RESILIENCIA EMPRESARIAL: ANTES, DURANTE Y DESPUÉS DEL COVID-19

Perspectiva actual. Planes de Continuidad de Negocio y Planes de Gestión de Crisis.
El COVID_19 ha puesto en evidencia el grado de madurez de la **Resiliencia de las Organizaciones** Empresariales ligado al tiempo máximo tolerable de caída de un proceso / actividad antes de que se produzcan efectos desastrosos en la compañía y repercuta en el negocio (*Maximum Tolerable Period of Disruption or MTPD)*. Las consecuencias del COVID-19 han supuesto que productos / servicios / datos se encuentren en un mínimo histórico, y las características de recuperación que antes se consideraban "deseables" ahora son obligatorias.

El impacto del COVID-19 nos ha enseñado , que las distintas Unidades de Negocio / departamentos tenían interiorizados y automatizados mecanismos verticales / jerarquizados de contingencia técnico- operativos específicos de respuesta respecto a la afectación en las áreas de producción, sin embargo lo que no estaba al mismo nivel de desarrollo era la configuración de comités de gestión y procedimientos de respuesta interdisciplinares en los que estuviesen integrados / implicados de manera colaborativa representantes de otros servicios corporativos o transversales de soporte a los procesos de negocio, tales como los servicios médicos, prevención de riesgos laborales, servicios jurídicos, relaciones institucionales, áreas de riesgos empresariales operacionales y seguros corporativos, etc.

Otro de los gaps observados fue que en los planes de contingencia implantados era más bien escaso o superfluo el análisis del impacto que podría producir una situación crítica, desde el punto de vista de su "real/auténtico C-Suite" que es su capital humano (empleados, contratistas, proveedores, sociedad en general), siendo básicamente la única referencia de amenaza e impactos previstos al respecto, la relativa a la cobertura de los servicios mínimos.

Lo anterior, provocó inicialmente un retraso significativo en la configuración de equipos de expertos, toma de decisiones y homogeneización de las respuestas, así como la identificación de canales oficiales de divulgación de las mismas ante COVID-19. Además, el calibre de los escenarios disruptivos hizo saltar por los aires los tradicionales cálculos de probabilidades de ocurrencia de los análisis de los riesgos, grado de exposición a los mismos y consecuencias de su manifestación.

Los hechos han demostrado que de la misma forma que un plan de continuidad tecnológica no es lo mismo que un plan de continuidad de negocios y este no es lo mismo que un plan de gestión de crisis, tampoco son lo mismo un equipo de respuesta ante una contingencia técnica – operativa específica, que un equipo de respuesta ante una interrupción o perturbación severa de uno o varios procesos de negocio, que un equipo de respuesta ante sucesos o situaciones que ponen en peligro de supervivencia a la empresa con motivo de una afectación crítica o catastrófica sobre activos tangibles o intangibles de la misma y no necesariamente dicha afectación tiene que venir derivada de una escalada del impacto o consecuencia de un Continuidad de Negocio *(BCP_ Business Continuity Plan). Así pues:*

- Un error muy común en muchas Organizaciones, puesto de manifiesto ante la amplitud y magnitud del COVID_19, fue sin duda creer que la tenencia de **un Plan de Contingencia en Tecnología de la Información (PCTI) o un Plan de Continuidad Tecnológica (PCT)** es asimilable a la disponibilidad de un Plan de Continuidad de Negocios (PCN). La Continuidad de Negocios va mucho más allá que la Contingencia / Continuidad Tecnológica en cuanto a objetivos, alcances y técnicas.
- Primero hay que comprender que el objetivo principal de la planificación de la continuidad de los negocios en una Organización, tras un evento que la interrumpe, es precisamente -y valga la redundancia- reanudar los negocios. La finalidad de las acciones de continuidad no es la restauración de los procesos de TI; es volver a hacer negocios. Más aún, la continuidad de negocios asume que los procesos TI son recuperables. La restauración tecnológica es necesaria, pero no suficiente para garantizar la continuidad.

