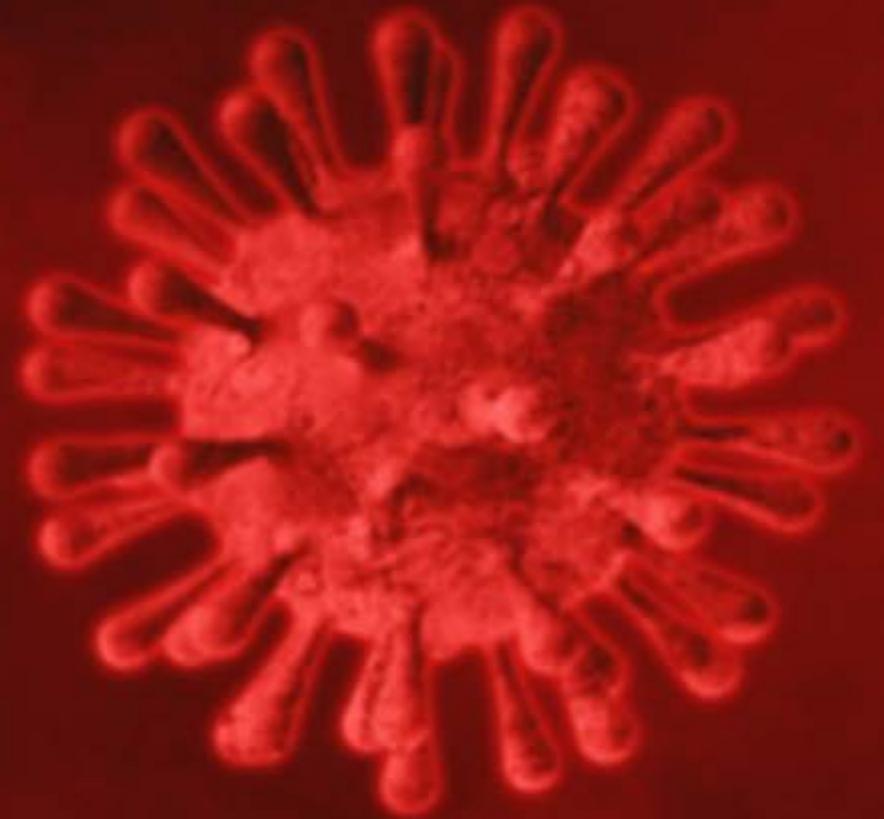
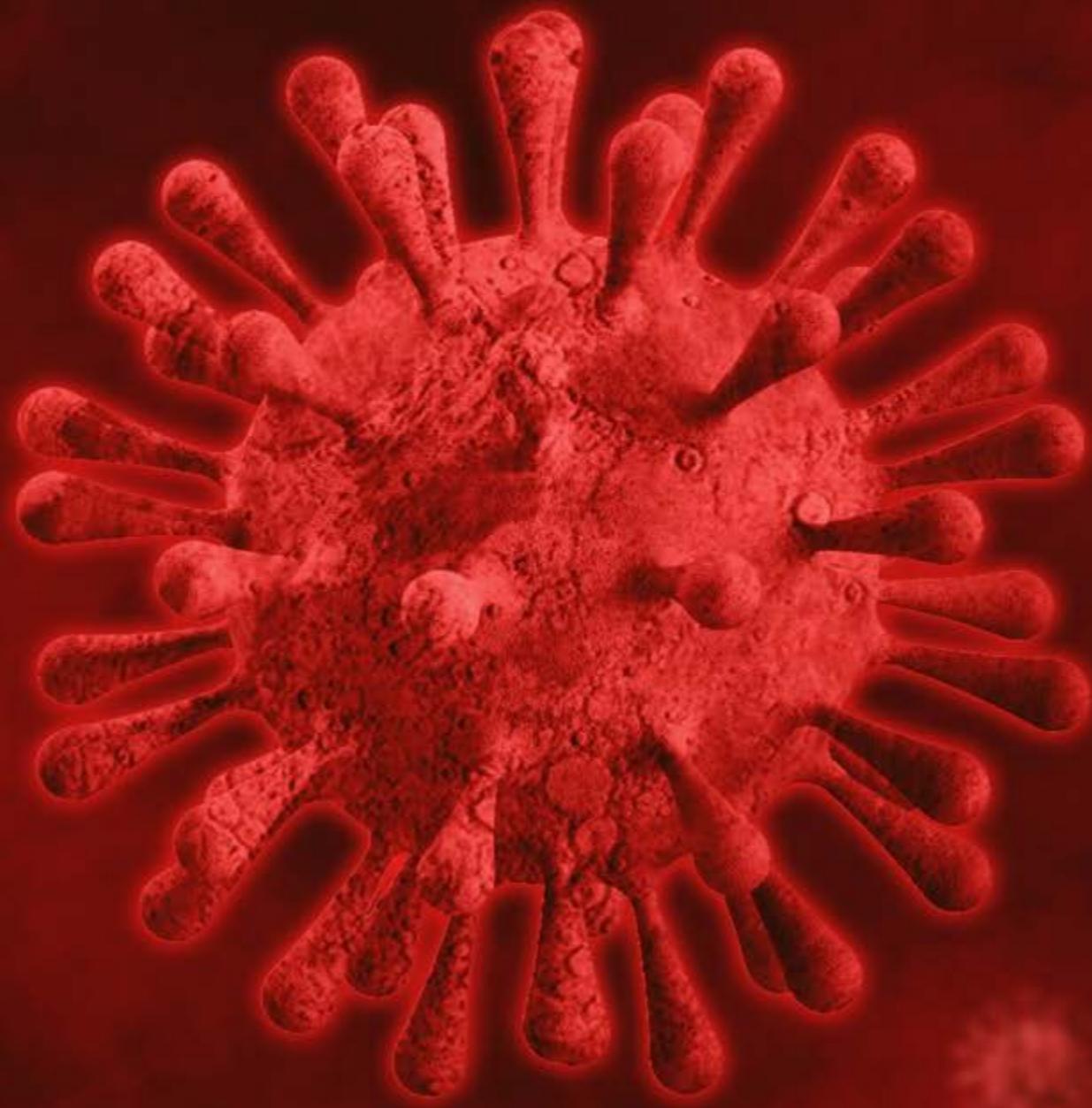


Lecciones aprendidas



ABSTRACT

La pandemia COVID-19 está afectando al mundo de una forma que la mayoría de nosotros ni imaginaba. En este contexto, las organizaciones públicas y privadas están enfrentando muchos desafíos para mantener sus operaciones, con diferente grado de éxito.

Indudablemente hay muchas cosas para mejorar en lo que a capacidad de respuesta se refiere y en estos aspectos nos queremos enfocar, ya que históricamente los momentos de crisis han sido un catalizador fundamental para mejorar los enfoques metodológicos que guían a las organizaciones en sus prácticas de gestión; y la planificación de la continuidad del negocio no ha sido una excepción.

Los atentados del 11S del 2001 dejaron en claro que las organizaciones tenían que prepararse para responder ante cualquier tipo de contingencias, incluso las inimaginables, lo que derivó en un cambio muy importante en los enfoques metodológicos aplicados hasta ese momento para el desarrollo de soluciones de continuidad del negocio. Más adelante, en el 2008, a raíz de la crisis financiera en USA, donde el 85% de los servicios básicos eran brindados por empresas privadas, se puso en evidencia la necesidad de contar con un marco de referencia que permitiera, en este caso al gobierno, evaluar la calidad de las soluciones de continuidad operativa con que contaba las empresas críticas del país, lo que impulsó la aplicación del estándar desarrollado por el British Standards Institution, BS 25999, que más tarde dieran lugar a la Norma ISO 22301.

