LA VELOCIDAD DEL RIESGO, EL COVID 19 Y LA HOJA DE RUTA PARA EL RETORNO

AUTOR: Armando Villacorta Cavero – Director de Consultoría DFK (avillacortac@dfkperu.com.pe)

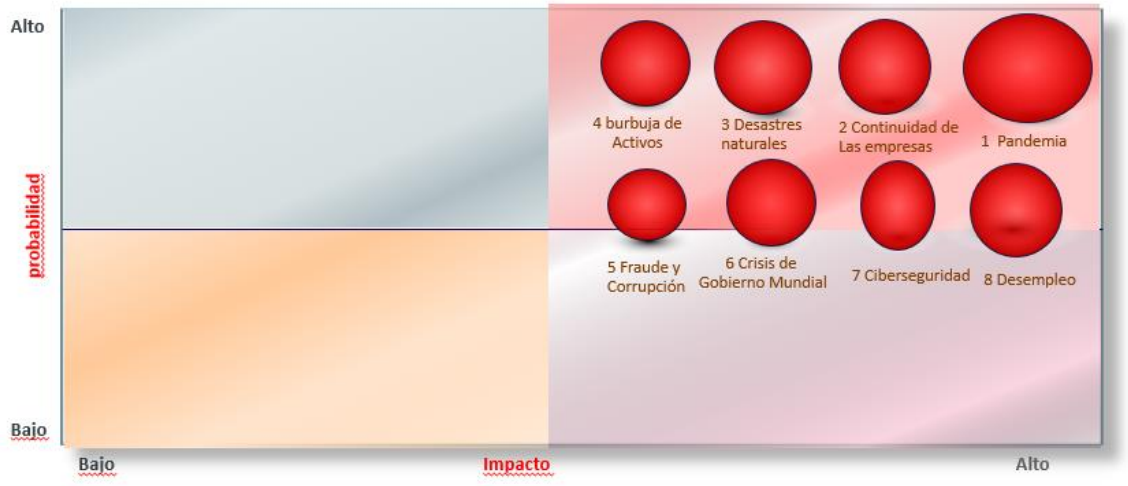
El Mundo es indiscutiblemente más cambiante e impredecible hoy, de lo que era hace un mes. La tecnología asegura que la mayoría de nosotros estamos continuamente "conectados" a este nuevo entorno. El negocio y su ambiente regulador se enfrentan a un panorama complejo y acelerado con emergentes disruptivos ambientales nunca vistos: el virus COVID 19.

En este entorno, la velocidad con que se presentan los hechos, La capacidad de gestionar el riesgo y la incertidumbre son variables esenciales. Pero el riesgo rara vez es estático, y la velocidad a la que un riesgo puede afectar a una organización ahora se considera como otro elemento vital para medir y responder a los riesgos (la tradicional medición binaria de probabilidad e impacto ya no es suficiente).

En la evaluación que se realiza según la Organización COSO (USA), debemos considerar que tienen mayor importancia los riesgos con mayor velocidad, es decir aquellos en los cuales el impacto afecta más rápidamente a la entidad. Para representar gráficamente esta evaluación, debemos recurrir a un mapa de riesgos que considere esta tercera variable, que la expresaremos en función al tamaño que el circulo que representa la coordenada (probabilidad, impacto) en una matriz tradicional.

A Continuación, empezaremos haciendo una propuesta de riesgos críticos, que de acuerdo a los expertos hoy vulneran en una primera línea a las organizaciones.

FIGURA No 1 – Mapa de Riesgos Críticos COVID 19



Fuente: Propia

La velocidad está representada en el tamaño del círculo, el círculo más grande representa el riesgo de mayor velocidad, es decir, el riesgo que tarda menos días en afectar la entidad. El riesgo de menor velocidad, su tamaño es más pequeño y por consiguiente se tarda más tiempo en afectar la entidad.

Esta "tercera dimensión del riesgo" es una idea cuyo momento ha llegado, y las empresas necesitan reconocerla, entenderla y tratarla como parte de sus procedimientos operativos estándar (CPA Journal, Managing Risk at the Speed of Change, A New Risk Vocabulary and a Call to the Profession, June 2017).