- En el diseño de un **Plan de Continuidad de Negocio (PCN),** a diferencia de lo que sucede con el PCTI o PCT, intervienen activamente todos los órganos y funciones de una institución, desde el gobierno corporativo hasta las áreas de seguridad y atención al público, pasando por las funciones de RRHH, legal, finanzas, comunicación, servicios generales, operaciones, etc. El diseño de un PCN es integral, solidario y realizado bajo una unidad de concepción y unidad de mando ante un evento interruptor. Es decir, establece la continuidad de una organización desde múltiples perspectivas: infraestructura TIC, recursos humanos, inmuebles, sistemas de comunicación, logística, sistemas industriales, etc. Cada uno de estos ámbitos tendrá a su vez un plan de contingencia / respuesta más específica, ya que no es lo mismo la inundación de un almacén de logística que el corte del suministro eléctrico en una sala de servidores.
- Otro error observado durante el COVID-19 en las Organizaciones fue no tener un **Plan de Gestión de Crisis (PGC)** , con diseño propio y diferenciado del PCN y PCT, dado que su objetivo es evitar que tomemos decisiones improvisadas que puedan empeorar la crisis, entendiendo esta como una situación con un alto nivel de incertidumbre que afecta las actividades básicas y/o la credibilidad de la organización y requiere medidas urgentes o, de otra manera, condición inestable que implica un cambio abrupto o significativo que impide la atención y la acción urgentes para proteger la vida, los bienes, la propiedad o el medio ambiente (ISO 22300).
- Quizá uno de los aspectos más distintivos de los PGC es la constitución, preparación y concienciación de los **Comités de Gestión de Crisis (CGC)** compuesto de antemano por personas con autoridad suficiente para, en última instancia, tomar las decisiones pertinentes y desplegar los recursos necesarios (humanos, económicos, materiales y tecnológicos) para gestionar una crisis o, de otra manera, grupo de personas funcionalmente responsables de dirigir el desarrollo y la ejecución de la respuesta y los planes de continuidad del negocio (en este caso tendremos en cuenta especialmente los MTDs y RTO de los procesos críticos), declarar una interrupción operativa o una situación de emergencia/crisis, y proporcionar orientación durante el proceso de recuperación, tanto antes como después de un incidente disruptivo.

Una vez más, otra de las lecciones aprendidas durante el COVID-19, es que **un Plan de Comunicación** ante situaciones de crisis de cualquier entidad, pública o privada, no puede ser un elemento aislado y no interrelacionado con todos y cada uno de los planes de: continuidad tecnológica, continuidad de negocio o gestión de crisis y todos ellos deben compartir los mismos:

- Criterios de Calificación y medios para la declaración de la situación de crisis
- Condiciones de disparo. Es decir, qué situación límite debe darse para que declaremos una situación de crisis.
- Flujos de toma de decisiones.
- Planes Operativos y personal responsable de su activación

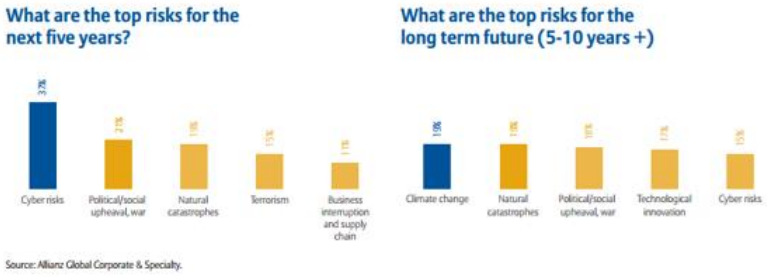
Como conclusión final del **Grado de Madurez de la Resiliencia actual en las Organizaciones**, podemos tomar como muestra los datos que arroja la encuesta llevado a cabo por la OSAC *(Overseas Security Advisory Council – USA Diplomatic Security*) durante los meses de abril/mayo-2020 en medianas y grandes compañías de los cinco continentes, respecto a su Retorno a la Actividad:

- 57 % Están actualmente desarrollando guías de retorno a la actividad
- 28 % Están actualmente ajustando / adecuando los PCN establecidos
- 10 % Están aplicando sus PCN establecidos
- 4 % No tienen Plan de Regreso a la Actividad

Principales riesgos para un futuro próximo

La última encuesta llevada a cabo por el "Allianz Risk Barometer_2020". Dirigida a más de 500 expertos del sector de seguros y a grandes empresas industriales de más de 40 países, destaca que las empresas actuales se enfrentan a nuevos retos derivados de un incremento de los escenarios disruptivos o perturbadores en un entorno empresarial cada vez más interconectado.