Hoy esta pandemia por su parte está impulsando fuertemente la adopción de un enfoque de "Resiliencia Corporativa" como un paso adicional a la Continuidad del Negocio, para efectivamente poder lograr lo que todas las organizaciones desean: garantizar la prosperidad de su negocio a largo plazo.

En tal sentido, vamos a analizar los principales aciertos y errores que se están registrando en relación a la gestión de la crisis y las medidas de respuesta que están adoptando las organizaciones para dar continuidad a sus operaciones, con la intención de capitalizar este aprendizaje, identificando oportunidades de mejora.

Graciela Ricci, CISA, CGEIT, CRISC - Directora Valor y Gestión TI

CONTENIDO

¿ESTÁBAMOS PREPARADOS?

**MÁS ALLÁ DE LA CONTINUIDAD
OPERATIVA: RESILIENCIA CORPORATIVA**

¿Y DESPUÉS QUÉ?

APRENDIZAJES DE LA SITUACIÓN ACTUAL

SUGERENCIAS

¿Estábamos preparados?

Claramente la capacidad de respuesta que están teniendo las organizaciones que han trabajado en la planificación de la continuidad de su negocio y cuentan con estrategias y planes en tal sentido, está siendo muy superior que la de la mayoría de aquellas empresas que nunca lo hicieron.

No obstante, algunas se sienten algo defraudadas respecto a la efectividad de los esfuerzos que venían realizando en el tema, o les parece que esta situación excede totalmente su nivel de preparación. En algunos casos han debido improvisar y definir respuestas "sobre la marcha" para enfrentar la situación que están viviendo, y presientes, por no decir que están seguras, que deberán enfrentar más desafíos que nunca antes habían imaginado.

Esta falta de preparación percibida suele ser más fuerte en las organizaciones que han trabajado en la planificación de la continuidad del negocio con el objetivo fundamental de satisfacer requerimientos de cumplimiento, lo que las ha llevado muchas veces a adoptar una perspectiva muy parcial en relación a la capacidad de recuperación real que buscan garantizar. Dicha "parcialidad" puede observarse en relación a las etapas y/o escenarios considerados, el entrenamiento del personal involucrado, la disponibilidad de los recursos requeridos para ejecutar las estrategias y planes definidos o el nivel de actualización de estos. Por otro lado la calidad de los planes desarrollados puede variar mucho dependiendo de los enfoques metodológicos aplicados así como del conocimiento y experiencia de los responsables de la tarea. A continuación presentamos algunos aspectos que entendemos de interés analizar en relación a la capacidad de respuesta observada en general.





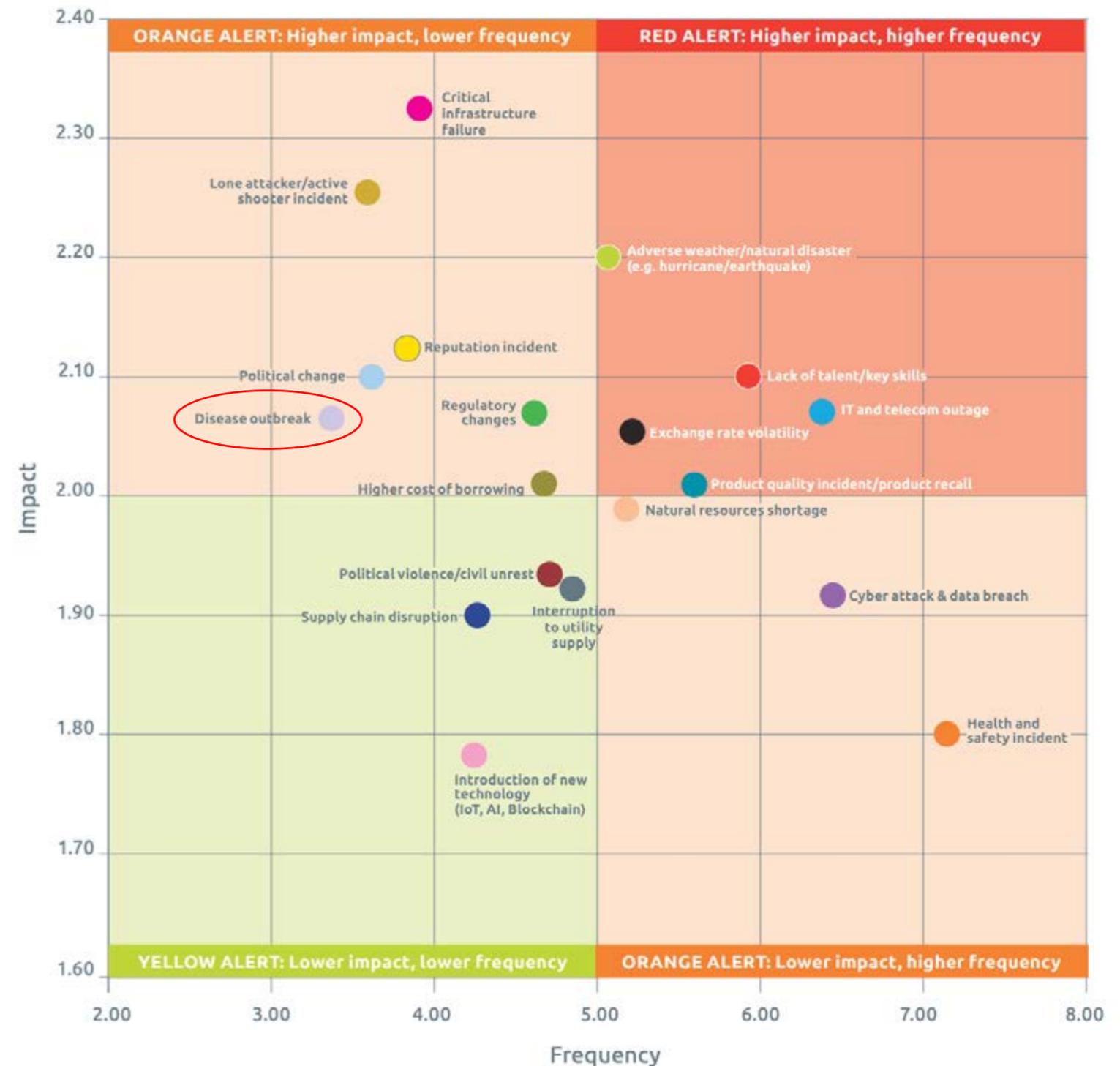
Capacidad de detección: ¿alguien lo esperaba?

La incapacidad de las organizaciones de poder anticipar la situación que estamos viviendo refleja lo que sucedió en líneas generales a nivel global. No obstante, para buscar señales de alerta no es necesario retroceder mucho en el tiempo: la epidemia de SARS en el 2004, la del virus H1N1 en el 2009, o el Ébola en el 2015, y en el 2018, la Organización Mundial de la Salud (OMS) advertía que “una epidemia desastrosa podía comenzar en cualquier país, en cualquier momento y matar a millones de personas, porque no estamos todavía preparados”

El informe del Business Continuity Institute (BCI) “Horizon Scan Report” correspondiente al año 2018, por su parte incluye un artículo específico en relación al tema: “Case Study: Pandemics”, donde menciona que varios gobiernos, entre ellos los de USA, Australia y Canadá; y organismos internacionales, son conscientes de la amenaza que supone una pandemia y están brindando asesoramiento a las organizaciones respecto a cómo prepararse para responder ante una emergencia sanitaria; considerando los Planes de Continuidad del Negocio una parte fundamental de esta respuesta. También incluye declaraciones de la OMS en relación a la importancia de contar con planes de continuidad del negocio., indicando que “están en el centro de la preparación ante una emergencia (sanitaria) de todos los niveles y grupos de la sociedad”.

