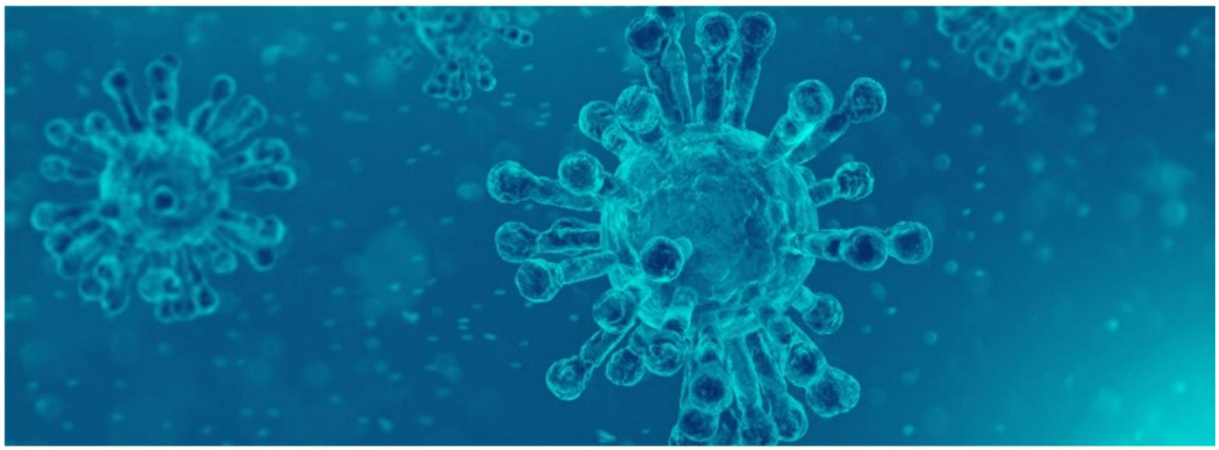
Grupo de Trabajo Business Continuity
Comisión de Gestión Empresarial

Enginyers Industrials de Catalunya



COVID-19: Rumbo a la empresa resiliente

Abril 2020

Versión 01

ÍNDICE

1. Introducción

Este documento pretende ser una guía práctica para la implantación de medidas de crisis (*Crisis Plans*) en organizaciones empresariales enmarcándolo dentro de las recomendaciones generales de las administraciones pertinentes en el presente momento, a la vez que para dar las pautas para crear un embrión de "*Business Continuty Systems*" en las organizaciones.

Desde hace unos años es frecuente oír a expertos de diferentes materias afirmar que estamos ante un cambio de época que se caracteriza por una mejora de las condiciones de vida en general, pero también por un incremento de la incertidumbre, aunque ambos conceptos parezcan contradictorios. Las relaciones sociales están cambiando, el mercado de trabajo está cambiando, las empresas están cambiando, la relación con el medio ambiente está cambiando, la tecnología está cambiando, los riesgos están cambiando...

Es decisión de las propias empresas visualizar este proceso de cambio continuo como un riesgo o como una oportunidad. La norma ISO-31000 ha definido la gestión de riesgos como la capacidad de gestionar cómo la incertidumbre afecta al grado de consecución de los objetivos de las empresas.

Las escuelas de negocio han trasladado el término, VUCA (*Volatility, Uncertainty, Complexity, Ambiguity*), acuñado por los soldados norteamericanos en los años noventa para definir el contexto de sus operaciones, para dibujar el entorno en el que operan muchas empresas hoy en día.

La pandemia mundial del Covid–19 ha puesto a toda la sociedad en general ante un escenario antes sólo previsto por los especialistas en epidemiología. Y nos sitúa en la antesala de una crisis económica caracterizada por la conjunción de una crisis de oferta y una crisis de demanda.

Resiliencia y adaptación

En estos momentos estamos pues construyendo una nueva forma de resiliencia. A pesar de la diversidad de respuestas organizacionales e institucionales y el hecho de que la situación nos ha cogido por sorpresa a todos, algunas organizaciones (pocas) disponían de planes para gestionar una pandemia en su proceso de gestión de crisis y escenarios. Aun así, la gran mayoría realizamos una planificación basada en lo que un antiguo dirigente de la FEMA en USA (*Federal Emergency Management Agency*) decía respecto a que planificamos con demasiada frecuencia para lo que somos capaces de hacer mejor y practicamos en lo que esperamos tener mayor éxito.

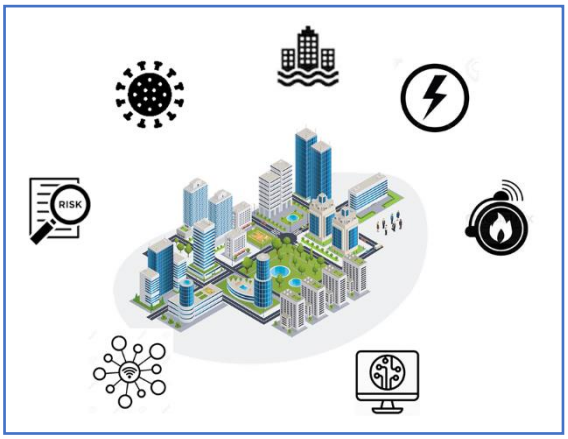
Así pues, es importante que las organizaciones se tomen el tiempo de implementar soluciones creativas y escalables para adaptarse mejor a la situación a pesar de la paradoja de "no tener tiempo" dados los caóticos impactos creados por esta crisis. Los planes deben por tanto estar abiertos a la incidencia, la flexibilidad, y a través de la agilidad del equipo reaccionar y readaptarlos. Las organizaciones deben tener planes con la visión de aprender a no poder prever todo, pero disponiendo de un marco que les permita la improvisación. En otras palabras, las organizaciones y sus planes deben desarrollar la capacidad de ser flexibles para su supervivencia en este tipo de situaciones estableciendo un equipo o comité de gestión de la crisis suficientemente preparado. Esta preparación habrá surgido de un trabajo previo conducido por el vector de la resiliencia que nos guiará para conseguir una organización resiliente garantizando la seguridad y la continuidad de la producción ante cualquier incidencia, obligado por las leyes y los contratos de los clientes y ser así capaces de Prepararse, Aguantar, Responder, Recuperarse y Aprender (PARRA), sobre todo aprender, de cualquier situación de crisis.

Se vislumbra un futuro en el que la definición de los procesos industriales más allá de la optimización, las economías de escala, la seguridad y calidad de los productos, deberá tener como pilar fundamental la capacidad de resiliencia. Es decir, la capacidad de sobreponerse a escenarios inesperados y adversos.

Centrándonos en el presente las recomendaciones incluidas en este documento son complementarias a las establecidas por las autoridades competentes en cada materia ante la situación actual de pandemia por Covid–19.

La pretensión del COEIC — a través del GT Business Continuity — es aportar una serie de recomendaciones mínimas de rápida implementación, ante la situación de emergencia en la que nos encontramos, y a la vez visibilizar la

necesidad de gestionar de manera formal los procesos de continuidad de negocio vía modelos que tienen ya amplio recorrido en muchas empresas como los modelos COSO, o bien modelo IS022301 entre otros. Finalmente hay que comentar que en el presente documento dispone de un sintético *checklist* a través del cual usted podrá visualizar la proximidad de que dispone su organización en disponer de un *Business Continuty System*.



2. Plan de crisis y recomendaciones COVID-2019 a empresas pequeñas y medianas

Objetivo y contenido: Dar pautas prácticas útiles para la Pyme y empresas en general de cómo actuar en la actual situación.

La estructuración del presente capítulo se realiza dando una visión y aspectos generales "ad–hoc" para pasar por los principales departamentos funcionales de la empresa:

2.1. Aspectos generales organizativos: comités de dirección y de crisis

La crisis del Covid–19 impone como medida de contención principal el distanciamiento social. La aplicación de esta medida en la mayoría de las empresas se ha realizado estableciendo el teletrabajo como forma principal de trabajar.

La implantación efectiva del teletrabajo requiere de una serie de medidas organizativas y de otras puramente tecnológicas.

Gerencia y Comités de Dirección

Identifique las personas "apoderadas" para actuar en nombre de la empresa.

Establezca un plan de actuación para el caso en el que estas personas no puedan actuar. Esto es especialmente importante en aquellas empresas que solo tengan un apoderado o representante legal.

Mantenga una comunicación fluida con el personal en caso de producirse cambios en la estructura, aunque sea de manera coyuntural.

