las unidades de cuidados intensivos serían saturadas rápidamente tras la llegada del virus. Los ventiladores, las camas de hospital y el personal competente escasearían. Los suministros antivirales en el país se agotarían en la mitad de la ola pandémica y los Centros para el Control y la Prevención de Enfermedades - CDC estimarían que la vacuna adaptada a esta nueva cepa de gripe pandémica no estaría disponible en el corto plazo; así mismo, anunciarían que podría haber una segunda ola de infección (inclusive una tercera ola). El ejercicio de 2007 fue una oportunidad invaluable de evaluar los planes de pandemia de las empresas participes, en un escenario riguroso y detallado. Los insumos para recrear paulatinamente el escenario fueron diseñados para estresar a los participantes asumiendo las siguientes condiciones:

- Impacto global de una infección ampliamente dispersa.
- Altos niveles de absentismo durante un período prolongado de tiempo.
- Daños e interrupciones en las infraestructuras críticas.
- La implementación del distanciamiento social y el teletrabajo.
- La disminución del desempeño de los servicios de Internet residencial.
- La reducción en los viajes aéreos y terrestres en un 40%.
- El aumento en los precios del gas.
- El estancamiento de la producción de refinerías.
- La cancelación de eventos masivos.
- El alto impacto en el mercado (bajo nivel de liquidez).
- Cambios en el comportamiento de los clientes (aumento en la demanda de comercio electrónico).

Al finalizar, el ejercicio destacó la necesidad imperante de incluir el escenario de pandemia en las fases de planeación de las organizaciones, debido a que al menos un tercio de las empresas participantes declararon que para la época aún no habían desarrollado planes de continuidad específicos para afrontar una situación similar. Otras organizaciones solo tenían planes de continuidad tradicionales que se centraban en interrupciones limitadas por factores de tiempo, geografía y a menudo, sesgadas en los niveles de impacto. Aquellas que si tenían un plan acorde y, en especial las de mayor tamaño, planeaban usar la estrategia del teletrabajo pese a que muy pocas de ellas pudieron simular dicha estrategia durante el ejercicio; mientras que las empresas pequeñas y medianas aplicarían estrategias basadas en el distanciamiento social, turnos intercalados, limitaciones en el uso de espacios físicos y el uso de equipo de protección personal (PPE). Así mismo, se identificó que la estrategia de entrenamiento cruzado para suplir la ausencia de personal era más probable en las empresas de mayor envergadura. Muchas empresas pequeñas y medianas argumentaron que el teletrabajo no era factible porque:

- Las funciones criticas requerían al personal en sitio.
- No se tenía la infraestructura informática necesaria.
- Se presentarían problemas de seguridad con los servicios de acceso remoto.

Durante el pico de la pandemia solo las empresas grandes tendrían mayor probabilidad de pagar salarios a sus empleados ausentes. Sin embargo, el porcentaje disminuiría a medida que el tiempo transcurría y la pandemia se aplacaba. Los resultados también indicaron que al menos el 20% de las empresas ofrecerían incentivos financieros para alentar a los empleados a ir a trabajar cuando el absentismo estaba en su nivel más alto.