Asimismo, el "Horizon Scan Report" del año 2019, incluye como "Cisne Negro"¹ (sucesos de baja probabilidad pero alto impacto), los "Brotos de Enfermedades". Aparentemente los avisos estaban, pero no los escuchamos.

¹ La teoría del cisne negro fue desarrollada por el filósofo e investigador libanés Nassim Taleb, y es una metáfora que se asocia a un suceso inesperado, de gran impacto socioeconómico y que, una vez pasado se racionaliza por retrospectión, haciendo que parezca predecible o explicable, dando impresión de que se esperaba que ocurriera. Algunos ejemplos de "cisne negros" son el inicio de la Primera Guerra Mundial, la gripe española o los atentados del 11 de septiembre de 2001. Algunos autores han identificado esta pandemia también como un "cisne negro", pero el propio Nassim Taleb lo ha rechazado al considerar que no cumple con los requisitos de su teoría. Otros analistas califican esta pandemia por coronavirus como "rinoceronte gris" porque lo consideran un evento predecible.



Horizon Scan Report 2019, Business Continuity Institute

Evaluación de riesgos y amenazas — últimos 12 meses

Los incidentes de salud reemplazan a IT como la principal causa de alteración en los últimos doce meses

Principales causas de alteración en los últimos 12 meses (Risk Index Rating)



Incidentes de salud

13.9



Interrupciones del soporte IT & comunicaciones

13.0



Incidentes de seguridad

12.0



Pérdida de talentos clave

11.5



Ciberataques y violaciones de datos

11.2

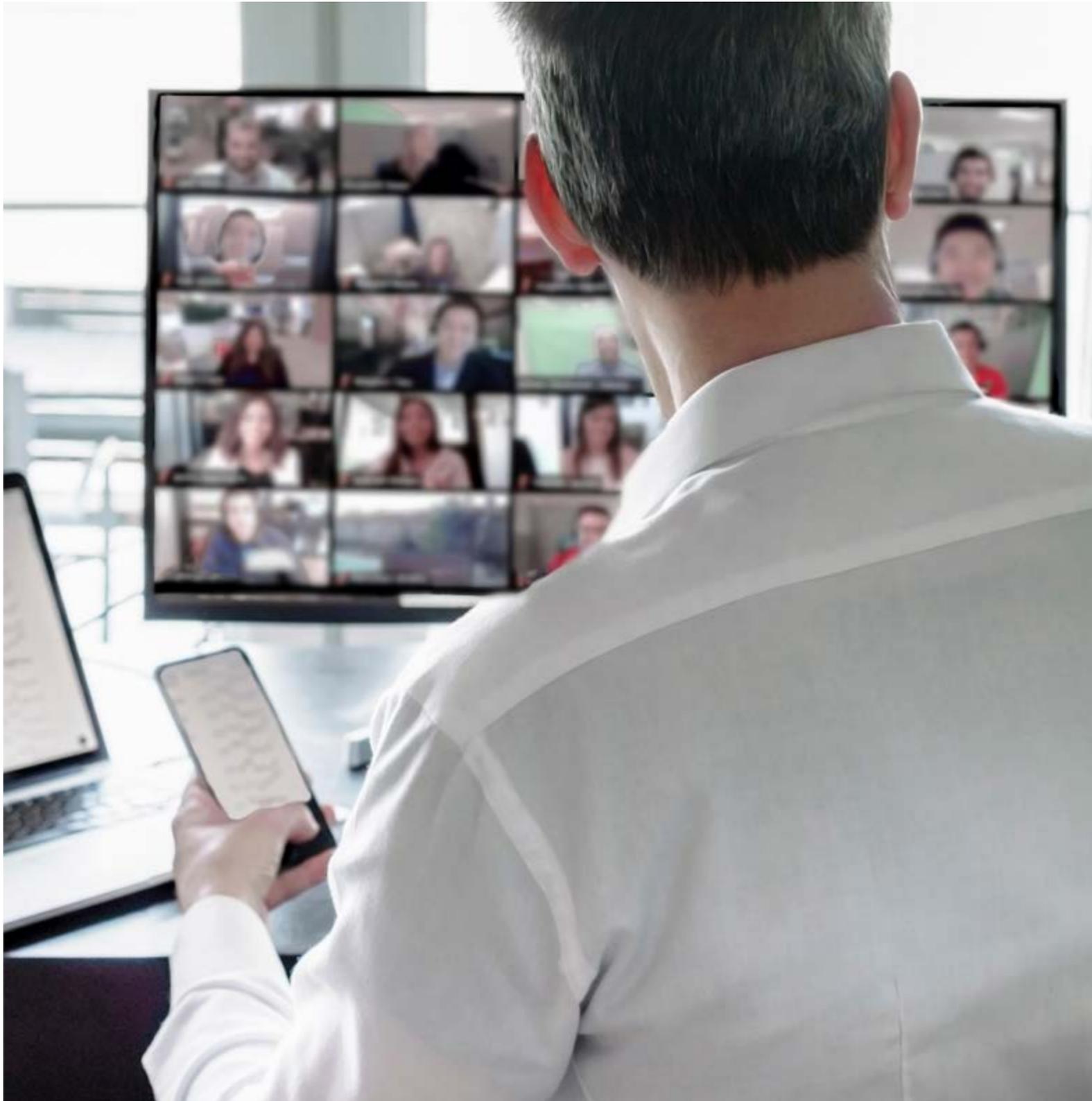
Horizon Scan Report 2020,
Business Continuity Institute

Mientras que en el reporte del año 2020, recoge las evaluaciones de riesgos realizadas por las organizaciones participantes, considerando los 12 meses anteriores, donde se ve que el riesgo “Incidentes asociados a la Salud” figura como el de mayor exposición, ocupando el primer lugar, desplazando al riesgo “Interrupciones de IT y Telecomunicaciones”, que históricamente encabezaba la lista, a un segundo lugar. Cabe acotar que al momento de realizarse ese estudio ya habían comenzado los contagios del COVID-19.

Y si bien este es un dato puntual y no una tendencia, nos hace preguntarnos en cuántos casos, si al área de Riesgos Operativos de una organización hubiera reunido evaluaciones con resultados similares a estos, si esta información hubiera llegado al área de Continuidad Operativa. De hecho ahora mismo hay varias organizaciones en la región, en las que los equipos de Continuidad Operativa no están participando en la gestión de la crisis, ni como asesores, poniendo en evidencia la falta de coordinación entre prácticas que deberían aportar a la capacidad de respuesta de las organizaciones, lo cual analizaremos en detalle más adelante.

Por otro lado, analizando estos reportes, llama la atención las diferencias existentes entre lo que las organizaciones indican como preocupaciones para un período y lo que finalmente sucede; incluso considerando un horizonte de solo 12 meses.

De todas formas, en relación a la pandemia, creo que si nos hubieran preguntado, solo 2 semanas antes de declarada la cuarentena que nos imaginábamos que iba a pasar, muy pocos hubieran descrito la situación actual.



Gestión de la crisis. ¿Qué sucedió diferente a lo planificado?