No olvide comunicar a sus proveedores cambios que puedan producirse en las personas asignadas como interlocutoras.

Personas

Identifique de las personas de su empresa:

- ¿Cuáles prestan servicios esenciales, entendidos como aquellos que caso de no prestarse pondrían en peligro la continuidad de la empresa?
- ¿Cuáles pueden trabajar de manera remota?
- ¿Cuáles disponen de credenciales de acceso o certificados digitales para operar a través de internet? Por ejemplo, banca online, portales de proveedores, Agencia Tributaria, Seguridad Social, etc.

¿Cuáles solo pueden trabajar de forma presencial? Identifique las personas clave de terceros

(proveedores, clientes, empresas de logística, empresas de servicios, gestorías, centrales de alarma, etc.), asegúrese de que están disponibles, solicíteles su plan de contingencia establecido, complementándolo o alineándolo con el suyo.
Asegúrese de que toda la información necesaria y las herramientas están disponibles para las personas que las deban utilizar.

El Comité de Crisis

El comité de crisis es el órgano ejecutivo que implanta la empresa para reponer la situación acaecida frente la eclosión de un riesgo disruptivo. Aunque depende del CEO y/o del Comité de Dirección tiene plenos poderes desde que se lo otorgan, y duran hasta que finaliza el período de recuperación de la empresa hasta llegar hasta los niveles operativos admisibles establecidos

En ausencia de un marco de referencia, una organización es libre de definir su propio modelo de constitución y organización de una célula o comité de crisis y adaptarlo a su organización, sus riesgos y sus capacidades. Generalmente distinguimos las funciones permanentes de funciones de apoyo, cuya movilización no es sistemática y depende de la naturaleza de la crisis y las necesidades de gestión de crisis. Sin embargo, la experiencia común que se observa es la de tener en cuenta todos los aspectos operacionales de una gestión de crisis con expertos de cada área.

Este comité de crisis debe aplicar el plan trazado y los protocolos, pero mantener la visión creativa, flexible y adaptable mencionada anteriormente.

Responsable de alertas

- 24 horas de guardia – 7 días a la semana
- Recoge la 1ra información sobre el evento
- Moviliza la unidad de crisis por función de criticidad

Director de crisis

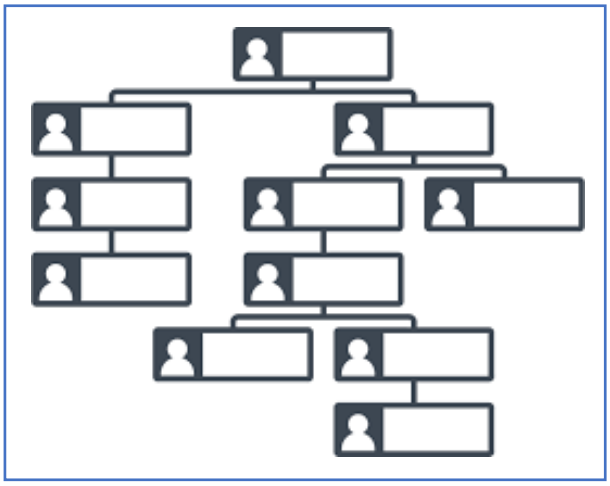
- Identifica los objetivos
- Define la estrategia general y el plan de acción
- Asegura la consistencia de las acciones llevadas a cabo
- Valida las comunicaciones antes difusión
- Trata los puntos a anticipar

Coordinador de crisis

- Pilota de la unidad de crisis (distribución tareas, cumplimiento de plazos, etc.)
- Asiste al Director de Crisis en su misión
- Ayuda a desarrollar acciones para lograr los objetivos identificados, determina las tácticas para implementar el plan y supervisa su ejecución.

Formarán parte del comité de crisis los siguientes cargos:

- Responsable operaciones (para informar del estado de los recursos disponibles)
- Responsable administración (para registrar las decisiones y mantener la documentación de la crisis)
- Responsable logística
- Responsable jurídico
- Responsable sistemas de información
- Responsable recursos humanos
- Responsable comunicación
- Asesor en continuidad de negocio y resiliencia. Este último aportará su experiencia en asuntos de BCM, y activará las soluciones de rescate y contingencia y asegurará la implementación efectiva de estas soluciones junto al director de crisis.



Herramientas y tecnologías

En todo este proceso existen herramientas y soluciones informáticas para la gestión de la continuidad que nos pueden ayudar. Desde soluciones *open–source* para implementar un teletrabajo ágil y rápido hasta plataformas con las que gestionar digitalmente estos planes de continuidad con funcionalidades especificas en la gestión de situaciones de urgencia como los diarios que registran la toma de decisiones (recordemos que ciertas decisiones pueden tener implicaciones judiciales y es conveniente llevar un registro de las

mismas o simplemente para aprender en el futuro sobre estas) además de poder compartir información en repositorios comunes con anuarios actualizados con los datos de nuestros recursos externos e internos para afrontar la crisis. Disponer de análisis sobre potenciales escenarios futuros con efectos cascada sobre nuestras cadenas de suministro, servicios básicos o infraestructuras pueden también ayudarnos.

Equipos informáticos

El acceso a los equipos dependerá de las medidas de seguridad implementadas y el método de acceso remoto que la empresa decida utilizar.

Identifique casuísticas particulares de algunos equipos informáticos, por ejemplo:

- Equipos que tienen instalados certificados de software. Si no podrá acceder a este equipo remotamente deberá exportar el certificado e importarlo en equipo que vaya a utilizar para acceder.

- Algunos productos de software solo pueden utilizarse desde el equipo que tiene instalada la licencia correspondiente o por motivos de seguridad se ha vinculado el acceso a una dirección ip interna o una *mac address* concreta.

Centralitas telefónicas de voz IP.

Gestione con su proveedor del servicio de voz IP el desvío a otro teléfono fijo o móvil que pueda estar atendido.

CPD propio

Si dispone de un CPD propio seguramente dispondrá de un equipo de TI. Nadie mejor que ellos conocerá su negocio y que opciones tecnológicas serán las más efectivas para su caso en particular.

Oficinas

Durante el período de contingencia debe permitirse el acceso a las oficinas únicamente al personal expresamente autorizado.

Deben establecerse las medidas de distan–ciamiento entre los puestos de trabajo.

Deben establecerse los protocolos de limpieza recomendados por las autoridades sanitarias.

Recomendaciones sobre el teletrabajo

El concepto de teletrabajo refiere en términos generales a trabajar de manera remota fuera de las instalaciones de nuestra empresa. Las medidas de confinamiento derivadas de la crisis del covid–19 han hecho que el lugar de trabajo sea nuestro hogar y que muchas empresas y personas sin experiencia previa en esta forma de trabajar se hayan incorporado al teletrabajo.

La ciber delincuencia está aprovechando esta situación de stress general para cometer fraudes, por ello es importante que todo el personal esté concienciado en una serie de buenas prácticas de ciberseguridad.

La empresa deberá evaluar los riesgos de activar el teletrabajo y en función de los datos y servicios a los que se quiera acceder remotamente se deberá aplicar una serie de controles de seguridad.

Es importante mantener dos principios básicos de la seguridad TIC:

- Mínimo privilegio. Sólo se dará acceso a las personas que lo necesitan y con los permisos adecuados al papel que desempeñan en la compañía.

- Necesidad de conocer: Sólo se dará acceso a la información que la persona necesita conocer para realizar su trabajo.

Una implantación acelerada del teletrabajo sin evaluar correctamente la aplicación de estos dos principios puede derivar en brechas de seguridad para la compañía. De hecho, se está produciendo un incremento de ciber ataques durante esta pandemia.

A continuación, relacionamos las cuestiones básicas a tener en cuenta:

Elabore un mapa sencillo de las aplicaciones que desea poner en teletrabajo y establezca que método de acceso desea emplear y con qué dispositivo está autorizado.

La siguiente tabla muestra los métodos de conexión y formas de autenticación utilizados de manera más frecuente:

Como podemos observar los tipos de conexión y formas de autenticación aumentan su robustez en función de la criticidad de los servicios e información a la que permiten dar acceso.

La recomendación de no utilizar ordenadores propios para el uso de algunas aplicaciones y servicios deriva de que existen una serie de cuestiones relativas a la seguridad que la empresa no podría comprobar. Al final de esta sección se relacionan una serie de medidas que si se toman pueden hacer que un ordenador particular sea tan seguro como un ordenador corporativo.