Como podemos apreciar en la matriz de la figura No 1, los riesgos externos (pandemia, discontinuidad del negocio y desempleo), a la empresa se consideran los más extremos y de mayor velocidad, quedando en un segundo lugar, los riesgos de ciberseguridad, fraude y corrupción, fallas de gobernabilidad y burbuja de activos).

El reto de los gestores es intentar gerenciar estos riesgos en lo que resta del año 2020 y el 2021, para lo cual, proponemos en este artículo una lista de temas y referencias que pueden ser de utilidad para vuestras organizaciones.

TRABAJANDO UNA HOJA DE RUTA PARA APRENDER A ENFRENTAR UN AMBIENTE DE PANDEMIA

Hoy la pandemia, de acuerdo a un esquema desarrollado por el IIA Argentina, nos ha ubicado en tres etapas muy críticas: **(i) la etapa de miedo:** acumular alimentos, contagiarme del miedo por las estadísticas, estado irritable, impotencia, luego evolucionamos a: **(ii) etapa de aprendizaje:** toma de conciencia de lo que está pasando y comenzamos a pensar cómo actuar, comienzo a recolectar información y a contrastar y reconozco que todos estamos tratando de hacer lo mejor dentro de las limitaciones que vivimos; y finalmente llegamos a **(iii) etapa de crecimiento**: vivo el presente y me enfoco en el futuro, pongo mi talento en función a los intereses de la sociedad y de los míos, y empiezo a adaptarme a los nuevos cambios y el entorno.

En este orden de ideas, por donde debo empezar al revisar la empresa y sus intereses dentro de la pandemia de COVID-19, que tiene todos los ingredientes para hacer perder el equilibrio a un gran número organizaciones. Es posible, que numerosas organizaciones, en particular pequeñas empresas, nunca se recuperen. Muchas organizaciones pueden encontrarse rápidamente en una situación realmente grave, y el resultado podría ser que muchos empleados pierdan el trabajo y que la comunidad sufra interrupciones de servicios y racionamiento de productos.

ACCIONES Y PRIORIDADES DE REFLEXION

	Referencias	*Herramientas y/o acciones*
1. GESTION DE CRISIS FINANCIERA	Cuando se desata una crisis, el Instituto Internacional de Auditores-IIA de Australia recomienda que las organizaciones evalúen la necesidad de tener acceso a efectivo suficiente para sobrevivir mientras dure la pandemia ¿Cuánto tiempo puede hacer frente la organización al pago de los sueldos de empleados, alquileres, arrendamientos y otras obligaciones regulares? ¿Qué medidas deben adoptarse para "asegurar" su liquidez? ¿En qué etapa se debe informar al regulador, la institución financiera, los proveedores y otras partes interesadas si la empresa empieza a caminar por la cuerda floja?	En esta parte: flujos de caja, estados financieros, revisión de ayudas financieras, laborales y tributarias del gobierno, identificación de personal clave, diseño de escenarios financieros, etc. Los ayudaran a tener una primera visión de lo que tiene, y lo que necesita financieramente su empresa.

