cooperación alemana
DEUTSCHE ZUSAMMENARBEIT

Implementado por:

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Guía para el diseño de un plan de continuidad de negocio para administraciones tributarias

En coordinación con:

COSEFIN
Consejo de Ministros de Hacienda o Finanzas de Centroamérica, Panamá y República Dominicana

SICA
Sistema de la Integración Centroamericana

CIAT
CENTRO INTERAMERICANO DE ADMINISTRACIONES TRIBUTARIAS
FUNDADO 1967

Guía para el diseño de un plan de continuidad de negocio para administraciones tributarias

cooperación alemana
DEUTSCHE ZUSAMMENARBEIT

Implementado por:
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

En coordinación con:
COSEFIN
Consejo de Ministros de Hacienda o Finanzas de Centroamérica, Panamá y República Dominicana
SICA
Sistema de la Integración Centroamericana

Guía para el diseño de un plan de continuidad de negocio para administraciones tributarias

ISBN: 978-9962-722-63-2

Publicado por:

Centro Interamericano de Administraciones Tributarias - (CIAT)
Avenida Ramón Arias, Ciudad de Panamá, Panamá
Tel. (+507) 307 CIAT (2428)
www.ciat.org

Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Domicilios de la empresa

Bonn y Eschborn, Alemania
“Programa Buena Gobernanza Financiera”
Agencia de la GIZ Bulevar Orden de Malta,
Casa de la Cooperación Alemana, Urbanización Santa Elena
Antiguo Cuscatlán, La Libertad El Salvador, Centroamérica.
Tel. +503 2121 5100
Giz-el-salvador@giz.de
Zentralamerika-giz.de

Versión

Noviembre (2024)

Por encargo del

Ministerio Federal de Cooperación Económica y Desarrollo (BMZ) de Alemania

Propiedad Intelectual

Autores

D. Ignacio González
D. Ana Maria Pastor Ruiz
D. Juan Carlos Román Cortes
D. Fernando Casquero Martin

Revisión por:

GIZ

Gustavo Ernesto Sánchez Buriticá
Orlando Castellón Tellería
Manfredo Octavio Chocano Alvarado

CIAT

Raul Zambrano
Mónica Alonso
Elizabeth Rodríguez

Contenido

1. Introducción

La actividad de la Administración Tributaria es imprescindible e insustituible. Sucesos inesperados, como la epidemia del COVID-19 o ciberataques han puesto de manifiesto la vigencia e importancia de garantizar la continuidad de la actividad de las administraciones tributarias durante y después de cualquier crisis.

El CIAT y la Cooperación Alemana para el Desarrollo, GIZ, son conscientes de la complejidad de las tareas de prevención aconsejables y de la necesidad de una planificación sistemática y coordinada de todas las áreas de una administración tributaria para garantizar la prestación de servicios a los contribuyentes y la continuidad de los ingresos. En consecuencia, han impulsado mediante una Acuerdo de Cooperación esta: **"Guía para la formulación del Plan de Continuidad de Negocio en la Administración Tributaria"**.

1.1. Objetivo de esta guía

El propósito de la iniciativa se manifiesta en su propio título:

a) **Guía.** Es un conjunto de normas orientativas sobre una materia, en este caso para la formulación de un *Plan de Continuidad de Negocio*. Su objetivo no es por tanto diseñar una alternativa a sistemas ya consolidados como la norma ISO 22301, que es reconocida como un estándar internacional, sino proporcionar los elementos de información oportunos para facilitar su objetivo declarado.

b) **Plan de Continuidad de Negocio.** Se pretende orientar la actuación de la Administración Tributaria con una visión amplia, que exceda lo meramente informático. El concepto de "negocio" es entendido en sentido extenso puesto que, junto con el mantenimiento de la recaudación y el servicio, se aborda cómo facilitar la actividad y el negocio del contribuyente que comparte, sin culpa, los efectos de la crisis.

c) **Administración Tributaria.** El concepto se entiende en sentido amplio, alcanzando a la Administración Aduanera, lo que es necesario en las agencias integradas, pero al tiempo acotado porque se focaliza en un conjunto limitado de administraciones con características propias.