Aplicaciones	**Ordenador propio**	**empresa**	**Tipo de Conexión**	**Forma de Autenticación**
Correo electrónico corporativa	✓	✓	HTTPS	Usuario / contraseña
Herramientas ofimáticas en línea	✓	✓	HTTPS	Usuario / contraseña
Internet corporativa con partes privadas	✓	✓	HTTPS	Usuario/contraseña
Intranet	⚠	✓	HTTPS	Usuario / contraseña
ERP / Aplicaciones corporativas	⚠	✓	VPN, VSSL, MTSC, VDI	Usuario / contraseña + opcionalmente doble factor
Carpetas de red	⚠	✓	VPN, VSSL, MTSC, VDI	Usuario / contraseña + opcionalmente doble factor

Nivel	Tecnología utilizada / Tipo de conexión
Alto	Acceso a los servicios a través de sistema VDI: cada usuario dispondrá de una máquina virtual que a todos los efectos será un equipo de la propia organización
Medio	Acceso a los servicios a través de un Servidor de Escritorios Remoto (MTSC): las personas usuarias accederían a una especie de máquina virtual con acceso a los mismos servicios corporativos que si estuvieran en la oficina.
Inseguro	Acceso directo a los propios equipos de los usuarios (p.e: Teamviewer, Real VNC, Zoho Assist, Ammy Admin, etc) **se desaconseja** de forma expresa. En caso de que esta sea la única alternativa posible deberían aplicarse las siguientes medidas de seguridad complementarias: • Restringir las direcciones IP desde donde se van a originar las conexiones. Hay que tener en cuenta que la mayoría de usuarios contarán con conexiones de internet con direccionamiento IP dinámico lo cual complicará la gestión de la implementación de esta medida de control. • Utilice un mecanismo de doble factor de autenticación. • Active el registro de auditoria de las conexiones remotas y guarde al menos los siguientes datos: 1. Dirección IP origen de las conexiones. 2. Hora de inicio y de fin de la conexión. 3. Comandos ejecutados. 4. Ficheros ejecutados o accedidos. 5. Unidades de red que se mapean directamente en el ordenador remoto, especialmente vulnerables ante ataques de ransomware.

Se plantean tres niveles de seguridad asociados al tipo de conexión utilizado:
Medidas de seguridad que deben tomarse desde la perspectiva de la persona trabajadora ante un escenario de teletrabajo en confinamiento:

- Utilice para conectarse su red wifi privada o conéctese mediante un cable Ethernet directamente a su router. Evite utilizar redes wifi públicas ya que podría exponer su equipo y la información que contiene.

- Si utiliza un ordenador particular verifique que:
  - El software del ordenador se encuentra actualizado.
  - Dispone de un antivirus actualizado instalado.
  - Dispone de control de acceso al ordenador con usuario y contraseña y la persona usuaria garantiza la confidencialidad de la contraseña.
  - Dispone de bloqueo de pantalla cuando no lo está utilizando.
  - No almacene información corporativa en el disco local.
  - Bloquee la estación de trabajo, si deja de trabajar temporalmente, aunque esté en su casa.

- Manténgase atento a cualquier comportamiento extraño del ordenador, como exceso de publicidad en la navegación por internet o una ralentización sin motivo del tiempo de respuesta del ordenador. Ambas señales podrían venir derivadas de una infección del *malware*.

- Los ataques que se están recibiendo en esta etapa de la crisis covid–19 suelen llegar a través de correo electrónico, mediante lo que se conoce como phising, se trata de una suplantación de identidad del remitente, que lleva asociado un fichero infectado o un enlace en cuerpo del correo. No abra correos sospechosos o de servicios no solicitados.

- Tenga especial cuidado de la información confidencial o sensible LOPD que comparte mediante el teletrabajo. Si dispone de acceso a las carpetas de información corporativa es mejor que comparta la información en ellas. Si no dispone de acceso a las carpetas corporativas

envíe la información a través del correo corporativo mediante un fichero adjunto comprimido con contraseña. Envíe la contraseña al destinatario por un canal alternativo como por ejemplo SMS.

- Aunque estemos en nuestros domicilios trabajemos en lugares que permitan garantizar la confidencialidad de la información sensible con la que trabajemos. Si tenemos que trabajar en un lugar sin garantías de privacidad, minimicemos al máximo la exposición que pueda sufrir la información.

- Si utiliza herramientas colaborativas gratuitas, para reuniones virtuales, videoconferencias, trabajo en equipo, etc. Minimice la información sensible que comparta. Algunas herramientas en sus versiones gratuitas se reservan un uso de la información que pasa a través de sus servidores.

2.2. Estrategia comercial

Introducción y aspectos generales:

La razón de ser de una empresa es producir un bien o prestar un servicio que cubra una necesidad y por el que se obtengan unos beneficios. La vida de la empresa depende de encontrar y mantener a los clientes que sigan valorando este bien o servicio.
El mercado en una situación de emergencia crítica puede colapsar durante el período de la catástrofe y dependerá de la resiliencia del sistema para volver a recuperarse. En la medida que un mercado es más distribuido en un tejido industrial–comercial, más fácil se recuperará si cada empresa consigue su grado de resiliencia y autosuficiencia.

El mercado está vivo si el motor de la economía está en marcha o lo que es lo mismo el dinero corre y transacciona. Para ello es importante que en el período de colapso las administraciones públicas y financieras ayuden a cebar/latir el sistema, para recuperarse cuanto antes sea posible.

Ante una macro catástrofe las administraciones de los países deben velar por el suministro de agua, energía, transporte materias primas y telecomunicaciones y mantener la rueda de la liquidez monetaria que cataliza el intercambio de bienes y servicios. Con el fin de garantizar a las personas la primera necesidad de alimentarse, salud y vivienda.
Ante una situación de confinamiento domiciliario y con estas necesidades cubiertas de las personas, responsables y empleados de las empresas deberían poder seguir manteniendo la actividad de la empresa, generando valor desde su puesto de teletrabajo.

Durante un período de colapso cobran cada vez más sentido los robots y las smartfactories, donde las operaciones pueden funcionar con las personas supervisando, controlando y actuando en remoto desde zonas de seguridad y/o confinamiento. De manera que sólo los servicios críticos de operación y mantenimiento, previamente identificados y plenamente constatados por una evaluación de riesgos de discontinuidad sean atendidos de manera segura por el personal estrictamente necesario y suficiente.

Actividad Comercial: El Cliente en el centro del negocio

La empresa transacciona con sus clientes, empresas y particulares. Ante un colapso es lo más probable que los clientes vean paralizados sus procesos y sus demandas a corto plazo, por lo que la cadena puede pararse por bloqueo e inactividad. Aquí es el punto crítico de la respuesta a la crisis:

"Cómo ayudamos a nuestros clientes a seguir activos"

Este debe ser el principal objetivo de nuestra empresa. Solidaridad y apoyo a la subsistencia de nuestros clientes y también a clientes potenciales que hayan podido quedar desamparados. En la medida que lo logremos conseguiremos la continuidad de negocio y el restablecimiento más rápido de la normalidad comercial.

Las relaciones comerciales se basan en la confianza.

- La confianza mutua entre cliente y proveedor.

- La comunicación es el pilar de la confianza.

- La información es la alimentación de la confianza.

- La transacción comercial sólo es duradera si hay confianza en el futuro de la relación.

- La confianza garantiza la fidelidad cliente–proveedor

Para ello debemos tener un sistema CRM que nos ayude en el trato diario y permanente con nuestros clientes, y si no lo tenemos debemos emularlo y cubrir necesidades qué si en una situación normal son básicas, en una situación crítica son vitales y marcarán la diferencia frente a nuestros competidores.

Ante una situación crítica, nos encontraremos con la necesidad de gestionar la escasez. Escasez de todo lo que nos podamos imaginar y que puede paralizar nuestra atención a nuestros clientes, o paralizarles a ellos.

La Gestión de la Escasez, nos va a marcar tener que tomar decisiones de prioridad, de previsión y planificación temporal y de reparto de recursos de la manera óptima y justa.

Por lo tanto, quien disponga de la mejor información, o sistema de predicción más fiable será el empresario que mejor gestionará la escasez y optimizará la atención a los clientes.

Conocimiento Vital del Cliente:

Debemos tener informado el máximo conocimiento del cliente:

- Es importante mantener un ABC de clientes por su potencial, su historial, sus proyectos en curso y su estrategia de futuro.