	Referencias	*Herramientas y/o acciones*
2. GESTION DE TELETRABAJO Y TECNOLOGIA	La NIST en su documento SP 800-46 nos introduce al teletrabajo y la seguridad de la siguiente forma: Para muchas organizaciones hoy en un entorno complejo, sus empleados, contratistas, socios comerciales, clientes, proveedores y / u otros usuarios podrían utilizar tecnologías de teletrabajo empresariales para realizar trabajos desde ubicaciones externas. La naturaleza del teletrabajo y las tecnologías de acceso remoto, que permiten el acceso a recursos protegidos desde redes externas y, a menudo, también desde hosts controlados externamente, generalmente los pone en mayor riesgo que las tecnologías similares a las que solo se accede desde dentro de la organización, Planifique las políticas y controles de seguridad relacionados con el teletrabajo basándose en el supuesto de que los entornos externos contienen amenazas hostiles. Los objetivos de seguridad más comunes para el teletrabajo y las tecnologías de acceso remoto son los siguientes: (i) Confidencialidad: garantizar que las comunicaciones de acceso remoto y los datos de usuario almacenados no puedan ser leídos por terceros no autorizados; (ii) Integridad: detecta cualquier cambio intencional o no intencional en las comunicaciones de acceso remoto que se producen en tránsito; y (iii) Disponibilidad: asegúrese de que los usuarios puedan acceder a los recursos a través del acceso remoto cuando sea necesario. Para respaldar la confidencialidad, integridad y disponibilidad, todos los componentes del teletrabajo y las soluciones de acceso remoto, incluidos los dispositivos cliente, los servidores de acceso remoto y los servidores internos a los que se accede mediante acceso remoto, deben protegerse contra una variedad de amenazas. Al planificar las políticas y controles de seguridad del teletrabajo, las organizaciones deben asumir que las partes malintencionadas intentarán acceder a datos confidenciales de los dispositivos o aprovechar los dispositivos para obtener acceso a la red empresarial. Las organizaciones deben asumir que los dispositivos del cliente se infectarán con “Malware” y planificar sus controles de seguridad en consecuencia. (Las organizaciones deben considerar cuidadosamente el equilibrio entre los beneficios de proporcionar acceso remoto a recursos adicionales y el impacto potencial de un compromiso de esos recursos. Las organizaciones deben asegurarse de que los recursos internos que elijan poner a disposición a través del acceso remoto se refuercen adecuadamente contra las amenazas externas y que el acceso a los recursos se limite al mínimo necesario a través de firewall y otros mecanismos de control de acceso.	Debemos revisar los contratos con proveedores de servicios y equipos de tecnología, el equipo de tecnología que nos apoya y/o asesora, los ambientes de trabajo y la seguridad en los sitios remotos habilitados, el nivel de seguridad de los proveedores, clientes u otros, incluidos en nuestra red remota.

	Referencias	Herramientas y/o acciones
3. GESTION DE CONTINUIDAD DEL NEGOCIO	Un plan de gestión de crisis o un plan de continuidad del negocio requiere personas y el trabajo activo en general suele desbordar a todos. Los departamentos de actividades no esenciales de un negocio pueden prestar a su personal para cubrir necesidades o colaborar con los esfuerzos de remediación y recuperación, y subsistir en esta etapa. En esta parte se debe: (i) categorizar las actividades en esenciales y no esenciales, (ii) redefinir los objetivos del negocio en una perspectiva de corto plazo, (iii) identificar productos y/o servicios, personal, proveedores y clientes claves; (iv) analizar diferentes escenarios que permitan establecer un abanico de estrategias, (v) revisión de contratos, leyes y subsidios potenciales, y (vi) redefinir la estructura, documentación, políticas y procedimientos de la organización. Interrogantes que pueden ser útiles reflexionar pueden ser, por ejemplo: - Disponibilidad del personal (en cantidad de días): el % de personal que posiblemente podría trabajar según la eliminación paulatina de restricciones y los niveles de seguridad implementados (en días: 0, 3, 7, 14 o 30). - Porcentaje probable de operaciones y/o espacio de oficina que se encuentra en condiciones (durante los días del proceso de reincorporación a actividades). - Interrupciones de suministros, entre los que se incluyen materias primas y servicios esenciales; - Fallas de equipamiento de producción, como motores, calderas o cintas transportadoras; o Falta de disponibilidad de servicios públicos de asistencia, como plantas de tratamiento y equipos para eliminación; - Fallas de almacenamiento, transporte y distribución de productos; - Demoras gubernamentales de permisos, certificación de personal, o en aduana - Alcance geográfico de las restricciones operativas o la logística de apoyo - Pedidos que quedaron pendientes de atender o se encuentran en proceso de ser retomados, y nuevos requerimientos.	Se debe realizar de una manera sencilla, un plan de trabajo de corto plazo, revisión de la estructura de costos en una perspectiva de costos fijos y variables, revisión de precios, descuentos y promociones, personal, proveedores y clientes críticos, disposiciones del gobierno sobre la industria, alianzas con empresas de cobranzas en línea, canales de distribución, evaluación de venta por delivery. nuevos mercados, alternativas de financiamiento, en resumen, debemos hacer una reestructuración del negocio. Trabajar una documentación simple y clara, que se enmarque sobre las nuevas políticas y el diseño de nuevos procedimientos necesarios para reorganizar la empresa.