1.2. Importancia de la continuidad de negocio en la administración tributaria

En el resumen ejecutivo del documento: *"Plan de Continuidad de Negocios: importancia creciente para las Administraciones Tributarias"* (CIAT, 2024) se expone que: "La reciente crisis provocada por la pandemia de COVID-19 ha puesto de relieve la importancia de contar con un Plan de Continuidad y ha recordado la necesidad de una atención extendida hacia este elemento estratégico". Se recuerda a continuación que "[…] Las crisis pueden afectar la continuidad de los procesos administrativos, tanto manuales como informatizados, y pueden abarcar desde eventos climáticos/fenómenos naturales hasta ataques cibernéticos, conflictos geopolíticos, cambios regulatorios y crisis sociales".

Señalan los autores que: "Las administraciones tributarias son organizaciones **vitales** para un país y no están exentas de este tipo de perturbaciones, por lo tanto, deben mejorar su resiliencia y abordar la protección de sus actividades como una necesidad estratégica".

Se observa que: "Sin embargo, hasta la fecha, de las 92 evaluaciones realizadas por TADAT (Herramienta Diagnóstica de Evaluación de la Administración Tributaria), la mayoría de los países de ingresos medios y bajos no contaban con un Plan de Continuidad de Negocios (PCN) robusto. Por lo tanto, surge la necesidad imperativa de contar con un PCN específicamente diseñado para las administraciones tributarias y sus complejidades inherentes".

La **guía** que introducimos ha sido concebida para responder al requerimiento de estar específicamente diseñada para ciertas administraciones tributarias, ajustada para permitir que países con ingresos medios y bajos la utilicen provechosamente y diseñada para integrarse en el contexto de las evaluaciones TADAT.

Su diseño pretende conciliar la filosofía subyacente en TADAT, el "*assessment*", el partir de evidencias, con la simplicidad, permitiendo la autoevaluación de las instituciones sin una costosa asesoría externa.

En resumen, la **guía** pretende satisfacer una necesidad acreditada con evidencias que afecta a intereses vitales de las Administraciones Tributarias (AT).

1.3. Estructura, alcance y público objetivo

Este documento describe los conceptos necesarios para evaluar el estado del proceso “Continuidad de Negocio” y una **guía** de diseño para elaborar un plan de continuidad.

Tras la Introducción realizada en el primer capítulo, se expone, en el segundo, el marco conceptual en el que se define el objetivo de estos planes, se acotan los conceptos y se muestran los beneficios de la práctica.

En el tercer capítulo se describe la estructura de la **guía** describiendo los materiales que contiene. En el cuarto se describen las cuatro áreas que aborda, actitud, visión, recursos y madurez, describiendo, en cada una de ellas, en primer lugar, el propósito central de la evaluación en el aspecto considerado y a continuación los indicadores relevantes.

En el quinto capítulo se expone el método propuesto para el diseño del Plan de Continuidad. Describe la arquitectura del método y muestra los pasos necesarios para el diseño de un Plan que contenga los modos de su autoevaluación.

En el sexto se aportan las referencias, seguido por un séptimo en el que se señalan las normas a las que hace referencia el texto. Por último, en el Capítulo 8 se incluye, como Anexo, el Cuestionario.

2. Marco conceptual

2.1. Definición de la continuidad de negocio

El CIAT ha definido: “Un PCN es un manual estratégico creado para ayudar a una organización a mantener o reanudar rápidamente funcionalidades del negocio ante una interrupción [o una disrupción]. Este Plan es el principal componente de un Sistema de Gestión de Continuidad de Negocios (SGCN)”. (CIAT, 2024).

El SGCN, por su parte, debe estar alineado con las estrategias de la organización […]. En la medida en que las estrategias son dinámicas, el SGCN también debe reflejar cambios. La juiciosa acumulación de cambios hace progresar la madurez de los procesos y de las organizaciones que los implementan.

Por definición, el estado de continuidad del negocio se manifiesta en la persistencia de la capacidad de una administración tributaria y/o aduanera para asegurar el cumplimiento de sus misiones. Entre ellas es principal la de proporcionar los bienes y servicios a la Nación para cuya producción fue creada, especialmente: (i) procesamiento de la recepción de impuestos, (ii) procesamiento de declaraciones de impuestos y gestión de la recaudación, (iii) procesamiento de reembolsos de impuestos, (iv) soporte al contribuyente en sus obligaciones, necesidades y en el disfrute de los beneficios a que tenga derecho y derivados de las políticas de gasto público.