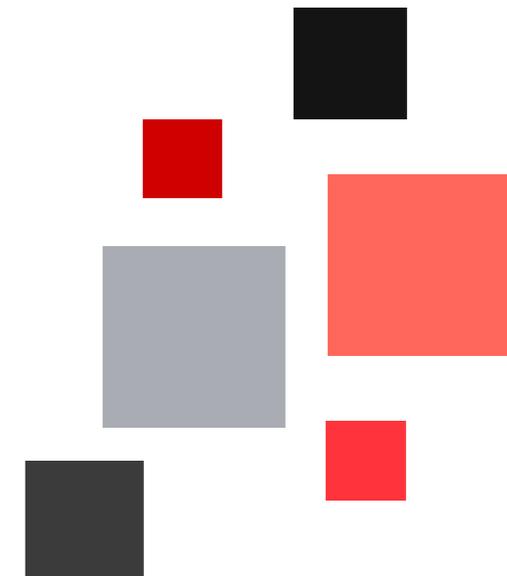
La planificación de la continuidad del negocio incluye la definición de las estrategias asociadas a la gestión de una eventual crisis derivada de la contingencia; las que recogen la forma en que la organización desea reducir y/o contener el daño, respondiendo en forma inmediata para proteger la integridad de las personas y sus activos; incluyendo como tales su imagen e información. No obstante lo anterior, muchas organizaciones debieron realizar "ajustes" a sus estrategias para responder a la situación actual.

¿Dónde se originaron las diferencias? Típicamente pensamos en una crisis de efecto "golpe": muy intensa en los primeros momentos, tendiendo luego a disminuir; pero estamos enfrentando una crisis tipo "quemadura", cuyo peor momento no necesariamente es el inicial, ya que probablemente pueda empeorar con el tiempo; y aunque en términos absolutos no sea así, su prolongación en el tiempo igual representa un complicación adicional.

Pero en general, si bien esta crisis nos colocó en un escenario diferente del que la mayoría de las organizaciones habían considerado, la planificación y el nivel de preparación que tenían les han resultado de mucha utilidad; pese a que hay cosas para mejorar.

Uno de los problemas es que parte de las actividades de "respuesta inmediata" se están debiendo prolongar en el tiempo, solapándose con las actividades en régimen de contingencia, lo que está ocasionando algunos inconvenientes en relación a:

- **Salvaguarda de las personas.** El seguimiento de la situación del personal se está extendiendo en el tiempo, demandando un mayor esfuerzo del planificado. Pero como veremos más adelante esta actividad es fundamental, tanto por el bien del personal como de la organización.
- **Protección de la información.** Usualmente las medidas de protección de datos consideradas en las estrategias de administración de una crisis se enfocan en el momento del incidente y poco más; y no durante la operación en régimen de contingencia, donde se podría haber asumido un nivel de seguridad y control inferior al habitual. Por lo anterior, al prolongarse en el tiempo el régimen de contingencia, aumenta la exposición a sufrir incidentes de seguridad, lo que comentaremos con mayor detalle más adelante. Nótese que en esta situación en particular surge una preocupación nueva para aquellas organizaciones que no manejaban las Historias Clínicas de su personal, y es asegurar que no se divulgue información respecto a los contagios más allá del cumplimiento de los protocolos establecidos por los prestadores de Salud, ya que ésta es información privada.
- **Estrategias de comunicaciones internas y externas.** No suelen ser pensadas para mantenerse tanto tiempo, demandando un esfuerzo mayor al esperado. Adicionalmente, en este caso es muy importante el trabajo de seguimiento de la prensa, tarea que no siempre está considerada en la planificación, fundamental en relación a los informes del Gobierno, tanto en lo que respecta al desarrollo de la pandemia como a las medidas de prevención y ayuda que se van definiendo.





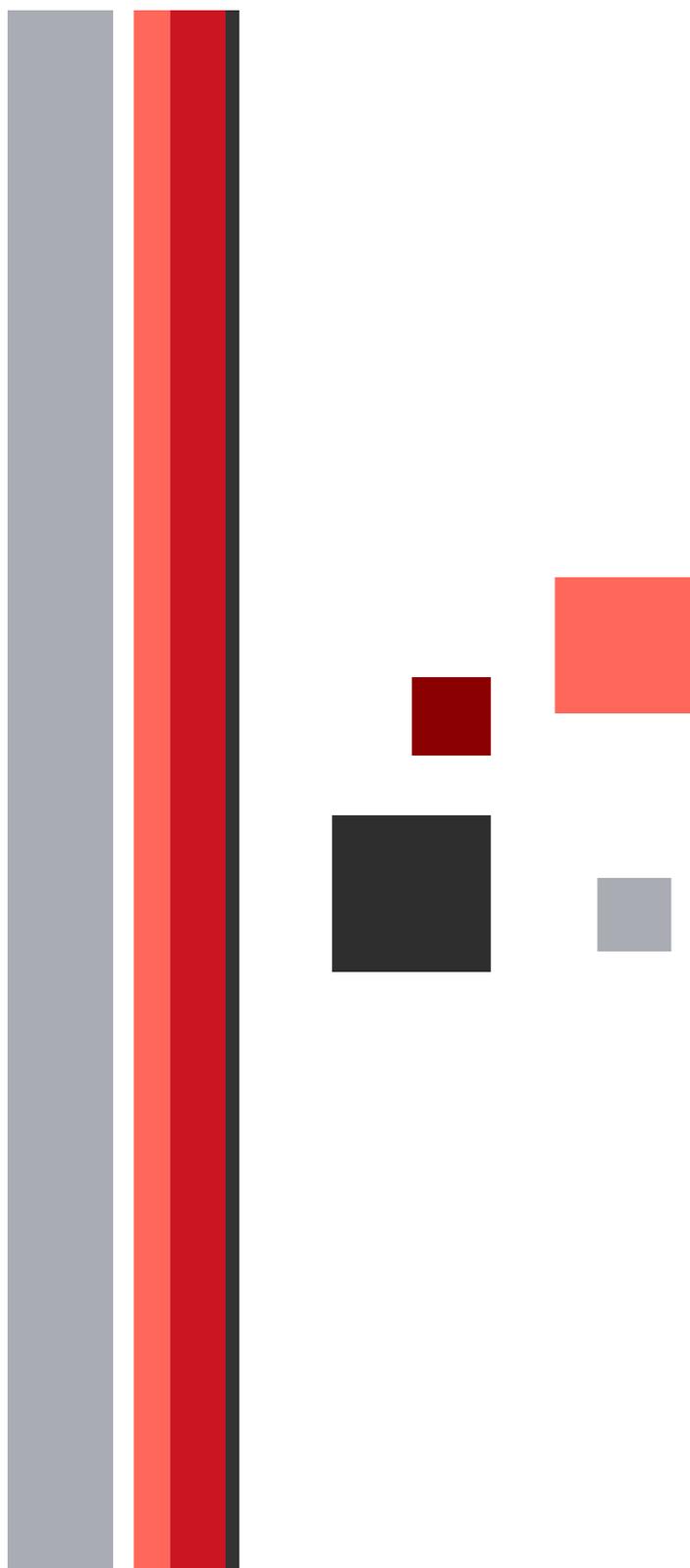
Recuperando las operaciones del negocio

Si bien las estrategias de recuperación del negocio planificadas en algunas organizaciones no se han adaptado completamente al escenario actual, en todos los casos contar con información respecto a los procesos críticos del negocio y los recursos requeridos para ejecutarlos (información recogida en los Business Impact Analysis – BIA) ha sido siempre de mucha utilidad.

Los enfoques modernos para desarrollar Planes de Contingencia, sugieren definir las estrategias de recuperación de los procesos críticos, considerando la falta de cada uno de los recursos identificados como necesarios para su ejecución. De esta forma, la respuesta no está asociada a una contingencia en particular, sino a cómo quedó la organización, luego de registrada cualquier contingencia, en términos de qué recursos están disponibles y cuáles no. El objetivo de este enfoque es garantizar que las medidas de respuesta definidas son independientes de la contingencia registrada. Entonces, ¿qué sucedió? ¿Por qué la necesidad de ajustes? Más allá de que obviamente la calidad de las estrategias de respuesta puede variar, tanto desde el punto de vista de su diseño como debido a las eventuales restricciones económicas o de cualquier tipo de cada organización; pueden haber existido problemas en relación a supuestos generales realizados y/o al análisis de cada uno de los recursos críticos considerados.

