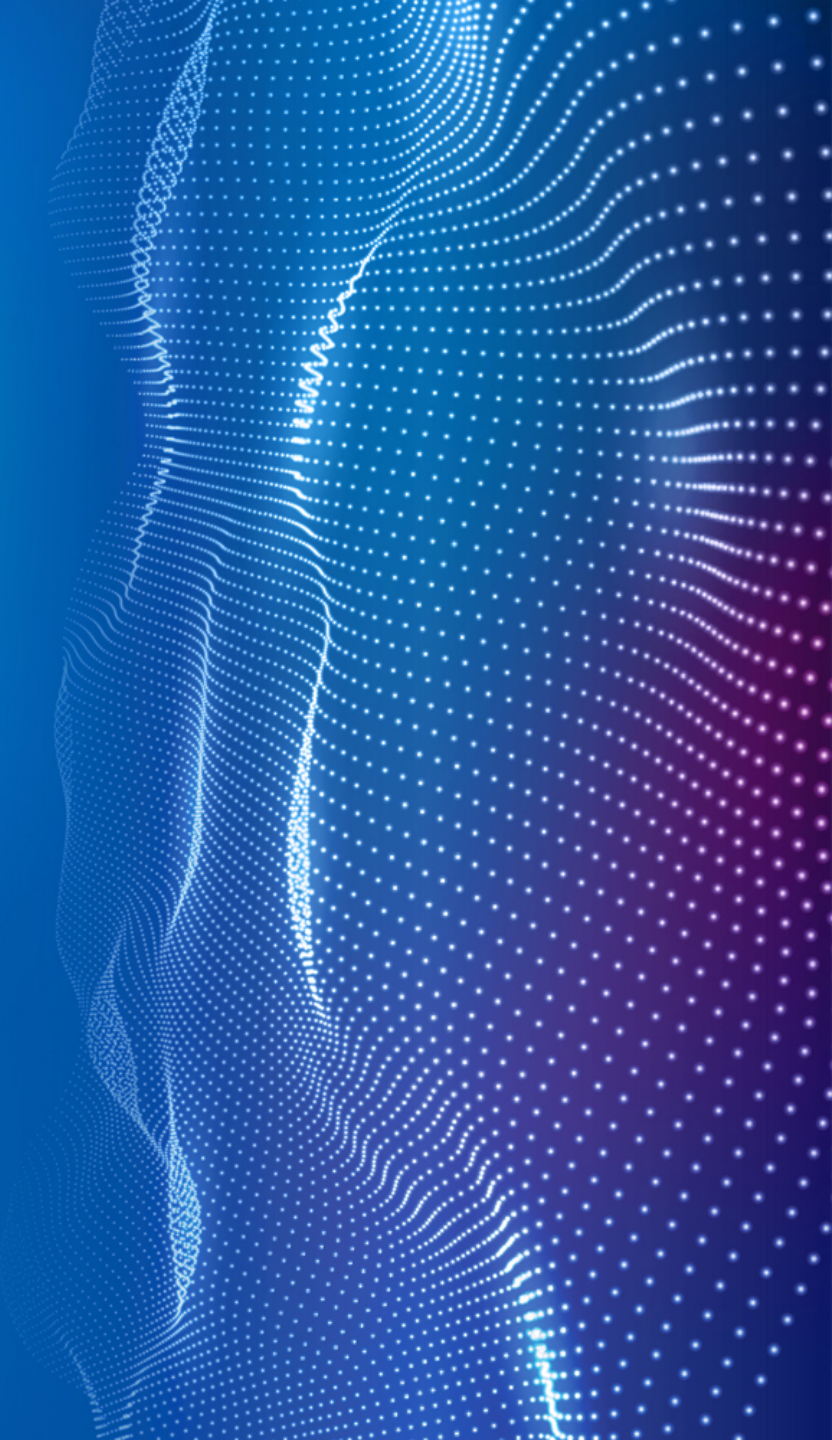
KPMG

# COVID 19

**Mantener la resiliencia del negocio**

—

2020 Marzo



# COVID 19 - Mantener la resiliencia del negocio

**COVID-19 se convirtió rápidamente en un amenaza global para las organizaciones. Entender qué es, qué precauciones considerar y cómo preparar a su organización para ser resiliente será crucial para proteger a sus colaboradores y mantener la operación. Esto implica entender cómo está su organización preparada en términos de Continuidad de Negocio y Gestión de Crisis, aspectos específicamente relacionados al personal, proveedores, cadena de suministro, infraestructura, operación TI, seguridad de la información y ciberseguridad.**

Considerando el creciente avance del COVID-19, las organizaciones deberían evaluar las siguientes consideraciones para protegerse y proteger a su personal.