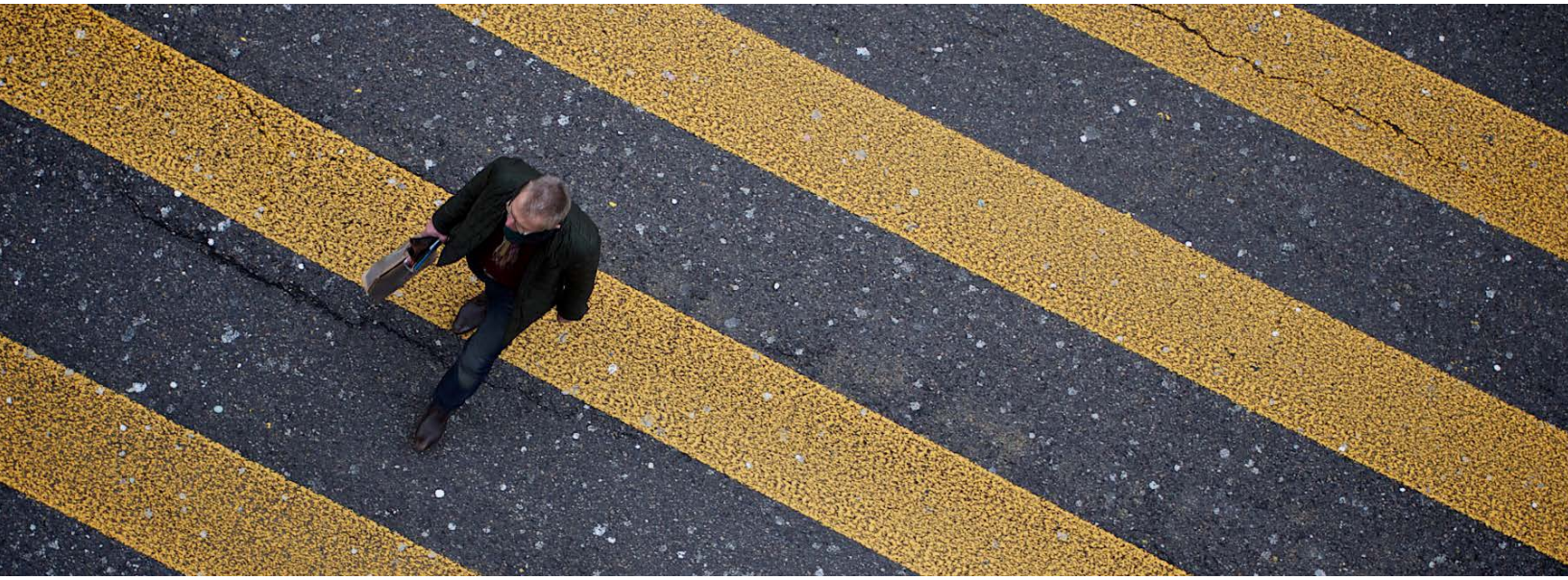
Conclusiones y Recomendaciones

Trabajo desarrollado en casa

Muchas empresas a nivel mundial han adoptado el teletrabajo como una estrategia de operación provisional que se extenderá hasta fin de año e, inclusive, para algunos que ya sopesaron el costo del riesgo y los beneficios de este modelo han instaurado la práctica como una medida definitiva. En este sentido, el Ministerio de Tecnologías de la Información y las Comunicaciones publicó el pasado 3 de junio de 2020, el Decreto 771 que faculta a las empresas para reemplazar el auxilio de transporte por el auxilio de conectividad. Los beneficiarios de este decreto reciente serían aquellos empleados cuyo ingreso mensual sea inferior a 2 salarios mínimos y el beneficio perdurará hasta el momento en que finalice la declaración de emergencia por pandemia. Para aquellas empresas que implementaron el modelo del teletrabajo se recomienda la puesta en marcha de algunas medidas mínimas iniciales de protección para sus usuarios remotos como:

- El robustecimiento de contraseñas en los dispositivos de acceso Wifi.
- La identificación de todos los dispositivos conectados en el hogar.
- En la medida de lo posible la implementación de parches de seguridad en los dispositivos conectados a la red Wifi.
- Cambiar las contraseñas de acceso a la red de Wifi que vienen por defecto y modificar las credenciales con regularidad.
- Seleccionar un protocolo cifrado adecuado en la configuración del dispositivo de Wifi (preferiblemente WPA3).
- Deshabilitar los servicios de configuración WPS.
- Deshabilitar las opciones relacionadas con Universal Plug and Play (UPnP).
- Deshabilitar las opciones de gestión remota en los dispositivos de conexión a los servicios de Internet.
- Cambiar el Identificador de red (SSID) que ha sido configurado por defecto.
- Usar la banda de 5 GHz para reducir el alcance de la señal inalámbrica.
- Apagar los dispositivos de conexión a la red cuando no estén en uso.
- Verificar que el dispositivo Wifi propio o el suministrado por el proveedor no esté siendo usado por desconocidos.
- Contactar al proveedor para solicitar ayuda con esta verificación puede ser útil.
- Evitar el uso de enlaces que parezcan sospechosos.
- Descargar contenido únicamente de fuentes confiables.
- No acceder desde redes públicas como aeropuertos, restaurantes, u otros.