2.2. Principales conceptos y terminología específica del sector

El capítulo cuarto y el cuestionario incluido en el Anexo recogen los términos habituales de la disciplina y utilizados en estándares como las normas ISO o los marcos ITIL (CIAT, 2024). El lector interesado debe remitirse a ellos.

Existiendo el propósito manifiesto de construir una guía alineada con TADAT se utilizan ciertos conceptos no habitualmente utilizados en el ámbito de la Continuidad de Negocio, que se explican a continuación.

Áreas de actividad

Las metodologías de evaluación más utilizadas describen los ámbitos tratados con términos como “áreas de rendimiento” (ARD en TADAT) o “áreas de performance”. En un Plan de Continuidad de Negocio, a diferencia de lo que sucede en otras facetas tributarias, como la recaudación, el rendimiento no es una medida primaria e inmediata pues muchos de los gastos se realizan para evitar que suceda algo y no para propiciarlo. Por este motivo se ha preferido utilizar área de *actividad*. Se trata de un término más genérico y no orientado exclusivamente a la precisión o el rendimiento. Por ejemplo, el mantenimiento y actualización de las normas es una actividad conveniente, una inversión a largo plazo, pero no produce un rendimiento medible.

PCN ofrece una evaluación global de cuatro áreas, como muestra la *Figura 1*.

Figura 1. Áreas tratadas en el PCN

PCN - Actitud
Es el compromiso institucional manifestado en políticas identificables, para actuar de un modo consistente en garantía de la continuidad del negocio.

PAV -Visión
Es la medida de la cualidad de la vision de la Administración para aplicar de forma integral las mejores tecnologías disponibles.

PCN -Recursos
Existencia del conjunto de capacidades y recursos que posibilitan la continuidad del negocio en caso de ataque o desastre.

PAM - Madurez
Es la medida del grado en que la organización utiliza sus políticas y recursos de modo oportuno y sostenible en esta área.

AA1 Actitud

Esta área evalúa una cualidad, la actitud, que es la "disposición manifestada de algún modo" (RAE), de la administración tributaria. Se evalúa el compromiso institucional con la continuidad de negocio, lo que ha sido dispuesto, **manifestado**, comprometido mediante políticas documentadas en planes, lineamientos y en prácticas consolidadas que institucionalizan las mejores prácticas, etc.

Se estudian:

- Los planes institucionales, documentos de objetivos, lineamientos, etc.
- La **cultura organizacional** explícita, la expresada, la disposición enfocada a la **resiliencia**, lo que incluye una actitud adecuada en la gestión de la seguridad y en lo referente a la trazabilidad de los datos.

AA2 Visión

En esta área se valora la "**profundidad**" o el "**alcance**" de la visión sobre cuál es el problema real y sus medidas de mitigación posibles.

La actuación de la Administración debe partir de la existencia de ideas claras y distintas entre sí sobre el desafío que implica garantizar la continuidad de negocio. Se debe exigir a los responsables de la continuidad del negocio, en resumen, a la Alta Dirección, mucho más que un enfoque superficial, acciones cosméticas y una delegación imprecisa de responsabilidades. No es suficiente cubrir las apariencias ni identificar de forma ingenua la continuidad con la seguridad. Hay que enfrentar los desagradables problemas y las duras decisiones necesarias para garantizar la continuidad.

La estrategia debe basarse en el conocimiento, en una idea **comprehensiva** de las muchas facetas que encierra el problema. La estrategia debe ser **profunda** en el sentido de que debe orientarse a lo esencial y no limitarse a causar "efectos de superficie". La estrategia debe ser oportuna, resiliente, completa y profunda. Entre sus componentes se encuentran aspectos técnicos, como el grado en que se ha implementado o está previsto incrementar técnicas avanzadas como *Zero Data Loss* o *Zero Trust*, pero debe exceder lo técnico.

Para evaluar la visión hay que cuantificar la brecha existente entre la comprensión del problema que tiene la administración y la que recomienda el estado del arte y por otra ver el grado de cobertura de todos los aspectos relacionados con el mantenimiento de la continuidad del negocio.

AA3 Recursos

En esta área se evalúa la **existencia actual** del conjunto de capacidades y medios financieros, tecnológicos, personales, organizativos y jurídicos necesarios para el buen fin de la estrategia. Estos recursos son habilitadores (en: *enablers*) de la resiliencia. Evaluándolos se alcanza conocimiento sobre las carencias existentes.