## ¿Cómo mantener su organización operativa?

Confirmar que los resultados críticos de la misión de la organización son bien comprendidos de principio a fin, y que existen planes de contingencia para mantenerlos operativos. En especial las dependencias claves – procesos, ubicaciones, personas, proveedores, y sistemas TI – deben ser confirmadas y documentadas (a través de un Análisis de Impacto al Negocio (BIA – Business Impact Analysis)).

## ¿Se puede confiar en las estrategias incluidas en nuestros planes de continuidad?

Se debe asegurar que los planes de continuidad (Business Continuity Plan) reflejan los resultados críticos. La organización debe tener un BCP y estrategias de continuidad que reflejen los resultados esperados en los procesos críticos del negocio y las dependencias mapeadas en un BIA. Si es posible, estos planes deberán ser probados (lo más pronto posible) para asegurar que aún cumplen con el propósito principal frente a una posible pandemia. Adicionalmente, se debe confirmar que los contratos de seguros asociados a la continuidad del negocio provean una cobertura adecuada (de aplicar).

# COVID 19 - Mantener la resiliencia del negocio

## ¿Cómo lo gestionamos si esto se convierte en crisis?

Para salvaguardar la efectividad de la estrategia de respuesta de la organización frente a un incidente global, es importante que se formalicen los protocolos de gestión de crisis. Esto incluye procesos claros y repetibles para que un equipo de liderazgo ejecutivo los active – ya sea localmente en un centro de respuesta a emergencias o de forma remota utilizando plataformas colaborativas – de forma de dirigir la estrategia de la organización, comunicando de forma clara a colaboradores y grupos de interés.

## ¿Hemos planeado como responder a una pandemia y estamos preparados para hacerlo?

El virus COVID-19 ha sido declarado como pandemia, por lo mismo las organizaciones deben tener o trabajar en una estrategia clara para gestionar sus acciones mientras el virus se propaga. En particular, mientras el personal continua trabajando desde las instalaciones centrales de la organización, se debe confirmar la profundidad y amplitud de los servicios de limpieza e higuienización. Sin embargo, para contener el virus, las organizaciones deberán formalizar las acciones sugeridas por la OMS – Organización Mundial de la Salud y organismos locales pertinentes, por ejemplo distancia social traduciéndose esto en home office, teletrabajo, turnos separados e incluso gestionar el cumplimiento de los resultados asociados a la operación crítica con el personal mínimo.

# COVID 19 - ¿Qué podemos hacer ahora mismo?

## Arreglos alternativos para el trabajo

Aclarar las implicaciones del home office o trabajo desde casa. Las organizaciones habitualmente confían en la estrategia “trabajemos desde casa” en las crisis de esta naturaleza. Sin embargo, es importante confirmar el número de preguntas claves relacionadas a esta estrategia, previo a su implementación:

- ¿Las políticas y procedimientos permiten a la organización trasladar capacidades al personal para hacer home office?
- ¿El personal clave cuenta con accesos remotos a los sistemas críticos de la organización?¿aseguramos el soporte remoto durante la operación?
- ¿Cuánto tiempo se pueden mantener los procesos críticos con el personal trabajando desde casa?
- ¿Cómo nos comunicaremos con el personal no clave que eventualmente sea requerido?
- ¿Se ha probado el rendimiento de los enlaces de comunicación y de los sistemas críticos?
- ¿La organización está preparada para permitir que la mayoría de los trabajadores estén en home office y mantener los resultados esperados en la operación de los procesos críticos?

## Comunicaciones con el personal

La organización debería monitorear y mantener comunicación constante con el personal, proveerlos de información actualizada del estado de propagación o medidas de contención del COVID-19 y de los procesos que serán implementados para protegerlos y mantener la operación crítica.

Las organizaciones deberán guiar al personal para que se comunique con el área de Recursos Humanos si tienen algún viaje personal o laboral dentro y fuera del país – especialmente a los países en los que han sido confirmados casos de infección.

# COVID 19 - ¿Qué podemos hacer ahora mismo?

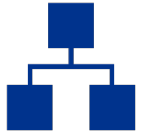
## Gestión de proveedores y cadena de suministro

Para las organizaciones cuyos procesos críticos de la cadena de valor dependen de personal externo o proveedores, se recomienda planificarse ante la eventualidad de no contar con su disponibilidad o que estos se encuentren inhabilitados e incluso trabajando en contingencia. Es importante que se tome contacto con los proveedores críticos para que la organización asegure los suministros necesarios para apalancar sus procesos críticos.