- Es fundamental conocer el ABC de clientes por su trayectoria, seriedad, solera, solvencia, mercados y clientes a los que se dirigen.

- Conocer a los otros proveedores vitales y críticos del cliente.

- Fomentar, haber desarrollado relación con los clientes y sus proveedores de *partners* colaborativos frente a una pura relación transaccional simple.
- Establecer los canales de marketing relacional con el cliente o usuario final, tanto en B2B cómo en B2C si es necesario, con respeto al RGPD, que nos permitan interrelacionar con el cliente.

- Desarrollar sistemas digitales de seguimiento, vía garantía, servicio soporte, servicio puesta en marcha, resolución de incidencias, actualización, información, formación, trazabilidad logística, campañas de puntos y fidelización, etc., etc., que nos permitan mantener la máxima relación con el cliente.

En situación de crisis, será importante utilizar todos estos recursos para aprovechar cualquier oportunidad para llamar al cliente o escribir un mensaje que nos ayude a conocer su estado y en cualquier caso ayudarlo a resolver su situación. Ante todo, ser proactivos frente a acciones exclusivamente reactivas.

Prever un plan de acción derivado de oportunidades y amenazas, evaluando posibles necesidades para nuestros clientes, tanto críticas como nuevas. En función de la información de nuestros equipos humanos (experiencia / conocimiento / intuición) y sistemas digitales (adquiridos / documentados):

- Estimar que necesidades reales pueden tener nuestros clientes

- Estudiar posibles nuevas necesidades fruto de la situación emergente, hasta ahora nunca previstas o imaginadas.

- Analizar, valorar nuestra situación, ver nuestros puntos fuertes y en qué podríamos ofrecer nuevas alternativas de valor a nuestros clientes.

- Definir soluciones de emergencia a corto plazo, con criterio de cubrir de lo mínimo imprescindible para la subsistencia de nuestro cliente.

- Evaluar nuestras capacidades, hasta donde podríamos cubrir de nuestro ABC de clientes, priorizando según los análisis anteriores.

- Estudiar servicios de valor alternativo a ofrecer en caso necesario.

- Definir otros servicios a medio plazo, para ayuda a la recuperación del cliente, ofreciendo ser partícipe en los pasos y compromisos mutuos hacia el retorno de la normalidad.

- Evaluar riesgos. Estudiar posibles problemas de especulación, acaparamiento, abusos, falsedad de necesidades, denuncias de incumplimiento, etc., etc., y definirlas previamente claras en las ofertas, acuerdos y contratos posibles con los clientes.

- Analizar a nuestros competidores y empresas similares. Estimar posibles pactos de colaboración, sinergias o complementos. Ante una situación crítica la unión en red puede ser fundamental para la resiliencia global y particular.

- Testear todas las acciones, previamente, con un cliente test, para comprobar la evolución y viabilidad.

Pasar a la acción, teletrabajo / telecomunicación es la baza disponible, proactividad, comunicación y escucha al cliente es no dejarlo sólo, la *solidaridad* profesional puede ayudar a nuestro cliente a seguir en activo. En los negocios los clientes tienen mucha memoria y muchas decisiones se toman por el recuerdo o la recomendación de aquellas empresas que en su momento estuvieron al lado del cliente en los procesos críticos.

Comunicación al Mercado

Mantener la notoriedad y la imagen de la empresa, transmitir al mercado estado de actividad, positivismo y continuidad.

Aprovechar el tiempo de inactividad durante la crisis para destinar al máximo la generación de contenido de valor, para la web y las redes sociales:

-
- Generar documentos de aplicación (*white–papers*, noticias, etc.)

- Preparar documentos técnicos para los clientes
- Preparar casos de éxito y pedir colaboración a clientes (win–win)

- Desarrollar ponencias, cursos, webinars, etc.,.

- Publicar los contenidos y agendas de actividad en la web
- Planificar cuadrante de publicaciones en redes sociales, linkedin, twitter, Instagram, etc.

- Desarrollar a actores de la empresa como líderes de opinión

- Sembrar durante el período de clausura, para tomar aceleración en la recuperación de la normalidad.

2.3. Zonas (y operaciones) de recepción de mercancía

Protocolos y pautas empresa cargadora:

Crear 1 *check point* de camiones. Proceder con un *Checklist* de salud chóferes y que los mismos lleven EPIS ad hoc previo paso con vehículos a zona de carga/descarga.
Fase preliminar antes de ubicar r camión en zona muelle de descarga–

- Si chofer pasa *checklist* pero no lleva EPIS proveerles—por parte de empresa cargadora—de los mismos de 1 solo uso. Si no se disponen los mismos permanecerán en la cabina de la tractora.

- Utilizar EPIS ad hoc (mínimo Mascarilla, Guantes Opcionales gafas, y mono de papel de 1 solo uso)

- Comunicar y Guardar la Separación de 1,5 metros entre los intervinientes (chofer versus

cargador/receptor). Inclusive al firmar documento albarán de entrega yo CMR.

- Permitir accesos a zona de servicios para choferes a efectos de aseo y necesidades básicas. Servicios para choferes con medios ad–hoc. de aseo y sanitarios.

- Incrementar frecuencia de limpieza y desinfección de los suelos superficies por donde circulan vehículos, y donde se depositan las mercancías y bultos. Por parte del propio personal de operaciones.

PD: La limpieza e higienización del personal de plantilla seguirá su plan reactivado en los líquidos de limpieza.

- Intentar disponer mínimo de 2 de turnos, y que las citadas plantillas de un turno no se solapen con el otro.

- En los cambios de turno "Cero contactos " entre los 2 turnos, a la vez que retirada de los EPIS salientes para higienización, o desecho.

- Limpieza regular —con hipoclorito diluido—de volantes de *For Leefts* carretillas, y diferentes botones y accionamientos del área intra–logística pro–carga , y pro–expedición.

PD: Por parte del propio personal de operaciones.

PD: La limpieza e higienización del personal de plantilla seguirá su plan reactivado en los líquidos de limpieza.

2.4. Planta industrial: transformación digital

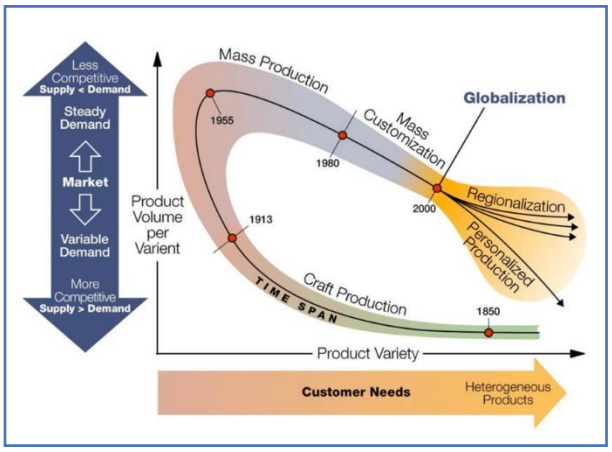
2.4.1 Digitalización y Control de plantas

La resiliencia de un sistema, entendida como su capacidad de adaptación a perturbaciones o a grandes perturbaciones (desastres), se basa en solamente en dos requerimientos: La capacidad de detección y la flexibilidad, que combinadas proporcionan la adaptabilidad.

Ésta es la tesis del profesor Duncan McFarlane de la Universidad de Cambridge, que va en la misma línea del informe de McKinsey "*Building resilient operations*", según el cual hay una relación directa entre el aumento de resiliencia y la aplicación de la digitalización en los procesos industriales.

La corriente de fondo iniciada en los años 60 hacia la flexibilidad, identificada y documentada por Boër y Dulio en 2007, está avanzando gracias a la Transformación digital de la industria (también conocida como Industria 4.0), planteando una producción en masa personalizada, es decir, con series muy pequeñas, denominada producción

"*Lot–size 1*". La siguiente figura ilustra el concepto, mostrando cómo se ha llegado al mismo con una perspectiva histórica:



La capacidad de detección es posible gracias a la Internet de las cosas (*Internet of Things*, conocida como IoT), mediante la cual es posible monitorizar y detectar mediante sensores, cámaras, micrófonos, etc. conectados en red, de modo que en función de sus lecturas se puedan disparar eventos. La necesidad de integrar estos sensores, con su electrónica a los sistemas físicos da lugar a los denominados sistemas ciberfísicos, los cuales incorporan electrónica embebida, que son el bloque constructivo fundamental de la Industria 4.0.