El objetivo final en la evaluación en esta área consiste en discernir si los recursos asignados son suficientes y si lo son valorar la asignación, efectiva o no, y su alineamiento con la visión.

Se estudian cuatro tipos de aspectos habilitantes, aunque son desglosados en siete indicadores:

- **Procesos Institucionales y sus productos.** Se valora de modo integral el marco organizativo y normativo.
- **Recursos de Infraestructura.** El objetivo no es la cuantificación ni la mera comparación, sino apreciar el grado en que los recursos asignados permiten, o no, a la administración el despliegue de su visión.
- **Recursos Humanos y Organizativos.** Se valora la asignación de recursos humanos capacitados, debidamente especializados en las áreas necesarias y comprometidos con el resultado.
- **Recursos financieros.** Para mantener la infraestructura, los medios y la formación adecuados.

AA4 Madurez

En esta área se valora el grado en que la organización ha aplicado y aplica sus recursos para el cumplimiento de sus políticas, de forma **sostenible** y con ello la madurez alcanzada. Se distinguen tres niveles: emergente, en progreso y establecido, descritos en la *Figura 2*.

Figura 2. **Niveles de madurez**

Emergente. Describe un estadio inicial de una práctica. En esta fase, el impulso de usuarios proactivos, muy frecuentemente destinados en IT, impulsa soluciones locales. Se dispone de copias de seguridad, de planes genéricos que son más bien declaraciones estandarizadas y se ha adquirido parte de la tecnología necesaria para evitar intrusiones y hacking.

En progreso. Describe la situación en que existe una política tecnológica y presupuestaria orientada a prevenir los riesgos y garantizar la continuidad del negocio. Se ha avanzado en el establecimiento de centros de respaldo, la normativa cubre aspectos fundamentales y se mantiene proactivamente con el esfuerzo de equipos con roles asignados. Existe una confianza razonable en que los servicios puedan ser restaurados en los plazos acordados de Nivel de Servicio, salvo causa de fuerza mayor.

Establecido. La organización es resiliente. Se dispone de sistemas documentados corporativos estables, utilizados masivamente, con control de versiones que se perfeccionan progresivamente y una planificación robusta. Se ha superado la mera prevención de los riesgos de Tecnología y se ha construido un modelo para garantizar la continuidad del negocio. Existe una organización que dispone de recursos suficientes.

Para evaluar estas circunstancias se tienen en cuenta tres indicadores:

- **Cobertura.** Mide el grado en se cubren sistémicamente los aspectos necesarios, pues existen áreas en que la debilidad de un elemento compromete todo o solamente un subsistema.

- **Pruebas y comunicación.** Las estrategias y los planes deben ser aplicados, los sistemas probados y el personal entrenado. Solo mediante la práctica continuada los elementos dispuestos, pasan de ser subsistemas "*a la vista*" a sistemas "*eficazmente implantados*".
- **Gestión.** PCN impulsa una gestión *cuantitativa* de la mejora.

2.3. Beneficios de implantar un plan de continuidad de negocio

Aunque parezca una tautología el beneficio de la Continuidad del Negocio es que continúe. Los administrativistas destacan que uno de los objetivos esenciales del Estado es "permanecer" a diferencia de los negocios particulares que desde su concepción tienen un horizonte de extinción, a veces deseado e impulsado, en la forma de absorciones o ventas. Frente al responsable de continuidad de negocio en una empresa, al que se le podría reprochar, en su caso, la omisión de la debida diligencia, al responsable de la continuidad de una administración tributaria se le podría reprochar el incumplimiento de un deber inexcusable.

3. Estructura y método de la guía

La **guía** propone seguir el ciclo de vida PDCA (Planear-Hacer-Verificar-Actuar) en cuatro etapas para implementar un PCN: entender la organización; determinar las estrategias; desarrollar e implementar las respuestas; y probar, mantener y revisar.

La **guía** que se presenta se centra en la primera fase "Planear", pues su objeto es proponer normas para realizar un Plan. Ni es un manual que desarrolle aspectos tecnológicos de la continuidad ni es una guía de auditoría ni de gestión ni un procedimiento para evaluar la madurez.