En particular, el cambio climático & desastres naturales, el riesgo de interrupción del negocio y los ciber incidentes son desafíos importantes que las empresas deben observar de cerca en la nueva década.



- Respecto al riesgo de **Cambio climático** las empresas están más preocupadas por las pérdidas físicas causadas por fenómenos meteorológicos extremos, pero también temen las críticas de los consumidores y el aumento de las acciones legales y regulatorias. Los análisis de riesgos en esta materia deben ser avalados por personal cualificado, los documentos de los planes / procedimientos operativos deben abarcar y contener información específica de respuesta ante la contingencia sobre todos los entornos que pueden verse afectados (personas sin posibilidad de traslado a sus centros de trabajo, infraestructuras inutilizadas o sin posibilidad de acceso, operaciones interrumpidas por incendios/inundaciones, sistemas inoperativos por fallo de suministro eléctrico, cadena de suministros por desabastecimiento, etc.) y los recursos disponibles o previstos de manera anticipada. A título de ejemplo hemos podido comprobar durante el año 2019/2020 como terremotos en Chile, ciclones en India, Tormentas/inundaciones en España, Incendios en USA, han provocado la evacuación de miles personas, han ocasionado grandes colapsos de infraestructuras / servicios y ante tales contingencias es el momento de actuar y no de planificar, es el momento de saber dónde acudir y a quién recurrir y de que recursos disponer y no empezar a analizar ¿para qué, cuándo, cómo, cuanto… debe ser la ayuda?

- Respecto a la **Interrupción del negocio** ocupa el segundo lugar, pero sigue siendo un desafío clave con la transformación digital y los disturbios civiles que crean nuevas causas de interrupción y pérdida de ingresos, principalmente derivados de:
    - Riesgos operacionales (personas): fraudes internos, perfiles inadecuados de empleados, pérdida de personal clave, etc.
    - Riesgos operacionales (procesos): fallos en los procesos, incumplimiento de normas o políticas, errores de ejecución, etc.
    - Riesgos operacionales (sistemas): fallos en comunicaciones, fallos en el software o hardware, interrupción de suministro, etc.
    - Riesgos operacionales (externos): fraudes externos, outsourcing, acciones regulatorias, riesgos geopolíticos, actos antisociales, etc.

  Los riesgos operacionales impactan en los resultados, la reputación y el negocio, por ello el personal que lleve a cabo, los Análisis de Impacto en el Negocio (BIAs), las estrategias de continuidad y recuperación, y los planes de actuación y contingencia para la gestión de las crisis y la comunicación, debe ser competente y con un gran nivel de conocimiento y experiencia sobre los procesos y activos críticos de la compañía.

Respecto a los **ciber incidentes**, de acuerdo con International Data Corporation (IDC), la pandemia está causando una importante repercusión en las industrias, y está empezando a reorganizar las inversiones en TI, ejerciendo presión sobre el gasto en algunas áreas y aumentando la demanda en otras tecnologías como videoconferencias, suministro inteligente, chatbots, plataformas de aprendizaje electrónico y herramientas colaborativas.
Con respecto a Europa, la previsión de crecimiento de gasto TIC para 2020 ha sido revisada a la baja, pasando del 3,3% según los últimos datos publicados por IDC Research, al 1,4% en el escenario más probable de acuerdo con las últimas encuestas realizadas en plena crisis del COVID-19. Sin embargo, esto contrasta con los últimos hallazgos del CERT de Kaspersky ICS, a

principios de 2020, que descubrió una serie de ataques dirigidos a sistemas de Japón, Italia, Alemania y el Reino Unido. La lista de objetivos incluía proveedores de equipos y software para empresas industriales.
Sería un error que "los árboles no nos dejen ver el bosque" por estar sumergidos exclusivamente en el impacto negativo del COVID-19 y el rebote sobre el crecimiento a corto plazo (en forma de "V", "U", "W" …) y ser incapaces de observar todo el contexto del problema en su plenitud. Es decir, ofrecer rápidamente al mayor número posible de empleados y clientes un fácil acceso a los sistemas, productos y servicios, rebajando o suspendiendo, los estándares de protección, dando lugar, por ejemplo, a potenciales riesgos de seguridad cibernética en las empresas.