La flexibilidad se obtiene utilizando sistemas de carácter descentralizado, los cuales se componen de subsistemas que en caso de desconexión tienen un alto grado de autonomía, y que en la reconexión son capaces de reacondicionar su operativa según el contexto al que se ha conectado de forma dinámica. Estos agentes inteligentes se denominan holones, dando lugar al "*Agent based and holonic manufacturing*", y para implementarlos es necesario un nivel de digitalización que requiere la convergencia de los mundos de las TIC (IT o *Information Technologies*) con el mundo de las operaciones (OT o *Operation Technologies*). Dicho proceso, identificado por *Rockwell Automation* en 2007 se denomina "Convergencia IT/OT" y es uno de los grandes retos técnicos y humanos de la Transformación digital de la industria, puesto que requiere de nuevos perfiles profesionales de carácter híbrido que se están formando actualmente.

La adopción de la Industria 4.0 en el tejido industrial, en particular el europeo, ha seguido un crecimiento sostenido desde que empezó a acelerarse en 2013 hasta hoy. Sin embargo, a pesar de estar inmersos en la Cuarta revolución industrial (de la que se deriva el sufijo 4.0), estudios como el *Digital Transformation Scoreboard* de la UE, ponen de manifiesto el retraso de las empresas respecto a la Transformación digital, especialmente en una parte significativa de PYMEs. Debido a ello, en el período 2015–2020 se ha puesto en marcha numerosos programas gubernamentales para la promoción de la Industria 4.0 tanto a nivel de la UE, como a nivel estatal (prácticamente cada estado ha puesto en marcha un programa nacional), a nivel regional y también a nivel local.

***Digital Twin*, o la simulación de robots y unidades productivas**

Con motivo del coronavirus COVID–19, ha emergido una corriente de opinión que sostiene que esta crisis va a suponer un fuerte impulso en los procesos de transformación digital, a pesar de las dificultades económicas que puedan derivarse de ella. Más allá de la eclosión forzada del teletrabajo, lo cual está llevando a un cambio de mentalidad respecto a esta forma de trabajar, conceptos centrales de la Industria 4.0 como el gemelo digital (Digital Twin), están adquiriendo un creciente protagonismo. Empresas como ABB han anunciado la disponibilidad gratuita de un gemelo digital de sus productos. En este caso, los gemelos digitales de los robots que fabrican y comercializan, incluyen un software de simulación (en este caso cinemática, dinámica, electromagnética y energética) que permite entender cómo funcionan, programarlos y comprobar que el programa y el comportamiento del robot es correcto sin necesidad de disponer del producto físico. Su producto *RobotStudio* será gratuito hasta finales de 2020 con el objetivo de no frenar actividades por la dificultad de trabajar con los sistemas reales o físicos consecuencia del COVID–19. Otros fabricantes de robots como *Universal Robots*, ofrecen desde hace tiempo el simulador de forma gratuita, descargable en su página web, y no es descartable que este enfoque se extienda de forma permanente al resto de fabricantes.

Según Jeremy Rifkin, autor de "***La sociedad del coste marginal cero***", los sistemas intensivos en software son la base de una nueva economía

caracterizada por unos costes marginales cercanos a cero, debido al bajo coste de almacenamiento y replicación de estos, independientemente de su coste de desarrollo, el cual puede ser astronómico.

Por otra parte, además del software de simulación, el otro elemento constitutivo de los gemelos digitales son los datos obtenidos de la operación en el día mediante la IoT . La proliferación de sensores de todo tipo para monitorizar los sistemas permanentemente en tiempo real está generando grandes volúmenes de datos (*big data*), que no sirven solamente para calibrar a los simuladores, sino que permiten anticipar el funcionamiento futuro de los sistemas, como en el caso del mantenimiento predictivo y la consiguiente eliminación de paros de línea. Asimismo, estos datos también se utilizan entrenar a los sistemas de inteligencia artificial (del tipo *machine learning*), que permiten que los sistemas tengan un grado de adaptabilidad desconocido hasta la fecha. Por ejemplo, sistemas basados en visión artificial pueden identificar, sujetar y manipular piezas nuevas sin tener que haberlas programado previamente en los robots y manipuladores, tal y como ha sucedido en la Industria 3.0.

Sistemas informáticos localizados, o "Edge": ISO/IEC TR 23188

Los datos obtenidos mediante la IoT pueden almacenarse local o remotamente. El almacenamiento y procesado local se basa en los sistemas denominados *edge*, es decir, sistemas informáticos locales cercanos al mundo físico, y el almacenamiento remoto se basa en los sistemas denominados *cloud* (o en la nube), es decir en centros de datos o *datacenters*. La definición de estos conceptos y la interacción entre ellos está formalizada en la norma ISO/IEC TR 23188, y su relación con la continuidad de negocio es objeto de estudio por parte de firmas consultoras y expertos en la materia.

Según David Linthicum, *Chief Cloud Strategy officer de Deloitte Consulting*, el criterio de separación entre *cloud* y *edge* debe ser considerado desde el punto de vista de la continuidad de negocio. La desconexión de un dispositivo basado en el edge respecto algún tipo de procesador maestro, ya sea un *cloud* público, *cloud* privado o sistemas locales tradicionales, puede ser visto como una situación de alto riesgo desde una perspectiva 3.0, sin embargo, bajo una óptica 4.0 éste puede ser el mejor enfoque, debido al alto grado de autonomía de los sistemas. Es el caso en que los dispositivos del *edge* tienen la capacidad de manejar el procesamiento de datos localmente, lo que podría incluir el aprendizaje automático y el análisis predictivo. Los dispositivos del *edge* son muy capaces en términos de procesamiento de datos medianos o livianos. Cuando hay pocos datos que guardar, tiene sentido almacenarlos en el *edge*, el cual se paga una vez, mientras que los sistemas *cloud* suelen cobrar por el uso. Desde la óptica de OT, el *cloud* puede actuar como un lugar para el almacenamiento fuera de línea de los datos en el *edge*, bien con fines comerciales o para planes de recuperación ante desastres.

Recomendaciones en la línea de combatir crisis de carácter sanitaria como el COVID–19

En base a los argumentos expuestos, se propone una lista que introduce en lo posible elementos de control remoto y automatización en los procesos productivos mediante telecontrol, robótica o sistemas de carga, operación y descarga que no requieran atención presencial:

- Incorporar sensórica para monitorizar constantemente los parámetros de los procesos y tomar medidas anticipativas que eviten interrupciones en la producción ("poner ojos y oídos dentro de los procesos").

- Utilizar la Internet de las cosas para transmitir y almacenar los datos obtenidos por los sensores con el fin de analizar y obtener información que permita adoptar medidas correctoras anticipadas.

- Utilizar en lo posible software de modelado, 3D y simulación para el desarrollo de productos y servicios, facilitando el trabajo colaborativo, transversal y remoto.

- Utilizar gemelos digitales (*digital twin*) para el desarrollo y puesta en marcha virtual (*virtual commissioning*) de sistemas de producción, lo que permite desarrollar las tareas de ingeniería de forma colaborativa y remota.

- Diseñar los nuevos sistemas productivos de forma holónica para maximizar la flexibilidad de mismo, y en consecuencia su resiliencia.

- Incorporar o planificar la incorporación de personal con perfiles híbridos IT/OT en la organización, para minimizar las barreras de carácter cultural a la digitalización.

- Definir una estrategia de separación de procesos y datos entre el *edge* y el *cloud*, teniendo en cuenta diversos escenarios de recuperación de desastres y continuidad de negocio.

Comentar finalmente en el presente apartado que la aplicación de la "Industria 4.0 "aumenta la resiliencia de los sistemas y reduce los problemas de riesgo sanitario derivados de la concentración de un alto número de personas en los espacios donde se realizan procesos productivos.

2.4.1. *2.4.2. Operaciones físicas en Plantas*

Seguidamente se exponen una serie de medidas donde la participación de operarios es precisa:

- Utilizar EPIS ad hoc (mínimo Mascarilla, Guantes Opcionales gafas, y mono de papel de 1 solo uso)[1]

- Disponer mínimo de 2 de turnos, y que las citadas plantillas de un turno no se solapen con el otro.

- En los cambios de turno "Cero contactos " entre los 2 turnos, a la vez que retirada de los EPIS salientes para higienización, o desecho.