La **guía** dirige y acompaña en los siguientes **procesos**:

1. Evaluación

Se realiza mediante el cuestionario que figura en el Anexo 1.

a. Se utiliza el método de autoevaluación, a diferencia de TADAT, ofreciendo el contexto que permite a los interesados ajustar sus respuestas, pero sin exigir evidencias auditables.

b. Tras la cumplimentación del cuestionario es posible obtener una calificación por áreas de actividad.

c. Con ello el usuario dispone de cuantificación de los atributos de la situación AS IS.

2. Consideración

Etimológicamente el término considerar es examinar mediante la observación el cielo nocturno local, y en él los *sidus*, de los astros visibles. Para una administración tributaria no es relevante considerar la mejor práctica de continuidad, por ejemplo, de Microsoft en Azure, ni siquiera cómo se comporta otra administración tributaria como el IRS con distinto tamaño y necesidades. Debe examinar lo que es propio y común con sus vecinos. Para ello:

a. El interesado parte de su autoevaluación. Para cada indicador compara su situación con lo deseable, que es la calificación A contenida en el cuestionario, que está calibrada para las administraciones tributarias regionales.

b. Ello le permite comparar su situación con la situación deseable TO BE.

c. Tras considerar la diferencia entre ambas debe realizar un análisis de las diferencias, esto es un GAP Análisis y luego utilizar la **guía** para diseñar un plan de mejora.

3. Diseño

El interesado diseñará un plan en el que se detallen las tareas priorizadas.

4. Gestión

Las actividades concebidas deben ser priorizadas, deben buscarse los recursos humanos y financieros y ordenadas en el tiempo. Esto implica materializar sucesivos Planes de Actuaciones para remediar las debilidades observadas.

El proceso y sus fases se detallan en el *Capítulo 6*.

3.1. Materiales y documentación de soporte

El núcleo de la **guía** es un cuestionario de autoevaluación, incluido en el Anexo, que versa sobre las cuatro *áreas de actividad (AA)*, que está precedido en la Sección 3.2 por materiales, donde a modo de manual se:

- Explica la lógica subyacente en la metodología.
- Proporciona el contexto para responder al cuestionario y pretende ofrecer información útil al analista y a los responsables de implantar el Plan de Continuidad de Negocio.
- Desambigua los términos contenidos en el cuestionario.
- Aporta las referencias sobre las metodologías utilizadas en las mejores prácticas.

En cada una de las cuatro Áreas de Actividad se han identificado un conjunto de *indicadores de esfuerzo (IE)*. En cada uno de ellos la evaluación cuantificará en una escala cualitativa (del tipo Likert) lo estudiado.

En otros términos

Se analizan áreas de actividad [4] mediante indicadores. Con ello se establece un paralelo con TADAT que, para cada una de sus Áreas de Resultado de desempeño, utiliza un conjunto de "indicadores de alto nivel y relevancia crítica". Mientras que en ese caso se evalúa el desempeño mediante 28 indicadores, en este caso se utilizan 17 para evaluar la actividad orientada a garantizar la continuidad del negocio como se muestra en la *Tabla 1*. Mientras que en TADAT se cuantifica la puntuación utilizando *dimensiones*, en este caso, por analogía se utilizan factores. Se trata de los requisitos que deben ser satisfechos para obtener una cierta calificación del indicador que los incluye, como se aprecia en el cuestionario que figura en el *Anexo*.

El objetivo final se resumirá en cuadros de datos con las calificaciones y gráficos.

Tabla 1. Áreas e indicadores

Área	Indicadores	
1. ACTITUD	1.1.	Liderazgo y Normas
	1.2.	Planes
	1.3.	Actividades
2. VISIÓN	2.1.	Visión tecnológica
	2.2.	Visión organizativa y procedimental
	2.3.	Gestión del riesgo
3. RECURSOS	3.1.	Marco organizativo
	3.2.	Infraestructuras
	3.3.	Salvaguarda de la información
	3.4.	Servicios de terceros
	3.5.	Infraestructura TI (Hardware, Software y comunicaciones) - Alta disponibilidad
	3.6.	Gestión de la seguridad y respuesta ante ciberincidentes
	3.7.	Recursos Humanos
	3.8.	Precariedad
4. MADUREZ	4.1.	Cobertura
	4.2.	Pruebas
	4.3.	Gestión cuantitativa

Se pretende que el cuestionario sea completado en modo de autoevaluación. La decisión, que ofrece la ventaja de la simplicidad, encierra el inconveniente de que no exige evidencia ni la participación de un experto en el método. Para facilitar que los resultados sean comparables entre países se incluyen materiales explicativos del alcance en el *Capítulo 4*.