Preparación ante futuros escenarios de sucesos y situaciones disruptivas
Fortaleciendo la **Resiliencia Organizacional (RO)** con estrategias basadas en mejores prácticas para la supervivencia, el BCI *(Business Continuity Institute)* lo define como la "capacidad de una organización, personal, sistema, red de telecomunicaciones, actividad o proceso para absorber el impacto de una interrupción o pérdida comercial y continuar brindando un nivel aceptable de servicio".

Es decir, la RO no solo aplica para eventos de crisis en las empresas, sino que también surge como una herramienta o guía que logra hacer a las compañías suficientemente sólidas, capaces de sobrevivir a cualquier dificultad mayor y obtener ventajas competitivas de situaciones adversas (ISO 22316: 2017). Así pues, con este nuevo enfoque la RO debe estar más asociada a la prospectiva y a la planeación. (BSI 65000)

Para ello, las empresas deben lograr su propio y único **Sistema de Gestión de la Continuidad de Negocio** (ISO 22301) y todo ello convenientemente evaluado bajo un **Modelo de Madurez** de su desarrollo e implantación o CMM (*Capability Maturity Model*)**,** que elimine las indecisiones o indefiniciones iniciales de liderazgo y respuesta ante un suceso/situación disruptiva y evite, en el mayor grado posible, la incertidumbre en los receptores / afectados / ejecutores de las medidas adoptadas, desde el principio. (ISO/IEC 15504, ISO/IEC 33000 evaluación y mejora de la capacidad y madurez de procesos). ¿Cómo hacerlo?

1. **Disponiendo de un Servicio de inteligencia empresarial** que facilite la toma de decisiones, teniendo como premisa la obtención de la información de las fuentes y canales preestablecidos, analizando la veracidad de los datos y su impacto en tiempo real o anticipándose a acontecimientos / consecuencias futuras para los intereses de la compañía, con el objetivo de ofrecer conocimientos y criterios para respaldar las actuaciones empresariales.

2. **Disponiendo de un Servicio y herramientas tecnológicas GRC** (Gobierno corporativo, Riesgos empresariales y Cumplimiento de obligaciones regulatorias) que facilite la implantación y ensayo periódico de Planes de Continuidad Tecnológica, Planes de Continuidad de Negocio, Planes de Gestión de Crisis y Planes Operativos específicos. Cada sector de actividad, cada situación geográfica, incluso cada negocio, por su propia idiosincrasia, deberá adoptar su propio modelo de RO. Previendo y preparando planes de acción ante escenarios de contingencias**.** No podemos cerrar ninguna opción y ante distintas estimaciones de las posibles situaciones que se nos presenten, tendremos que tener distintos escenarios y protocolos de respuesta (desde la perspectiva más favorable a la más desfavorable).

3. **Disponiendo de un Servicio de Ciberseguridad alineado con el Esquema Nacional de Seguridad (ENS).**
   En España, el ENS es el Sistema de Gestión de Seguridad de la Información (SGSI) para las Administraciones Publicas (AA.PP.). Es el marco, obligatorio para las AA. PP., para la protección de la información y su gestión a través de los medios electrónicos.

El ENS no se trata de estándares internacionales o normas discrecionales, son disposiciones legales o normas jurídicas, estando constituido por principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Su creación se contempla en la Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos, se regula a través del Real Decreto 3/2010 y ley 40/2015 de Régimen Jurídico del Sector Público y se desarrolla sobre las recomendaciones de la UE y los estándares internacionales de seguridad de la información, como la Norma ISO 27001.