Algunos supuestos que resultaron no tan ciertos:

- **La contingencia no afectará a todos los proveedores y menos a todos los clientes en forma simultánea.** Usualmente en territorios como el nuestro, donde es difícil imaginar una contingencia de efecto masivo, se suele asumir que los proveedores siempre podrán asistirnos y nuestros clientes comenzarán a acercarse una vez que nos recuperemos.
- **Efecto Dominó.** No se "enlazarán" contingencias, no al menos en forma importante.



- **Servicios básicos.** Si bien afortunadamente los servicios básicos están operativos en Uruguay (energía, telecomunicaciones, gas, agua, transporte), en otros países de la región por su parte la infraestructura de telecomunicaciones está tratando de superar esta prueba con muchas dificultades. Por otro lado, la población está renuente a utilizar el transporte público, el cual en algunos casos se ha visto menguado, lo que ha dado lugar a estrategias nuevas, como la modalidad “full car” implementada en varios sitios.
- **La operación en régimen de contingencia no se prolongará mucho en tiempo.**
- **Vuelta a la normalidad.** Usualmente implica retornar a las operaciones tal y como eran antes de la contingencia. En relación a este supuesto, en realidad aún no hemos podido constatar en qué medida es cierto o no en este caso; pero teniendo en cuenta los comentarios de muchos expertos y nuestras propias especulaciones, sospechamos que no lo será completamente. Por este motivo, lo analizaremos con más detalle más adelante.

Analizando las posibles opciones de recuperación frente a la falta de los principales recursos críticos que típicamente se identifican, realizaremos las siguientes consideraciones:

- **Personal.** El escenario más pesimista de un eventual contagio puede resultar en que no contemos con el personal mínimo requerido para operar. Este caso, más allá de la preocupación obvia por la salud de las personas, desde el punto de vista del negocio es una situación compleja de solucionar; el problema no radica en si se evaluó esta hipótesis o no; es que en muchos casos no existe una solución satisfactoria. Por ejemplo, puede suceder que no haya en el mercado personal con el perfil necesario, la curva de aprendizaje de una determinada tarea es muy grande, etc. Lo que si puede ser una novedad es la consideración de una disponibilidad “parcial” de las personas: solo contamos con ellas en forma remota; y este último punto tiene que ver con los dos aspectos que analizaremos a continuación.

- **Instalaciones.** A raíz de la cuarentena muchas organizaciones han cerrado sus instalaciones, escenario que eventualmente se podría asimilar a "operar fuera de las instalaciones habituales", pero las estrategias definidas en este caso son válidas si se basan en el Teletrabajo ("Home Office"), siempre y cuando se cuente con la infraestructura tecnológica necesaria y ésta esté probada; pero no si dependían del traslado a instalaciones alternativas. En este caso no siempre es posible improvisar una estrategia de "Home Office", al menos no en relación a todos los procesos críticos de la organización. Basta pensar en los sectores retail, agro, transporte, manufactura, por citar algunos.
- **Teletrabajo ("Home Office").** Pese a que en muchos casos es una excelente opción en este momento, su implementación también puede presentar problemas. No todas las personas están acostumbradas a trabajar de esta forma y adicionalmente lo tiene que hacer en un momento complejo, de incertidumbre y preocupación, que puede estar afectándolos en mayor o menor medida. Por lo anterior, ser productivos hoy trabajando en forma remota, no es solo cuestión de tener disciplina y contar con los recursos necesarios (equipamiento, Internet de calidad, un ambiente adecuado, tranquilo y cómodo, etc.), lo que ya es todo un desafío; sino que hay que sobreponerse a los efectos que puede estar ocasionando el aislamiento social, la incertidumbre económica y demás preocupaciones del momento. En tal sentido es importante que las organizaciones realicen un seguimiento de la situación de sus colaboradores, tanto desde el punto de vista laboral como emocional, tratando de brindarles las herramientas y contención que necesiten.





- **Procedimientos de autorización, revisión de documentos y/o validación de registros.** La modalidad de trabajo remoto ha obligado a introducir cambios por ejemplo en los procedimientos de autorización, revisión, etc. que se hacían en forma presencial y con documentos físicos. Indudablemente contar con un Sistema de Comprobantes Fiscales Electrónico (Facturación Electrónica), el alto grado de bancarización en el país y la Firma Digital reglamentada, están siendo de gran ayuda en ese sentido en este momento.
- **Seguridad de la Información / CyberSecurity.** Por diversas restricciones, en muchos casos las organizaciones aprueban estrategias de operación en régimen de contingencia con un nivel de seguridad y control inferior al habitual. Pero en general lo hacen bajo el supuesto de que éste no se extenderá mucho en el tiempo. La situación actual, por lo tanto, puede significar una mayor exposición a riesgos de lo esperado. Por otra parte, recordemos que muchas organizaciones hoy han debido improvisar sus estrategias de operación en régimen, por lo cual el nivel real de seguridad y control puede ser incierto. Por ejemplo, puede haber muchas más personas trabajando remoto, incluso con sus propios equipos, sin que se haya revisado la política de la organización en relación a la conexión de dispositivos propios a la red corporativa ("Bring Your Own Device -BYOD), por lo cual esto puede significar una exposición desde el punto de vista de seguridad. Por otro lado, el aumento exponencial del uso de Zoom como herramienta para realizar video conferencias, que hoy congregan a muchas personas y/o en las cuales se tratan temas confidenciales, han alentado a hackers y activistas a explotar debilidades propias de esta herramienta para ganar accesos no autorizados a dichas sesiones. Ha aumentado también la exposición a hackeos en general, explotando debilidades de los accesos remotos habilitados, así como respecto al robo de identidad (Phishing²).

² El termino Phishing es utilizado para referirse a uno de los métodos más utilizados por delincuentes cibernéticos para obtener información confidencial como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima, en forma fraudulenta.

Más allá de la continuidad operativa: Resiliencia Corporativa

La capacidad de prevención y respuesta ante contingencias son dos características deseables para toda organización y el foco de la planificación de la continuidad del negocio. Por otro lado, como ya comentamos, para enfrentar esta pandemia muchas organizaciones han debido realizar ajustes en las estrategias de recuperación de sus operaciones y prácticamente todas han debido modificar su forma de operar, o lo deberán de hacer en un futuro cercano, para poder garantizar la sustentabilidad de su negocio a largo plazo. Y si bien esto genera un espacio de mejora en lo que a planificación de la continuidad operativa se refiere, en relación a lo cual realizaremos algunas sugerencias más adelante, para que las organizaciones puedan asegurar su prosperidad "más allá de la pandemia", queda claro que deberán adaptarse a una serie de cambios, tomando medidas que exceden a lo contemplado en la planificación de la continuidad de sus negocios.

Obviamente que aquellas organizaciones capaces gestionar los cambios e innovar ágilmente, adaptándose con un perfil de riesgos gestionado, tendrán una ventaja significativa sobre el resto. Esta capacidad o comportamiento la denominaremos "resiliencia corporativa" y si bien se puede presentar naturalmente en algunas organizaciones, es posible desarrollarla metódicamente.

La resiliencia corporativa busca mejorar el posicionamiento de la organización para poder anticipar y explotar cualquier tipo de cambio, incluso los derivados de una crisis, pero no solamente estos; tratando de adaptarse para prosperar, no solo para "sobrevivir". El foco en este caso pasa a ser que la organización permanezca en el tiempo siendo relevante, viable y competitiva; respondiendo positivamente al cambio.