- Si se utilizan equipos de cómputo compartidos, crear perfiles de acceso separados.
- Uso de sistemas operativos, software y antivirus legal y actualizado.
- Implementar al menos dos mecanismos de autenticación para el acceso a las aplicaciones.
- Implementar un procedimiento para la gestión de incidentes que permita atender la propagación de amenazas originadas desde los equipos de cómputo personales y/o dispositivos móviles.
- Considerar diversas opciones de conectividad remota: software VPN, VPN a través de hardware y el uso de tecnología VDI.
- Desarrollar políticas enfocadas a la práctica BYOD (Bring Your Own Device).
- Verificar que el acceso a servicios de computación implementados en la nube está restringido al direccionamiento IP de la Organización.
- Asegurarse que existen líneas de comunicación exclusivas entre el proveedor de servicios de computo en la nube y la Organización.
- Verificar los niveles de uso y desempeño de los servicios que son consumidos en un esquema de computo implementado a través de un CSP (Cloud Service Providers).
- Si las condiciones de operación lo exigen, se recomienda hacer uso de las videoconferencias solo cuando sea necesario, fomentar el uso de las comunicaciones por voz y/o a través de texto.
- Revisar y considerar las coberturas de las pólizas de seguro de responsabilidad profesional que garanticen un cubrimiento adecuado cuando sea necesario implementar las estrategias de trabajo remoto por largos periodos de tiempo.
- Desarrollar y/o ajustar sus planes de comunicación para cubrir necesidades de información de empleados no acostumbrados al teletrabajo.



Continuidad del Negocio y Ciberseguridad

Los resultados del evento que el mundo vive hoy en día, permiten consolidar una serie de recomendaciones que incitan posibles ajustes a las buenas prácticas ya establecidas por los diferentes organismos que a nivel internacional promueven esta doctrina:

- Acudir con regularidad a los resultados de los análisis de riesgos para identificar escenarios y elegir aquellos que proponen un nivel de impacto inherente especialmente alto sin subestimar las posibles amenazas relacionadas. Hacer uso de estos escenarios como herramienta de análisis a través de lo que denominamos frecuentemente como “el peor escenario”.

- Está en los líderes de las organizaciones exaltar el impacto que la pandemia generó en los negocios, la comunidad y la salud de las personas. Cuando la crisis actual finalice las empresas deberán fortalecer sus controles y aprovechar el resultado para aumentar el grado de conciencia y preparación.

- Las empresas que logren superar esta adversidad (*reconfigurando o rediseñando sus servicios, productos y/o su enfoque empresarial*), sobrevivirán ya que adaptarán sus modelos de negocio a las nuevas circunstancias a las que nos enfrentaremos. Las empresas renuentes al cambio posiblemente tenderán a desaparecer.

- Para ciertos escenarios, las estrategias implementadas por las organizaciones deben evitar la dependencia en la respuesta y/o el apoyo de terceros, ya que estos se pueden ver impedidos por el mismo evento y eventualmente, se concentrarán en resolver y/o mitigar sus propios impactos.

- Las estrategias previstas también deben contemplar posibles cambios supeditados a la evolución del evento inicial.

- Las organizaciones pueden plantearse la posibilidad de participar activamente en la creación de asociaciones regionales que ofrezcan la oportunidad de trabajar conjuntamente para mejorar el intercambio de información y la coordinación de respuestas a eventos de gran magnitud. Dichas asociaciones también permitirán crear vías de acceso a agencias gubernamentales locales, estatales y/o federales.