El ENS aplica a la Administración General del Estado, de las CC.AA., de las Entidades Locales y demás Organismos, Empresas, Universidades Públicas y particularmente recogido en la Ley 9/2017, de Contratos del Sector Público (LCSP) y el Real Decreto-ley 14/2019, art. 122, estableciendo como elemento primordial del contrato, el cumplimiento con la legislación de protección de datos, así como especificaciones en materia de seguridad.

El ENS y la LOPD española 3/2018, precisan que los proveedores de servicios (de TI o que manejen datos personales) de las AAPP cuenten con un nivel de madurez de la seguridad equivalente al de la entidad contratante. Los pliegos de condiciones de los procesos de contratación pública exigirán, en su caso, la certificación en ENS para poder ofertar. Esto provocará que se valorará a aquellos proveedores que tengan certificados relevantes de gestión o de productos. (Modelo de cláusula para los pliegos de prescripciones técnicas).

Lección clave aprendida para una mayor capacidad de resiliencia frente a contingencias futuras

Debemos ser honestos con nosotros mismos y con los demás en este entorno global con una volatilidad, incertidumbre, complejidad y ambigüedad sin precedentes, reconociendo que nadie tiene todas las respuestas. Tener el valor de compartir las vulnerabilidades y ayudarse a encontrar un cambio para mitigar de manera integral el riesgo.

Fruto de esa reflexión sería una buena ocasión para buscar un nuevo enfoque:

- Pasando del tradicional Modelo Gestión del Riesgo Empresarial *(Enterprise Risk Management _ ERM)* basado en el control y reporte de la exposición al riesgo operacional derivada de la explotación de activos y contratos y susceptible de ser mitigable a través de la contratación de coberturas en el mercado asegurador;
- Al Modelo *Enterprise Security Risk Management (ESRM)* que permita y facilite un proceso transversal y colaborativo en la gestión de contingencias, manteniendo relaciones cruzadas funcionales para respaldar resultados compartidos y no verse atrapados en silos dentro de los organigramas, de modo que, entre otros, Seguridad Física, Seguridad TI, Prevención de Riesgos Laborales, Servicios Médicos, Medio Ambiente, Servicios Jurídicos, Recursos Humanos, Administración de Instalaciones, Cadena de Suministro y Comunicaciones estén proporcionando una mejor comprensión e implantación de :
  - ✓ Las capacidades de continuidad de negocio de socios y proveedores relevantes.
  - ✓ La definición de los recursos necesarios para reanudar las actividades en los tiempos requeridos (MTPD y RTO).
  - ✓ Diseño de estrategias de respuesta para riesgos específicos.
  - ✓ Nombramiento de equipos de respuesta específicos para el desarrollo y mantenimiento de SGCN con la pertinente cualificación / certificación.
  - ✓ El de SGCN, SGSI, debe estar evaluado, auditado, documentado y ensayado periódicamente y revisado / apoyado por la Dirección.
- La Nueva Realidad, tras el COVID-19, no debería pasar por la reducción transversal y generalizada de inversiones y costes en la empresa, sin previamente realizar un profundo análisis de riesgos y si el negocio / servicio podría aguantar el impacto de una nueva contingencia severa como consecuencia de una reducción o eliminación poco meditada de partidas presupuestarias relativas a "La Seguridad, sin apellidos"

(física, cibernética, laboral, medioambiental, industrial, médica, etc.). A título de ejemplo: si un incidente por causas de origen natural, tecnológico, actos antisociales / ciberdelitos, deriva en una interrupción eléctrica catastrófica y prolongada, esta provocará serios problemas en la Continuidad de Negocio de terceras partes y a su vez que ocurriría sobre el ¿IoT? ¿teletrabajo?, ¿comercio electrónico? cuya mención inunda librerías, webinars y foros empresariales de buen gobierno. Por último, podría derivar en la pérdida de servicios esenciales para la ciudadanía. En este escenario, después de una economía y mercado bajos mínimos provocados por el COVID-19, ¿Cuál sería el impacto negativo y el rebote sobre el crecimiento?, en forma de "U", "W", ¿"L"…?. Sería un error que "los árboles no nos dejen ver el bosque"

Roberto Hermida Areses
Jefe de Servicios de Resiliencia
EULEN Seguridad