- Limpieza regular –con hipoclorito diluido– por parte del personal de operaciones de todas las de superficies de contacto habitual: botones de accionamientos de máquinas y mando, teclados de PC, pantallas táctiles, pomos, puertas, cortinas separadoras internas de PVC...

Nota: La limpieza e higienización del personal de plantilla seguirá su plan reactivado en los líquidos de limpieza.

- Incrementar la frecuencia y la intensidad de limpieza de wc y duchas de planta.

- Guardar —en la medida sea posible— 2 metros de distancia entre operarios. Cuando no sea posible se activa la recomendación de utilizar monos de 1 solo uso y gafas protectoras.

- Aplicar la Reglamentaciones de aplicación en función del sector, y actividades de la empresa

- Facilitar la comunicación del trabajador caso que tenga síntomas

2.5. Zonas (y operaciones) de expedición

Las operaciones de expedición guardaran las mismas pautas que las operaciones de recepción de mercancía (punto 1.3–)

2.6. Mantenimiento de instalaciones

Para la actividad de las empresas, el mantenimiento de las instalaciones es vital para la continuidad de negocio.

Si en situación normal ya es un imperativo, en momentos de crisis las empresas proveedoras de bienes de equipo y servicios deben tener previsto recursos específicos para atender a sus clientes ante incidencias.

Para ello, ante situación de confinamiento, será imprescindible disponer de herramientas previstas e implantadas de mantenimiento remoto, para atender a los clientes.

[1] Normas ISO vinculadas a COVID-19
https://www.iso.org/covid19

Se deben disponer herramientas de mantenimiento:

- Mantenimiento preventivo: Inspeccionar y monitorizar las instalaciones en remoto, seguir protocolos de revisión puntos clave y respetar períodos de ciclo de operaciones.
- Mantenimiento correctivo: Tener plan de formación, información de manuales y asistencia remota al cliente.
- Mantenimiento predictivo: Si es posible ir implementando sistemas de evaluación de rendimiento y acceso a datos en tiempo real, para realizar analíticas con previsión de riesgos.

Recomendar tener previstas soluciones de comunicación video–llamada y realidad aumentada de apoyo al mantenimiento, y en su caso emular el espíritu de la realidad aumentada utilizando los medios disponibles.

Las tareas de mantenimiento son operaciones normalmente de alta complejidad, donde aparecen parámetros no previstos, averías intempestivas, variables nuevas no contempladas y el usuario en la urgencia no está preparado para actuar sólo, lo que le induce a llamar y pedir ayuda a su proveedor.

En esta comunicación en tiempo real proveedor usuario ante una avería o anomalía se requiere una cantidad relevante de información, procedimientos y técnicas, por lo que el usuario en el campo de operaciones no lo dispone y el proveedor podrá ser muy útil en remoto si se han armado de herramientas adecuadas.

2.7. Plan de continuidad dentro la gerencia de riesgo. Visión aseguradora

El seguro, con sus más de 4.000 años de antigüedad, ha acompañado a las personas en su continuo desarrollo, adaptándose en cada momento a las necesidades y nuevos riesgos que se iban presentando hasta llegar a la sociedad actual que se ha definido como la sociedad del riesgo en la cual el seguro, con su continua evolución, ha demostrado una adaptación a las nuevas necesidades de cobertura de los nuevos riesgos.

Las empresas en la actualidad tienen multitud de interdependencias tanto con sus clientes como con sus proveedores, lo que hace que el riesgo de estos también suponga un riesgo para la empresa.

El riesgo existe y es necesario que las empresas sepan gestionarlo adecuadamente, lo que se conoce como “Gerencia de Riesgos” y que consta de una serie de acciones tendentes a suprimirlos o minimizarlos, pero, como existe la incerteza de que nunca vayan a ocurrir o de que si ocurren las consecuencias podrán ser asumidas sin problemas, se dispone de un amplio abanico de seguros que suponen el último eslabón al que acudir cuando ocurre un siniestro.

La ocurrencia de desastres de diferente magnitud y alcance han provocado que las empresas sientan la necesidad, no sólo de garantizar la recuperación

tecnológica, sino también la continuidad de la operativa de sus procesos de negocio, y por tanto de todos aquellos recursos que lo soportan, como sus infraestructuras, los centros de trabajo, el personal, la red de proveedores, etc.

Para garantizar la recuperación de la operativa de los procesos de negocio en las empresas tras un evento catastrófico, se debe trabajar en tiempo de normalidad analizando, diseñando e implantando soluciones que hagan posible su recuperación en el tiempo de afectación.

En este sentido y pensando en el *Business Continuty System* (BCS) es importante recordar que el seguro debe ser considerado como una inversión y no como un gasto, es decir, siempre debe contratarse los seguros que mayor cobertura ofrezcan en función del riesgo que se quiera garantizar, sin olvidar de ajustar lo máximo posible el capital asegurado, ya que la mejor póliza con un capital deficiente, es un mal seguro.

Dentro de la gran variedad de seguros que existe, podemos hacer una primera clasificación indicando que, por el tipo de cobertura, los BCS pueden disponer de los siguientes seguros:

- Sobre Personas como los seguros de vida, accidente, jubilación, pensiones, salud, enfermedad, etc.

- Sobre Bienes con una alta variedad de seguros que van desde el incendio, robo, avería, vehículos, transportes, multirriesgos (los más contratados), etc.

- Sobre el Patrimonio, también con una gran variación que van desde el Seguro de crédito, caución, Responsabilidad civil, Lucro cesante, DyO (directivos y administradores), *Compliance*, Cyberriesgos, etc.

- Asistencia en el hogar, comercio, en vehículos, en dependencia, en decesos, en viajes, etc.

En relación con el COVID–19 y muy especialmente a otras posibles pandemias que puedan ir apareciendo, es importante realizar una correcta evaluación de las posibles consecuencias que puede producir y realizar las inversiones necesarias para el control y respuesta para amortiguar las consecuencias. Para ello es imprescindible revisar los seguros actualmente contratados conjuntamente con su Mediador de seguros para adaptarlos a estos nuevos riesgos, analizando los contratos de seguros para valorar si las consecuencias de una pandemia dan cobertura tanto en los seguros personales, de asistencia en viaje, como en el lucro cesante entre otros.

En el caso del Lucro Cesante es importante analizar si la afectación de un proveedor o de un cliente puede tener consecuencias importantes para la empresa, en cuyo caso es recomendable incluir esta contingencia después de una correcta fijación del tiempo que la incidencia puede afectar al negocio.

También es importante la cobertura de los Cyberriesgos, en estos momentos en que la mayoría de los procesos están informatizados y que el trabajo a distancia cada vez tiene mayor protagonismo.

3. Definir las pautas de como embrionar un "*Business Continuty System*"

Objetivo y contenido: Definir conceptos básicos para empezar a entender en qué consiste, y que pretende un BCS (*Business Continuty System*). Dar pautas tipo preguntas y/o reflexiones de planteamiento a través de un sintético *checklist* que "iluminen" a la empresa a visualizar la necesidad y utilidad de disponer –a partir de ya mismo– de un BCS.

3.1. Definiciones preliminares de partida

Conceptos básicos para iniciarse en qué consiste, y que pretende un BCS (*Business Continuty System*):

- Continuidad de Negocio (*BC Business Continuity*): Capacidad de una organización para recuperarse de un incidente disruptivo y reanudar o continuar sus operaciones a niveles predefinidos aceptables, es decir, planificar como se debe actuar ante un suceso y/o evento inesperado o la posibilidad de que este ocurra.

- Riesgo: Efecto de la Incertidumbre sobre lo esperado, lo previsto, sobre un objetivo deseado, o sobre una meta.

- Mapa de riesgos: Grafico que en el disponemos identificados –en 2 dimensiones (probabilidad, e impacto)– los diferentes tipos y clases de riesgos de tipo disruptivo.

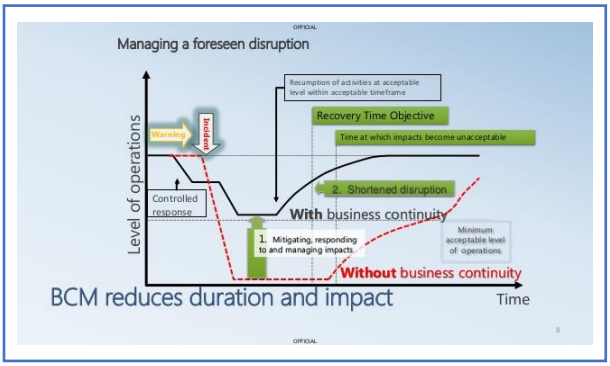
- Impacto: Efecto de la eclosión del riesgo. Se puede medir en tiempo de parada de mis instalaciones (que comportarán un para en la producción/realización de mis productos / servicios), o bien en términos económicos de perdidas. BIA: *Business Impact Analisys*

¿A qué medios generalmente afectan los incidentes disruptivos? Edificios, instalaciones, Personas, Servicios Informáticos (TIC), Servicios prestados por proveedores (*Supply Chain*), ...o a un conjunto de los mismos.