- Los bancos deberían revisar sus planes de financiación en situaciones de contingencia y hacer ejercicios que permitan verificar las necesidades de proporcionar servicios más flexibles de cara a sus clientes. Las empresas también podrían prever la necesidad de explorar fuentes alternativas de financiamiento sobre las ya disponibles.

- Es probable que haya escenarios que requieran la implementación preventiva de medidas que permitan reducir los encuentros cara a cara, modificar el horario de atención y/o reubicar al personal en oficinas para disminuir la posibilidad de propagación de enfermedades infecciosas.

- Las organizaciones deberán reforzar sus estrategias de entrenamiento cruzado. Esto debe ser acompañado de actividades periódicas de revisión y prueba sobre las actividades de delegación y respaldo de personal crítico requerido.

- El nivel de cultura y compromiso de la alta dirección debe ser fortalecido.

- Se deben fortalecer las regulaciones enfocadas a promover practicas asociadas con la gestión de riesgos operacionales en los diversos sectores de la industria y, en especial, en aquellos de nivel crítico para mantener la operación de los servicios básicos necesarios de un país.

Referencias

Título	Autor
Fiscalía colombiana pide captura de alcaldes por presunta corrupción durante pandemia.	DW Made for Minds.
Estudio sobre el modo de gestionar la salud en Colombia.	Ministerio de Salud y Protección Social.
¿Cómo está derrotando Corea del Sur al COVID-19?.	El planetario, Camilo Prieto.
COVID-19: Programa especial.	DW Español.
Teletrabajo: Gestión de seguridad de la información.	América Economía, César Pallavicini.
Event 201 Pandemic Exercise: Highlights Reel.	Johns Hopkins Center for Health Security, World Economic Forum, and Bill & Melinda Gates.
5 herramientas para ayudarnos a detectar 'fake news'.	TICbeat, Alberto Iglesias Fraga.
Entender la infodemia y la desinformación en la lucha contra la COVID-19.	Organización Panamericana de la Salud.
Podcast: COVID-19 and Operational Resiliency.	Kenneth E. Bentsen, Jr. and Thomas F. Price.
Colombia ocupa el puesto 39 en el ranking mundial sobre Ciberseguridad.	La República, Paola Andrea Vargas Rubio.
Instrucciones generales para la implementación de mejores prácticas organizacionales.	Superintendencia Nacional de Salud.
Management checklist for teleworking surge during the COVID-19 response.	Healthcare and Public Health Sector Coordinating Council.
Los países de Latinoamérica con más bajos estándares en ciberseguridad.	MasContainer logistics & trade news.
THE FBIIC/FSSCC PANDEMIC FLU EXERCISE OF 2007 AFTER ACTION REPORT.	U.S. Department of the Treasury, el FBIIC, la FSSCC, y la SIFMA.
The Global Risks Report 2019.	World Economic Forum.
Coronavirus (COVID-2019) en Colombia.	Instituto Nacional de Salud.

Contáctenos

Luis Alberto Páez Puerto
Gerente
CISSP, MBCP, 27001LA,
25999LA, CCNA, CCSA, CCSE
luispaez@kpmg.com
KPMG en Colombia

Bibiana Alejandra Cogollo
Consultor Senior
CBCP, Cobit Foundation,
ISO22301 AI
bcogollo@kpmg.com
KPMG en Colombia

Andrés Felipe Jaramillo González
Consultor Senior
CBCP, CFC, ISO22301 AI
andresjaramillo@kpmg.com
KPMG en Colombia

Andrés Ricardo Díaz Buitrago
Consultor Senior
22301LA, 31000A, 27001A,
ITIL Foundation
andresdiaz@kpmg.com
KPMG en Colombia

Mayra Alejandra González Uribe
Consultor Junior
mayraagonzalez@kpmg.com
KPMG en Colombia

Visita nuestra página web
home.kpmg/co

KPMG en Colombia | KPMG en Colombia | KPMG_CO | KPMG en Colombia | Kpmgencolombia