De acuerdo al British Standards Institution BS 65000 (2014) resiliencia se define como la capacidad de una organización de anticipar y reaccionar ante un cambio, incluso una crisis, no solo con el fin de sobrevivir, sino también para evolucionar y fortalecerse.

Por todo lo anterior, es un enfoque más amplio que la planificación de la continuidad de las operaciones, por lo que se requiere de una visión de largo plazo, práctica, disciplina y compromiso.

"No es la especie más fuerte la que sobrevive; sino la que mejor se adapta a los cambios"

Charles Darwin

De acuerdo a esta visión, el BS 65000 integra pues aspectos que hacen a la prevención (antes del incidente), usualmente trabajados de acuerdo a la Norma ISO 31000 o el enfoque COSOII; aspectos vinculados a la gestión de una eventual emergencia (durante el incidente), cuyos lineamientos se pueden obtener de la Norma ISO 22320; y las actividades de respuesta inmediata y recuperación (una vez registrado el incidente) que se pautan en la Norma ISO 22301; agregando los aspectos específicos que hacen a una mejor adaptación, que se podrían desarrollar a partir de la Norma ISO 22316.

Las prácticas que sustentan la resiliencia corporativa no son ajenas a las organizaciones, pero usualmente no se las visualiza en forma integrada bajo este enfoque. Las principales son:

- Estrategias de gestión del cambio
- Gestión Integral de Riesgos (Enterprise Risk Management – ERM)
- Gestión de la Planificación de la Continuidad del Negocio
- Seguridad y CyberSecurity
- Adicionalmente existen otros aspectos necesarios para articular y potenciar los anteriores, que usualmente se consideran en forma implícita, o "no consciente", y tienen que ver con la estrategia, cultura, valores y liderazgo de la organización.





Por su parte las principales características de la resiliencia corporativa son:

- **Adaptación:** se refiere a la capacidad de organizarse para responder a un cambio, esperado o no, y gestionarlo como una oportunidad, creando diversidad, bajo un perfil de riesgo controlado. Esto requiere poder estar atento al entorno e identificar estos potenciales cambios y comprender que implican oportunamente.
- **Confianza:** se refiere a la capacidad de monetizar relaciones satisfactorias con los interesados y definir cómo se debe invertir en éstas.
- **Agilidad:** implica la capacidad de tomar e implementar las decisiones necesarias a la velocidad necesaria, brindando la oportunidad de actuar más rápido que la competencia.
- **Relevancia:** se refiere a "ser relevantes" para sus clientes y tiene que ver con la capacidad de brindar el servicio que realmente satisfaga las necesidades de éstos, para lo cual, además de perseguir la calidad del servicio se debe lograr mantener la flexibilidad.
- **Coherencia:** se refiere a la capacidad de tomar decisiones, en forma articulada pero alineada, asegurando el mayor beneficio a nivel corporativo. Poder actuar como células capaces de gestionar y decidir en forma individual pero coordinada, permite ser más ágil y refuerza el relacionamiento entre las diferentes áreas de la organización.
- **Confiabilidad:** ser confiables para los clientes tiene que ver con la capacidad de brindar los servicios en forma consistente de acuerdo a lo especificado en relación a la calidad y oportunidad

En la medida que las organizaciones mejoren su resiliencia, estarán mucho mejor preparadas para trabajar bajo estrés en entornos cada vez más dinámicos; y seguramente no habrá que esperar una próxima pandemia para ponerlo a prueba. Las organizaciones que logren aprovechar lo disruptivo como una oportunidad, tendrán una ventaja significativa sobre las restantes.

Muchas veces el problema es que si bien los Ejecutivos poseen un enfoque estratégico del tema, los mandos medios y operativos lo siguen visualizando como un problema de continuidad del negocio, por lo que no generan la información de gestión que requiere la Alta Gerencia.

¿Y después qué?

Una frase que se repite mucho en este momento es “cuando se vuelva a la normalidad”. Pero la mayoría de los especialistas coinciden en que no vamos a volver a la misma “normalidad” de antes de la pandemia; y que la “nueva normalidad” se va a ir logrando de a poco, no de un día para otro.

Para bien o para mal esta “economía confinada” que ha surgido ha cambiado a las personas y organizaciones, las que seguramente incorporarán las herramientas y nuevas prácticas de negocio que han sido exitosas.

En su afán de sobrevivir muchas organizaciones han logrado adaptaciones muy interesantes movidas por la necesidad, que probablemente no van a abandonar. Por mencionar algunos ejemplos: las tiendas y mercados que por necesidad debieron transformarse “digitalizando” su función de ventas, y que de hecho a muchas les está yendo muy bien, no van a volver a su antiguo modelo de negocio. Los restaurantes que no contaban con servicio de delivery y que hoy éste se ha transformado en prácticamente su única forma de trabajo, tampoco volverán a su viejo modelo de negocio; es más, algunos quizás adopten la modalidad “dark kitchen” y pasen a trabajar solamente para delivery, cerrando sus salones. Muchas empresas profesionales, con altos costos de infraestructura edilicia y mantenimiento, se pueden ver tentadas de adoptar en forma permanente, aunque sea de manera parcial, la modalidad “Home Office”. Asimismo, en lo que refiere a las habilidades y conocimientos esperados del personal, la capacidad de poder trabajar en forma remota con buenos niveles de desempeño, así como lograr un relacionamiento efectivo bajo esta modalidad, será muy valorado. Algunos autores están llamando a estos cambios el “Darwinismo Profesional”



Aprendizajes de la situación actual

Indudablemente son muchos los aspectos a mejorar que están quedando en evidencia a raíz de esta pandemia. Ahora bien, si nos enfocamos estrictamente en lo que a la sustentabilidad de las organizaciones se refiere, nos podríamos enfocar en 3 puntos:

- **Trabajar en continuidad del negocio es obligatorio, no opcional.** Más allá de que las estrategias definidas se adecuen completamente a todas las situaciones, siempre posicionarán mejor a la organización de cara a su recuperación. En tal sentido vale la pena hacer las siguientes reflexiones:
 - Dada la relevancia del tema y la realidad de que no es una tarea sencilla, no es una buena idea improvisar. Es indispensable que se apliquen enfoques metodológicos maduros por parte de profesionales con experiencia, para lograr soluciones de continuidad del negocio de calidad.
 - Trabajar en este tema sólo por razones de cumplimiento no tiene sentido; el esfuerzo es prácticamente el mismo y los resultados muchísimo más pobres.
 - Muchas veces cuando se trabaja en la planificación de la continuidad de las operaciones se hace foco en la respuesta, lo cual es correcto ya que es lo fundamental. No obstante, puede resultar de interés evaluar en qué situación se encuentra la organización para trabajar, desde Continuidad del Negocio, en prevención. En tal sentido es importante analizar el nivel de madurez de la práctica de gestión de riesgos operativos y de IT de la organización.