Objetivo que persigue un BCS (*Business Continuty System*): Que "–***no dejen de funcionar los servicios y medios esenciales*** ", o bien o –caso de caída– ***reponerlos en un mínimo de tiempo) para continuar dando servicio/producto al cliente***.

¿Como definiré los "Servicios y medios esenciales "en mi empresa? A través de un "***mapa de Interdependencias***" que incorporen medios y procesos.

3.2. Fases y metodologia de un bcsm (gestión de sistema de continuidad de negocio)



Fase 0 – Framework Definition (Marco de Gobierno)

Fase 1 – BIA–Análisis IMPACTO

Fase 2 – ANALISIS de RIESGOS

Fase 3 – Definición de ESTRATEGIAS DE CONTINUIDAD

Fase 4 – PLAN DE CONTINUIDAD (CP–Continuity Plan)

Fase 5 – Formación y Sensibilización del Personal

Fase 6 – Testeos–Pruebas. Simulaciones de "*breakdown*".

Fase 7–Mantenimiento, Revisión y Mejora del BCM

Que *Outputs* se derivarán del CP (*Continuity Plan*)

a) Las acciones que tomaré frente a cada riesgo: MITIGARLO, ASUMIRLO (aceptarlo), o TRANSFERIRLO (ver para este último en punto *1.7 Seguros ad–hoc*)

b) El *Recovery Plan* (RP): Plan de actuación cuando se da la eclosión del riesgo.

c) El tiempo objetivo para recuperar procesos: Determinar un tiempo T objetivo en el que recuperar la actividad esencial de la empresa. RTO: (*Recovery Time Objective*).

d) Comité de Crisis: Está compuesto por aquellos directores (de área o funcionales) sobre los que recae la decisión de la activación de sus respectivos planes de actuación en situación de contingencia. (Ver apartado 1.1)

¿Qué modelos disponemos para preparar e implantar un BCS (*Business Continuty System*) en mi empresa? COSO, MAGERIT, ISO22301:2019.

3.3. *Check list business continuity*, o como debería proceder para disponer de su bcs

Contenido: Preguntas tipo *checklist* y / reflexiones de planteamiento que "iluminen" a la empresa a visualizar la necesidad y utilidad de disponer –a partir de ya mismo– de un BCS.

Finalmente –en función del grado de cumplimentación de este; se visualiza un resultado orientativo de lo cercano que se encuentra de disponer de un BCS.

Asimismo –aprovechando la situación actual en que vivimos inmersos, y que genera sensibilidad y predisposición– se dan de manera indirecta: las pautas sobre como embrionar un *Business Continuty System* en su empresa.

3.3.1. Check –list ABC*:*

PARTE A (Nivel A):

- ¿Dispone su empresa de una identificación de riesgos disruptivos, con su correspondiente valoración a nivel de impacto en su organización? Nota: Incluimos aquí también la disposición de un mapa de Riesgos.
- ¿Posee un mapa de interdependencias de medios y procesos?
- ¿Ha considerado los riesgos derivados de la eclosión de otro riesgo raíz?
- ¿Ha considerado que un porcentaje significativo de su plantilla pueda no tener la posibilidad de no asistir a sus instalaciones?
- ¿Dispone identificado –entre su plantilla– el personal que es esencial para el funcionamiento de su empresa?
- ¿Dispone de una estrategia de Continuidad?
- Dispone de Planes de Continuidad

- Dispone de Equipo de Crisis definido en base a N escenarios de eclosión de riesgos.

- ¿Dispone de Planes de Crisis?

- ¿Ha considerado medios alternativos de comunicación –entre su plantilla– para utilizar en una Crisis?

PARTE B (NIVEL B)
Nota: Complételo si dispone de todo lo anterior (A)

- ¿Dispone documentado lo anotado anteriormente?

- ¿Los revisa y actualiza con 1 periodicidad definida?

- ¿Ha sensibilizado, y formado al personal en los anteriores aspectos?

PARTE C (NIVEL C)
Nota: Complételo si dispone de todo lo anterior (A y B)

- ¿Ha realizado simulaciones de crisis (de desencadenación y/o eclosión de riesgos)?

- ¿Registra los incidentes derivados en la simulación de situaciones de crisis?

- ¿Adapta los Planes de crisis después de los 2 puntos anteriores?

3.3.2. *Autodiagnosis (resultado de cumplimentar el check– list A + B + C)*

- Si dispone de un 50% de respuesta afirmativas de la Parte A– Su empresa está sensibilizada con el B.C., y está en condiciones propensas para desarrollarlo, e implantarlo

- Si dispone un 90% de la PARTE A, y un 77% de la PARTE B– Ya dispone de un Pseudo sistema de B.C., aunque debe formalizarlo, y madurarlo.

- Si dispone de un % de la PARTE A y PARTE B del 100%, y de un 77% de la PARTE C está próximo a disponer formalmente de un BC implantado

4. Conclusiones

La forma de proceder y gestionar– hasta el momento –en las empresas ya no es válida a día de hoy –post covid-19–.

La superación en breve de todo el *breakout* en las empresas van a obligar a los CEOS a replantearse buena parte de la estrategia incorporando –de manera emergente– el área de *Bussines Continuity*, muy extendida, desarrollada e inherente en el ámbito anglosajón (Great Britain, EEUU).

Esta parcela ya se está teniendo en cuenta, y valorada de cara a establecer relaciones comerciales con otras organizaciones (proveedores principalmente) que deberá exhibir y demostrar su "***músculo resiliente***", o –de lo contrario– estarán fuera de mercado. El concepto de "*Risk thinking*" hace irrupción pues en la empresa occidental.

Al igual que considerábamos las validaciones de AMFE para procesos, deberemos de incluir el concepto de "*Resilience by Design*". Es decir que –en el actual contexto VUCA– se deberán diseñar especialmente los procesos críticos como resilientes por definición (*Security by Design*)

Es deseo expreso de los autores del presente artículo que un gran porcentaje de empresas y organizaciones salgan indemnes de la presente crisis.

5. Autores del documento

El presente documento ha sido redactado de forma colaborativa en régimen de teletrabajo –durante la semana del 23–3–2020—por un equipo de personas “ad hoc” perteneciente al GT –Business Continuty del COEIC / EIC Enginyers Industrials de Catalunya:

Josep Ma. Peiró i Alemany
Ingeniero Industrial superior, especialidad eléctrica, por la ETSEIB / UPC (Universitat Politècnica de Catalunya) y Dirección Comercial y Marketing por EADA Barcelona, se ha dedicado durante 36 años al desarrollo de negocio (estrategia, marketing i ventas) en empresas de los sectores de gestión de la energía y automatización industrial, destacando Square D, Telemecanique, Merlin Gerin, Crouzet y Schneider Electric. Actualmente es miembro de la Comisiones de Energía y Sociedad Digital del Colegio de Ingenieros Industriales de Catalunya. Colabora como secretario técnico del Grupo de Business Continuity del COEIC, ejerce cómo secretario técnico de CMES, Colectivo para el Nuevo Modelo Energético Social y Sostenible de Catalunya impulsando la transición energética y es colaborador freelance de la revista infoPLC++.

https://www.linkedin.com/in/josep–maria–peir%C3%B3–alemany–77aa2527/

Xavier Pi i Palomés
Se define a sí mismo como knowmad. Es Ingeniero Industrial por la UPC (Universitat Politècnica de Catalunya), Perito Judicial experto en Informática Industrial y TIC por el COEIC. Es apasionado sobre la Internet de las cosas como factor central de la 4ª revolución industrial y como herramienta de empoderamiento para los ciudadanos (profesionales, makers y estudiantes). Su perfil híbrido en ingeniería mecánica y del software le ha aproximado al mundo de los sistemas ciberfísicos. Combina su actividad profesional en el campo industrial con la co–dirección del Máster en Industria 4.0 de la UPC y con la docencia en Ingeniería del software y en Industria 4.0 en la UOC. Es miembro del Consejo editor de la revista InfoPLC++ y asesor en el proyecto europeo DITRAMA en Industria 4.0.