	Referencias	Herramientas y/o acciones
4. PLAN DE HIGIENE GENERAL Y EQUIPAMIENTO DE PROTECCION INDIVIDUAL	De manera general se debe cumplir con "Procedimiento de limpieza y desinfección de superficies y espacios para la prevención del Coronavirus" Los equipos de protección individual (EPI) son esenciales para el control del riesgo y deben utilizarse cuando los riesgos no se puedan evitar o no puedan limitarse suficientemente por medios técnicos de protección colectiva o mediante medidas, métodos o procedimientos de organización del trabajo. El personal laboral precisa: Mascarillas auto filtrantes, que contienen un filtro de micropartículas para proteger 'de fuera hacia dentro' en distintos grados. Su finalidad es proteger al usuario frente a la inhalación de contaminantes ambientales en partículas o aerosoles, como agentes patógenos, agentes químicos, antibióticos, citostáticos, etc., Guantes no estériles, Gafas o protector facial, entre otras ideas que deberán evaluarse para cuidar el bienestar común.	Se necesitará trabajar para obtener certificaciones de limpieza y desinfección, inversión en pruebas de medición de COVID 19 (opcional), certificaciones por médicos ocupacionales, compras de equipos de seguridad personal, redefinición del layout e la empresa,

	Referencias	Herramientas y/o acciones
5. RESPONSABILIDAD SOCIAL Y EL BIENESTAR COMUN	El análisis de costo-beneficio que muestran que el valor en soles de una vida salvada por el distanciamiento social es demasiado alto para sostener las restricciones existentes. Este enfoque puramente utilitario está lejos del ideal de solidaridad, que requiere que demostremos tanto cuidado y preocupación por aquellos que son débiles y vulnerables como por aquellos que son fuertes y poderosos. ¿por qué no considerar, como condición para enviar a los peruanos de regreso al trabajo, extender estas protecciones económicas y de salud a todos durante los próximos meses? Quizás este gesto de solidaridad del Estado demuestre la creación de hábitos, y valga la pena continuar incluso cuando el virus retroceda, y realmente sea un respaldo para el proceso de recuperación.	Se debe evaluar nuestro aporte como respaldo social a la comunidad a través de donaciones, cuidado de los puestos laborales, precios sociales para ciertos sectores entre las principales ideas, que junto a lo que haga el gobierno son un reto para todos en esta búsqueda de la estabilidad social.

	Referencias	Herramientas y/o acciones
6. DETERIORO DE LOS ACTIVOS (EFECTO BURBUJA), LOS FRAUDES Y LA CORRUPCION, YLA SEGURIDAD PERSONAL	La interrupción de las cadenas de valor mundiales y la creciente limitación de la vida social están pasando factura. El impacto sobre la economía es grave, por lo que en las próximas semanas los economistas y los analistas ajustarán sus estimaciones de la actividad económica y las previsiones de beneficios, en algunos casos de forma considerable. En vista de estos acontecimientos económicos, la probabilidad de recesión en la economía mundial también ha aumentado considerablemente, por lo que ahora forma parte de nuestro escenario básico: pérdida o ajuste de los activos. Asimismo, Ante la crisis sanitaria mundial debido al COVID-19, es de esperar que haya quien quiera aprovecharse y sacar un beneficio económico de todo esto. Los ciberdelincuentes no descansan y siempre encuentran nuevas formas de llevar a cabo sus estafas y fraudes online. Hoy a más de uno le echa humo el móvil con mensajes, noticias y cadenas sobre el coronavirus o COVID-19. El uso de las redes sociales también se ha disparado, generando y compartiendo contenido sin cesar, aunque no siempre es información verificada. Entre los fraudes a tener en cuenta se tiene: venta de material sanitario de baja calidad, llamadas de un supuesto “soporte técnico” del operador contratado para colaborar mientras duren estas semanas de teletrabajo, un malware llamado “Coronavirus”, que trae archivos adjuntos que contienen malware que terminen por infectarnos y tomar control de nuestros equipos. No hay que perder de vista los fraudes internos de falsas ventas, apropiación de cobranzas, falsos reportes, etc. Finalmente, hay que tener presente que en la medida que el bienestar común no sea suficiente, el incremento de la delincuencia puede aumentar (secuestros, asaltos, pandillaje, etc.	Evaluar el valor de nuestro patrimonio empresarial, establecer un plan de control antifraude, utilizar líneas de denuncia colaborativas, y finalmente trabajar un plan de protección personal, por si las cosas se desbordan y la delincuencia se incrementa.