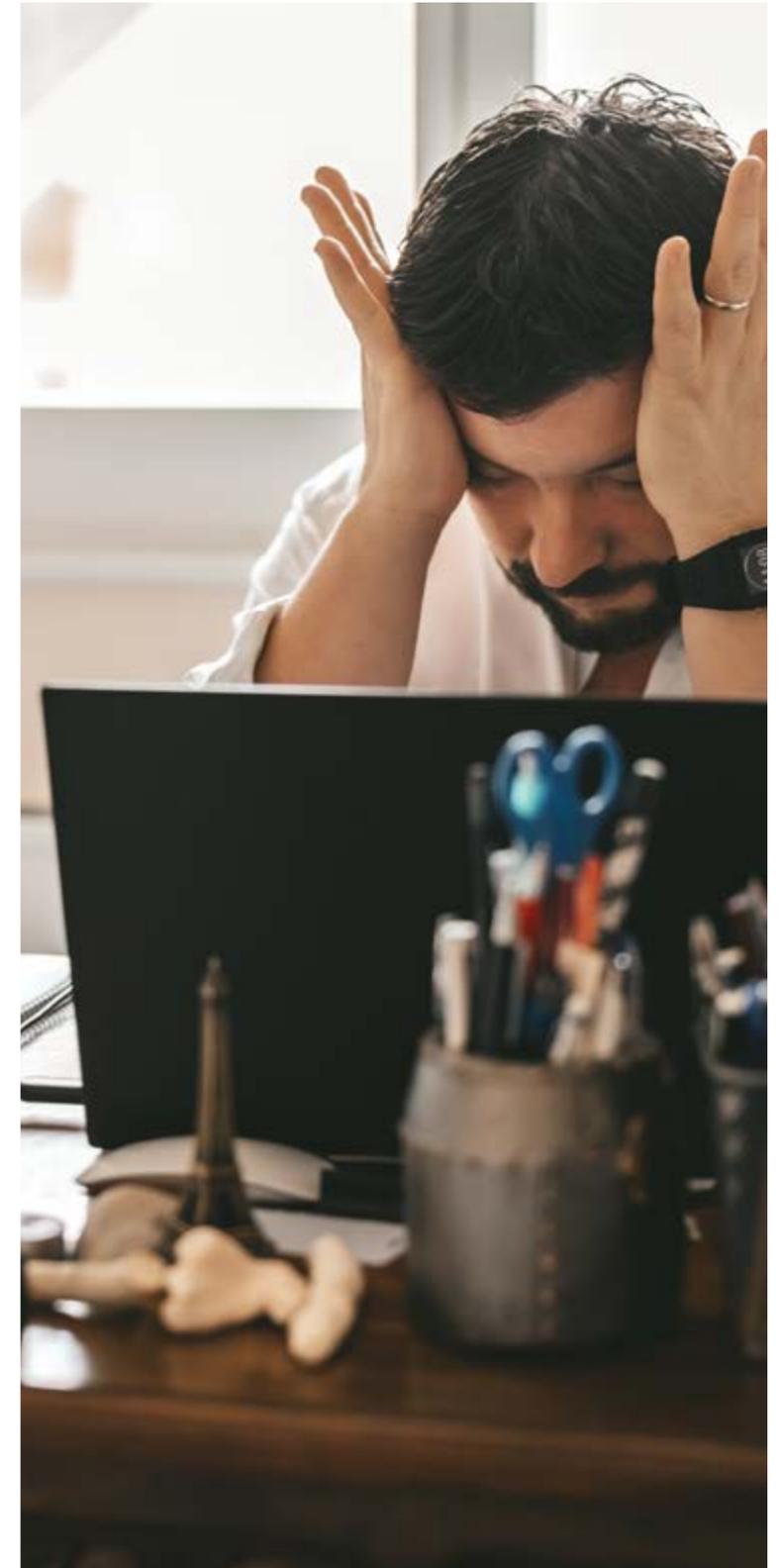
- **Convertirse en organizaciones resilientes.** Si pensamos “en el día después de la vuelta a la normalidad” o incluso en el período de operación en régimen de contingencia en el caso de escenarios masivos, como el que nos aqueja, vemos que haber recuperado la operativa crítica de la organización no siempre garantiza la sustentabilidad futura del negocio. Es importante que la organización sea resiliente, como un paso adicional a la planificación de la continuidad del negocio, para poder asegurar su prosperidad.
- **Evaluar desarrollar un Plan de Respuesta a Pandemias** por lo sensible del tema, ya que afecta directamente a las personas y la sociedad en su conjunto; lo que repercute en las organizaciones y el impacto en estas vuelve a afectar a las personas, ahora desde el punto de vista económico.

Sugerencias

Independientemente de cómo estén operando hoy las organizaciones, a continuación se listan una serie de aspectos que se sugiere atender ya que pueden permitirnos capitalizar beneficiosos en este momento o de futuro.

A implementar a la brevedad:

- Realizar seguimiento a la situación del personal. El cansancio/estrés acumulado, tanto por trabajar en condiciones diferentes a las habituales por tanto tiempo, así como por la incertidumbre general o la situación personal que atraviesen, los puede estar afectando. La cuarentena puede provocar un desgaste emocional en las personas, que puede afectarles en distinta medida, en distintos momentos; y es deseable que la organización esté atenta para brindar su apoyo.
- Evaluar periódicamente la suficiencia y adecuación de los recursos tecnológicos. En muchos casos éstos son la base de las operaciones, por lo tanto es vital anticipar cualquier problema que se pueda registrar con ellos.
- Revisar si tareas que no fueron consideradas críticas en los BIAs y por ende no se recuperaron, comienzan a acumularse pudiendo generar un impacto negativo mayor al estimado.
- Realizar un seguimiento a la situación de los Proveedores ya que pueden comenzar a tener problemas y afectar la cadena de abastecimiento.
- Realizar un seguimiento de la situación general de la Infraestructura país y servicios básicos por si comienzan a fallar.





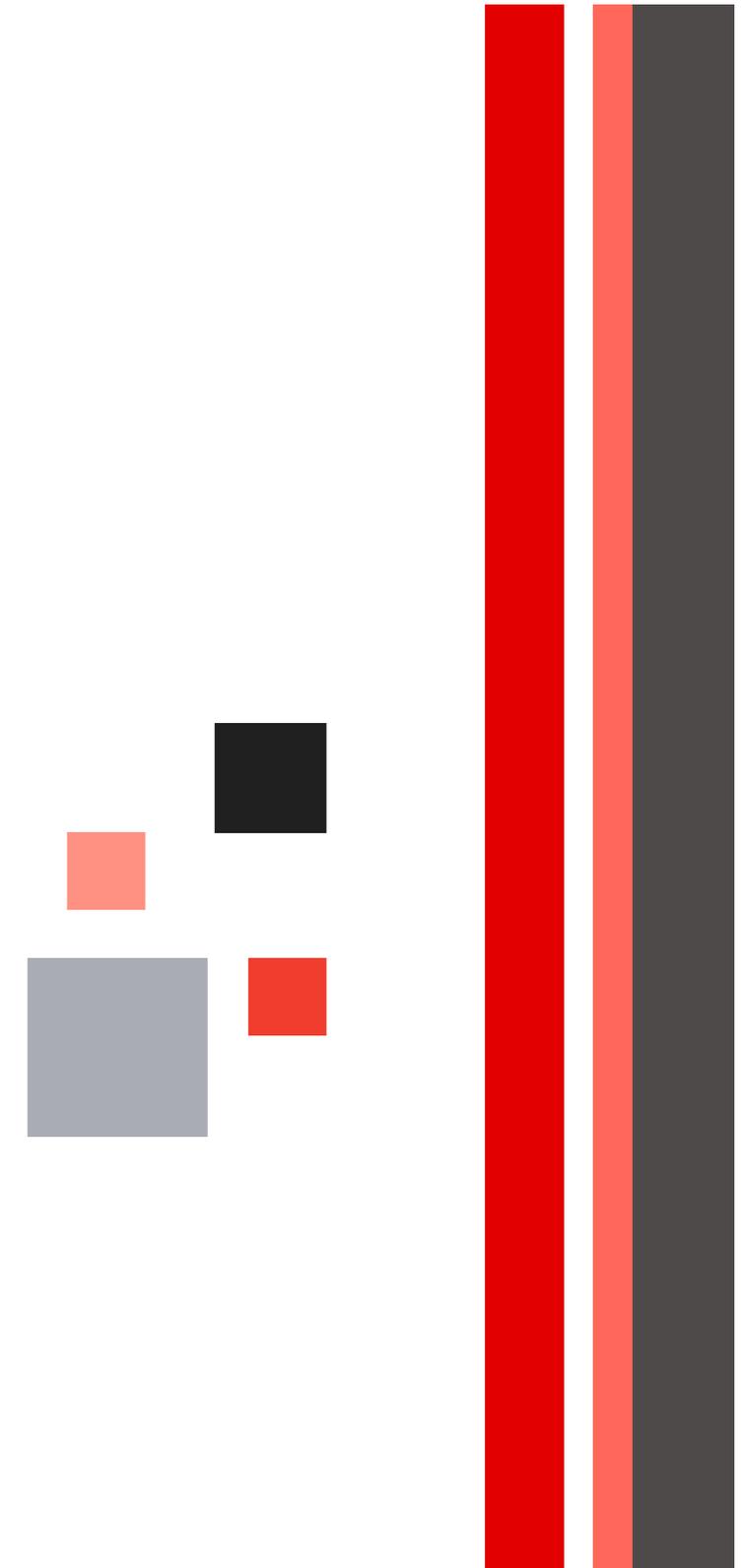
- Tener presente que probablemente cambien las prioridades de la organización, lo que puede llevar a tener que “repensar” muchas cosas. En este sentido es importante nunca perder de vista los valores de la organización, pese a la presión que se esté soportando, incluso financiera.
- Asegurarnos el Cumplimiento de las normas, políticas y procedimientos que corresponda. Se debe considerar además la capacidad de adaptarse a las nuevas medidas que defina el Gobierno en el marco de la pandemia.
- Tratar de estimar las pérdidas financieras que pueden ser mayores de lo esperado.
- Evaluar opciones de reducción de costos. Revisar leyes y regulaciones referentes a temas económicos y financieros con el objetivo de poder aprovechar beneficios y prórrogas; y revisar contratos también buscando oportunidades de reducción de costos
- Adecuar la producción a la demanda real
- Segmentar/focalizar clientes targets y tratar de conocer sus nuevas necesidades
- Concientizar al personal en temas vinculados a la seguridad de la información
- Reforzar el soporte remoto (Servicios de Mesa de Ayuda, internos o para clientes dependiendo del sector)
- Incrementar los niveles de monitoreo de Seguridad
- Recordar al personal las medidas de seguridad de la información, en particular aquellos aspectos vinculados a privacidad, confidencialidad y ciberseguridad.