**Como parte de sus planes de continuidad, las organizaciones deberán considerar:**

- Determinar proveedores y vendedores críticos según lo definido por el negocio.
- Contactar con proveedores críticos de la cadena de suministro para informarse de sus planes de contingencia para proporcionar productos / servicios neurálgicos para sus clientes.
- Trabajar con el área de aprovisionamiento o compras para identificar proveedores alternativos (que puedan haber sido evaluados previamente).
- Desarrollar e integrar una estructura de control para las exportaciones de países potencialmente afectados.
- Determinar la ubicación de los vendedores / proveedores y definir rutas críticas.
- Explorar alternativas de transporte.
- Revisar los contratos con clientes y proveedores claves, para comprender las responsabilidades en caso de escasez de suministros.
- Revisar junto a los proveedores críticos los planes de continuidad de ambas partes.
- Desarrollar planes para compras repentinas antes, durante y entre olas pandémicas.
- Establecer escenarios para los cuales las órdenes se podrían ver potencialmente afectadas.
- Tener visibilidad de los niveles de madurez de su cadena de suministro para evaluar el impacto general de la pandemia.
- Obtener transparencia sobre cuáles son los materiales críticos con el mayor impacto en sus procesos de negocio, si corresponde.
- Evaluar las posiciones de inventario y las prioridades de fabricación, si corresponde.

# COVID 19 - ¿Qué podemos hacer ahora mismo?



## Operaciones de TI

Las organizaciones que delegan el soporte de sus operaciones de TI en servicios internacionales con terceros, deberán planificarse para una carga adicional en caso de que el proveedor se vea afectado por el virus. La planificación debería considerar evaluación de capacidades, herramientas y requerimientos técnicos, gestión de seguridad y accesos,  las capacidades para entregar soporte al trabajo remoto, entre otras.

Los equipos de TI onsite/internos pueden verse igualmente afectados. Para mitigar ese impacto, las organizaciones deberán considerar establecer equipos separados o guardias pasivas / activas.

La posibilidad de autoservicio o autogestión debería ser potenciada para aliviar la carga de trabajo del personal mínimo asignado. Se debe definir un nivel mínimo aceptable de soporte para aplicaciones críticas y servicios centrales, y se deben definir SLA para pandemias. Estas definiciones deberán comunicarse oportunamente al negocio para mostrarse alineados.

## Infraestructura TI

Las organizaciones deberán identificar los momentos de altas cargas de tráfico en la red ante eventos donde todos o la mayoría del personal esté en home office, pudiendo tomar definiciones de bloqueo de tráfico no corporativo. Se deberá realizar una evaluación para identificar cualquier brecha y remediarla. La seguridad en la red, incluida la gestión de accesos remotos, deberá ser incluida en el plan. En un evento donde el personal clave no se encuentre disponible, se deben identificar alternativas y proveer accesos desde ubicaciones remotas incluso locaciones internacionales.

Los accesos a servicios Cloud deberán ser revisados para asegurar que cumplan con eventuales requerimientos de usuarios remotos. Es importante entender que los procesos de negocio pueden cambiar durante una pandemia, que se puede incurrir en mayor demanda de la habitual sobre los servicios TI.

# COVID 19 - ¿Qué podemos hacer ahora mismo?

## Manténgase ciber vigilante

Mientras más energía se invierte en asegurar el bienestar del personal, el equipo de Ciberseguridad debe mantenerse alerta para confirmar que los procesos de seguridad no se quiebren. Se debe evitar la tendencia de crear soluciones que puedan introducir nuevos riesgos al ecosistema tecnológico de la organización.

Ya existen señales de criminales que han utilizado el coronavirus para desinformar, infectar redes con virus informáticos ya conocidos como el ransomware e incluso para perpetrar ataques de ingeniería social y phishing dirigidos. Se debe trabajar a la par con los proveedores y partners claves de ciberseguridad y TI para asegurar que se entiendan las nuevas amenazas de seguridad y los planes de resiliencia que deben ser activados. Si se conocen los desafíos del proveedor, se debe trabajar en determinar el impacto en la seguridad y su cumplimiento.

Las organizaciones deben considerar establecer protocolos de ciberseguridad para mantener una comunicación actualizada, al personal informado y proveer los accesos a recursos claves. Se debe mantener especial énfasis en nuevos vectores de ataques informáticos, considerando: periodos largos en el proceso de parcheado de seguridad, aumento en patrones de ataques, la recepción de campañas de correo electrónico malicioso y dirigido al personal de la organización, así como a la navegación por redes públicas de los usuarios, entre otros.

**kpmg.cl**