Un proyecto de elaboración de planes, políticas y procedimientos para época de crisis implica trabajo en equipo y tiempo. A continuación, sugerimos opciones para el desarrollo de éstos:

- PRIMERA OPCIÓN. Que las personas de un mismo proceso o área trabajen todas en tiempo, día y hora definidos. Por ejemplo, el área de Ventas podría reunirse varias horas los miércoles en orden y por prioridades hasta que termine de elaborar todos los documentos que le corresponden.
- SEGUNDA OPCIÓN. Que todas las personas encargadas de los procesos trabajen todas las semanas en tiempo, día y hora definidos. Por ejemplo, todos los responsables de elaborar el plan de trabajo a corto plazo podrían reunirse varias horas durante 5 días para trabajar en orden y por prioridades hasta que terminen de elaborar un borrador.

Lo Importante, es que sea cual fuese su opción cuente con una metodología de trabajo o un equipo asesor externo que los apoye, si ustedes lo consideran oportuno.

CONCLUSIONES

1. Los profesionales a cargo de la implementación de planes de crisis en las empresas, ya sean externos o internos, deben pensar de manera amplia sobre cómo actualizar sus modelos de negocios y la evaluación de riesgos; e incluir la velocidad del riesgo (VoR), y los auditores deben idear métodos para evaluar si las organizaciones han diseñado e implementado estrategias de respuesta adecuadas, lo que les permite servir mejor a sus clientes y partes interesadas, en un entorno que cambia rápidamente. Hay temas complementarios como “la persistencia del riesgo”, que sería importante complementar al revisar el concepto de velocidad del riesgo.

2. Los temas de riesgos vinculados a desempleo, desastres naturales o crisis de gobierno no son parte de este artículo.

3. Los aspectos legales y normativos han ido evolucionando; y continuaran modificándose en este entorno, y sobre estas referencias hay interesantes reflexiones que se aconseja revisar con detenimiento.

REFERENCIAS

Committee of Sponsoring Organizations of the Treadway Commission (2013). Internal Control — Integrated Framework- Executive Summary. USA. PriceWaterHouseCoopers.

Rivero, Ariamna. (2006) "Análisis comparativo entre los informes Coso, Coco y la Resolución 297". En:*monografías.com.* 18 de julio del 2008. Fecha de consulta: 2 de Noviembre del 2013. http://www.monografias.com/trabajos59/analisis-informes-Coso-Coco/analisis-informes-Coso-Coco2.shtml

COSO. (2017). Enterprise Risk Management- Integrating with Strategy and Performance. Executive Summary. En línea, disponible en: https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

Global Risk Management Survey: Fifth Edition – Accelerating Risk Management Practices, Deloitte, 2007, http://bit.ly/2q9Fge7; Stephen Davis and Jon Lukomnik, "Risk Velocity, the Unknown Dimension in ERM," ComplianceWeek, Dec. 8, 2009, http://bit.ly/2qaF0Lq).

Harry Hall on the PM South blog ("How to Evaluate Risk Velocity," Apr. 25, 2014, http://bit.ly/2qjRlcX),

Karel Simpson, "Risk Velocity", Capable People, 31 de marzo de 2015, http://bit.ly/2pG3qsx)

CPA Journal, Managing Risk at the Speed of Change, A New Risk Vocabulary and a Call to the Profession(2017), Sridhar Ramamoorti, Barry Epstein, Dorsey L. Baskin, CPA and James Wanserski.

The Global Risks Report 2019, Edition 14th, Word Economic Forum, https://www.weforum.org/reports/the-global-risks-report-2019

Hoja Informativa: Auditoría interna y Pandemia (2020). The Institute of Internal Auditors, Australia.

NIST Special Publication 800-46 Revision 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security (2016), USA.