A implementar en un corto o mediano plazo:

- Incorporar el concepto de resiliencia corporativa. Por todo lo antes mencionado queda claro que trabajar solamente en continuidad del negocio no basta. Se debe contar con la capacidad de garantizar la sustentabilidad del negocio a largo plazo, por lo que se sugiere comenzar a trabajar en la mejora e integración de las prácticas de soporte de la resiliencia corporativa y en el desarrollo de sus principales características.

Pasos sugeridos:

- Identificar/evaluar si se está realizando una inversión directa en fomentar estas características. Probablemente se pueda obtener información respecto al costo de implementar la política de Seguros de la organización, pero ¿se conoce cuánto se invierten en construir confianza, mejorar la imagen o su relevancia?
 - Evaluar la calidad de las prácticas de soporte a la resiliencia
 - Evaluar la situación de la organización respecto de las características de la resiliencia (estado del "sistema inmunológico" de la organización)
 - Analizar esta información con la Alta Gerencia y obtener su apoyo para elaborar la estrategia de Resiliencia Corporativa
 - Comunicarla a los mandos medios haciendo énfasis en diferenciarla de la estrategia de continuidad del negocio pero mostrando su sinergia
- En relación a la Planificación de la continuidad del negocio:
 - Revisar/mejorar la calidad de los BIAs en base a la experiencia; sobre todo en lo que se refiere a la identificación de los recursos críticos que se requieren para llevar adelante cada proceso crítico.





- Revisar las estrategias de administración de la crisis. Si bien en general éstas se adecuaron a la situación actual, se han mencionado algunos aspectos que pueden significar oportunidades de mejora.
- Asegurarse que los planes que guían la recuperación de los procesos del negocio se han definido teniendo en cuenta la disponibilidad o no de los recursos críticos; no son estrategias de respuesta ante un incidente en particular. Esto es fundamental para asegurar que los planes son lo suficientemente flexibles como para adaptarse a todas las situaciones, con la menor cantidad de ajustes posible.
- Revisar que los equipos de respuesta estén integrados por personas con un claro conocimiento del negocio
- Validar que la estructura de gobierno de los equipos de respuesta que forman parte de la Solución de Continuidad esté completamente alineada a las características de la organización, de forma de promover un buen relacionamiento en todos los niveles.
- Lograr el involucramiento y apoyo de Alta Gerencia a través de la Política de Continuidad del Negocio y lograr una visión compartida del tema por parte de toda la organización.
- Verificar que los Planes brinden la capacidad de tomar conciencia de las situaciones que se van viviendo a partir reglas básicas de evaluación
- Definir y ejecutar los procedimientos de prueba de todo lo que se planifique, como forma de asegurar la efectividad de la respuesta futura.
- Desarrollar un Plan de Respuesta a Pandemias, alineado e integrado al Plan de Continuidad del Negocio.

ENCUESTA: Evaluación del nivel de madurez en continuidad del negocio y resiliencia corporativa

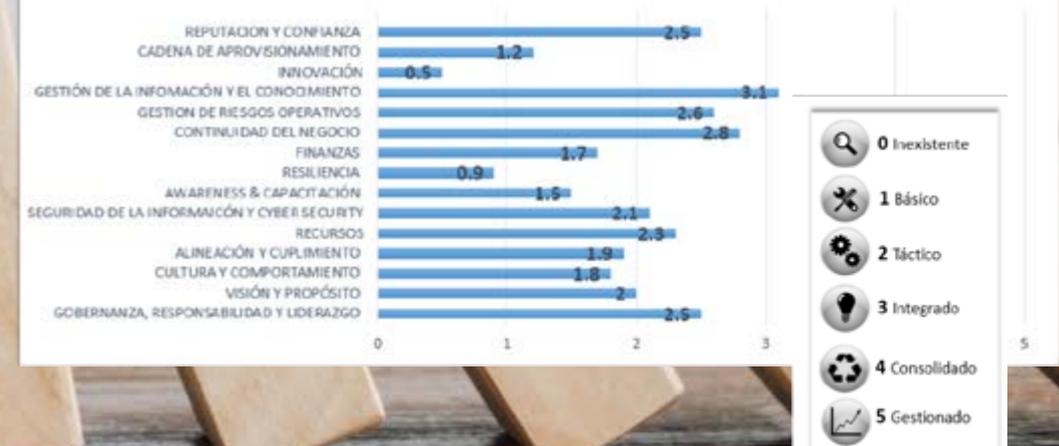
Como parte de las herramientas con que contamos para asistir a nuestros clientes en la mejora de sus prácticas de Continuidad del Negocio y Resiliencia Corporativa, en Quanam hemos desarrollado Modelos de Madurez que nos permiten identificar sus fortalezas y debilidades en relación a estos temas.

Y dado lo importante que es hoy para las organizaciones mejorar estas capacidades, estamos ofreciendo una versión "on-line" reducida de este estudio sin costo.

Para esto los invitamos a acceder a una encuesta, cuyos resultados procesaremos para usted.

La información registrada será utilizada bajo estricta confidencialidad, con la única finalidad de completar este estudio.

**Acceder a la encuesta
y recibir los resultados**



Fuentes

Horizon Scan Report 2020, Business Continuity Institute

Horizon Scan Report, 2019, Business Continuity Institute



Una empresa de conocimiento
e innovación