http://es.linkedin.com/in/xavierpi

José Luis Rubiés Viera
Cursó estudios de las licenciaturas de ciencias económicas y empresariales, ciencias políticas y de la administración y la diplomatura en gestión y administración pública en la Universidad de Barcelona. Es funcionario de carrera del Ayuntamiento de Barcelona en la categoría de Técnico Superior de Gestión desde 1988, donde ha ocupado diversas posiciones siempre vinculadas a las Tecnologías de la Información y la Comunicación, la gestión de la innovación, la sociedad del conocimiento y la ciberseguridad. Así mismo está en posesión de diversas certificaciones profesionales reconocidas internacionalmente en los ámbitos de la auditoria (CISA), gestión de la seguridad (CISM), gestión de riesgos (CRISC) y gobernanza de las TIC (CGEIT). Es lead auditor certificado en las normas ISO–27001 Gestión de la Seguridad de la Información, ISO–20000 Gestión de Servicios TIC, ISO–9001 Gestión de la Calidad e ISO–22301 Gestión de la Continuidad de Negocio. Actualmente es vicepresidente del capítulo Barcelona de ISACA (Asociación para el Control y la Auditoria de los Sistemas de Información). Miembro de la Comisión TIC del Colegio de Profesionales de la Ciencia Política y la Sociología de Catalunya y miembro del grupo de Business Continuity del COEIC.

http://es.linkedin.com/in/jlrubies/

Miguel Ángel Estruga Camacho
Ingeniero industrial Superior en Organización—– colegiado 7.700—Ha desarrollado su trayectoria profesional entre las empresas AUTOLIV–KLIPPAN , GRUPO SCHNEIDER , y MAASTRICHT CONSULTANTS donde es el Director Técnico de Proyectos “ ERIM “ (Enterprise Risk Integrated Management” , “Business Continuty Systems “ ,y “ Recovery y Contingency Plans “.Sectores principales : Logística (de productos de alto valor, sanitarios, farmacéutico, alimentación, ...), Distribución, Hoteles, , Industrias , Procesos Alimentarios. Referenciales; TAPA (FSR y TSR), GDP (Distribución y Logística de medicamentos), ISo22301 (Business Continuty) , ISo27001(Seguridad de la Información) , ISO 9001 (Gestión de la Calidad),BRC–IFS, ISo22001 , Codex alimentarius.Es profesor asociado a Departament de Formació de “Enginyers Industrails de Catalunya “ en sus áreas de expertisse .

https://www.linkedin.com/in/miguel–angel–estruga–camacho–358ab416

Ignasi Fontanals Vidal
Emprendedor en el sector de la resiliencia desde de 2012, cofundador de varias iniciativas empresariales y asociativas entorno a la resiliencia de las organizaciones y los territorios. Ha participado en diversos proyectos de investigación en resiliencia. Ha sido líder de paquete de trabajo en uno de los mayores proyectos europeos en Resiliencia Urbana y cambio climático del programa H2020 de la UE. Actualmente es Director Europa de la *spin–off* canadiense Rezilio Technologie.

https://www.linkedin.com/in/fontanals/

Salvador Brugarolas Costa.
Ingeniero Industrial Superior especialidad mecánica, por la ETSIIB. Dispone de amplia experiencia en el sector asegurador, en Endidades como La Unión y el Fénix Español, AGF–UFE y Allianz Seguros, desde 1980, hasta 2.017 realizando actividades de: a)Verificación de Grandes Riesgos Industriales, b) Suscripción de Seguros de empresas en el Departamento en Grandes Cuentas. Actualmente es miembro de las Comisiones/Grupos de Trabajo de: Seguridad, Compliance y Continuidad de Negocio en el *Col.legi d'Enginyers Industrials de Catalunya*,

http://linkedin.com/in/salvador–brugarolas–19ba9252

Rafael Nadal Ribas
Ingeniero Industrial, Corredor de Seguros, Perito de Seguros y Judicial, es miembro de la Junta del Colegio de Mediadores de Seguros, de la Junta de la Asociación de Ingenieros Industriales de Cataluña y asesor del IDES. A lo largo de la vida profesional, ha trabajado en Compañías de seguros, correduría y es socio fundador de las empresas Gestión Técnica de Riesgos (GTR) y Asesores en gerencia de Riesgos2 (AGR2). Docente en los centros EPSI de la UAB, ICT, INESE. UPC, CEU y autor de las siguientes publicaciones: Valoración previa de los Bienes en los seguros de daños, Anatomía de un siniestro industrial, La Gerencia de Riesgos, La Pérdida de Beneficios, colaborando en la publicación de La Investigació d'Incendis i Explosions y en el Semáforo de los Riesgos, habiendo publicado artículos diversos.

http://linkedin.com/in/rafael–nadal–b00133102

6. Bibliografia e informacion complementaria de utilidad

- D. McFarlane, R. Srinivasan, and A. Thorne, “Identifying the Requirements for Resilient Production Control Systems,” in Service Orientation in Holonic and Multi–Agent Manufacturing, T. Borangiu, D. Trentesaux, A. Thomas, and D. McFarlane, Eds. Cham: Springer International Publishing, 2016, pp. 125–134.
- Rockwell–Automation, “Come Together: IT–Controls Engineering Convergence Furthers Manufacturers,” Rockwell Automation, 2007.
- J. Rifkin, “The Zero Marginal Cost Society: The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism” . St. Martin’s Press, 2014.
- European Commission, “Digital Transformation Scoreboard,” European Commission, 2018
- ISO/IEC “ISO/IEC TR 23188:2020 Information technology — Cloud computing — Edge computing landscape”, 2020
- McKinsey, "Coronavirus: las recomendaciones para las organizaciones respecto a la fuerza laboral y relacionadas con el teletrabajo “, marzo de 2020
- MA.Estruga . Artículo en SIL 2019: Planes de Contingencia frente acontecimientos disruptivos en el Sector Logístico https://www.silbcn.com/es/blog/sil-planes_de_contingencia_frente_a_acontecimientos_cyberdisruptivos_en_el_sector_logistico-64.html
- MA. Estruga. Artiulo en SIL 2020; Planes de Contingencia: un antes y un después de MArzo 2020 https://www.silbcn.com/es/blog/sil-planes_de_contingencia_un_antes_y_un_despues_de_marzo_de_2020-74.html
- Linthicum, David. “Edge computing in hybrid cloud: 3 approaches”, https://techbeacon.com/enterprise–it/edge–computing–hybrid–cloud–3–approaches
- Fontanals, L., Tricàs, J., Canalias, F.,2014 “Resiliencia territorial, vector de gestión de servicios. Estudio de Caso de la Garrotxa”, Estudios Empresariales, 144, 2014/1.
- Compilación de Normas ISO vinculadas a COVID–19: https://www.iso.org/covid19
- Normas ISO relativas a sistemas de gestión de la continuidad de negocio y resiliencia
- ISO 22301:2019 Security and resilience – Business continuity magement systems – requirements
- ENGINYERS INDUSTRIALS DE CATALUNYA https://valuexperience.com/enginyers–treballa–eficacment/?id_mail=51872326)
- INCIBE (Instituto Nacional de Ciberseguridad) https://www.incibe.es/protege–tu–empresa/blog/pautas–teletrabajar–seguro https://www.incibe.es/protege–tu–empresa/avisos–seguridad/distribucion–malware–vinculado–covid–19–suplantando–varias
- GOVERN GENERALITAT DE CATALUNYA:. Recomanacions per a Empreses i Persones Covi–19 https://treball.gencat.cat/ca/inici/ https://portaljuridic.gencat.cat/ca/pjur_ocults/pjur_CoV–2/
- GOBIERNO DE ESPAÑA: Guía para los Centros de Trabajo: https://www.mscbs.gob.es/gabinetePrensa/notaPrensa/pdf/GUIA110420172227802.pdf https://administracion.gob.es/pag_Home/atencionCiudadana/Estado–de–alarma–crisis–sanitaria.html#.XoS3P2MzZ1s
- OMS https://www.who.int/es/emergencies/diseases/novel–coronavirus–2019

EDITA
Associació / Col·legi
d’Enginyers Industrials de Catalunya
Via Laietana, 39
08003 Barcelona
93 319 23 00
www.eic.cat