4. Área que analiza la metodología

4.1. Actitud

Propósito central de la evaluación del área

Se quiere evaluar:

a) **La disposición manifestada** por la AT en relación con la continuidad de negocio. Se quiere evaluar hasta qué punto las buenas intenciones que se han manifestado, haciéndolas con ello exigibles, se han concretado en realidades observables, tangibles.

b) **Si las políticas de continuidad son explícitas y públicas** o meramente se asume que existen.

El cuestionario interroga para calificar tres indicadores:

- Liderazgo y normas
- Planes
- Acciones y actividades

La **lógica subyacente** es que sólo si la Dirección es consciente del problema de la continuidad, si tiene la actitud adecuada frente al desafío, si asume esa carga con decisión y responsabilidad y vela por su mitigación creando estructuras eficaces y dictando normas publicitadas de obligado cumplimiento, el personal de la organización comprometerá esfuerzos y recursos y realizará acciones que reportará a la Dirección, cerrando un círculo virtuoso de calidad.

Liderazgo y normas

El indicador 1.1 (Liderazgo y normas) pregunta por un amplio número de cuestiones: si existe un PCN con responsables, si existe una norma que identifique a los componentes del Comité de Crisis, si están definidas para cada caso las actividades esenciales que deben tener continuidad junto con las métricas que permiten saber si se cumplen o no los objetivos de continuidad, así como si existe una unidad de auditoría que valide la información.

Liderazgo. La norma ISO 22301 requiere que el «Plan de continuidad del negocio» esté liderado por la alta dirección que: *"Asegura los recursos adecuados, establece la política y nombra las personas para implementar y mantener la gestión de la continuidad del negocio"*.

La metodología de la **guía** pide algo más, que el Comité de Dirección asuma el problema no de una forma ambigua y genérica sino **personal**, que uno de sus miembros asuma el problema. Por esta razón para obtener la cualificación A, el factor 1.1.1 requiere en su letra b) este requisito.

- **Normas.** Se distinguen dos tipos:
  - *Organizativas.* Se busca conocer si incluyen la regulación de la composición y competencias del Comité de Crisis o de una figura organizativa similar.
  - *De procedimiento.* Se busca conocer si los procedimientos están reglados y existen normas escritas difundidas y accesibles que establezcan cómo responder a eventos, escalar decisiones y asignar competencias, incluyendo la activación del personal de respaldo. Se concede relevancia singular a estos en el factor 1.1.2.

Se pregunta y se invita a verificar la existencia de:

- **Una autoridad con competencias globales.** Se busca conocer, repetimos por hacerlo más explícito, si existe en el más alto nivel de la organización, no en Informática, una autoridad que entre sus misiones tenga la de asegurar la continuidad del negocio, que exista un plan y que se hayan delegado responsabilidades concretas para que el plan se mantenga y que se realicen las actividades necesarias.
- **Procedimientos aprobados.** Se cuenta que cuando, después de una batalla, los mariscales felicitaron a Napoleón por la rapidez de sus decisiones, les contestó que él no pensaba rápido, sino que pensaba antes. El objetivo del factor 1.1.2 es evaluar hasta qué punto la organización es previsora y, al menos en los aspectos básicos, dispone de procedimientos ya aprobados, para que el Comité de Crisis puedan tomar decisiones directamente.

Planes

Se pretende evaluar en el indicador 1.2 si los planes existentes cubren todo lo necesario para garantizar la continuidad del negocio y ello exige mucho más que la apertura de las oficinas, la presencia parcial del personal y el funcionamiento de la informática. Se ha incluido un solo factor (1.2.1 Actuaciones). Incluyendo las que tienen un objetivo externo y una interno.

La lógica que subyace es que se debe haber actuado previamente a las crisis, disponer de planes de acción y normas en todas las áreas (Gestión, Recaudación, etc.) y entre ellas, muchas veces descuidada, el Servicio Jurídico, pues en los momentos de crisis es posible que se deban tomar decisiones que, no por ser extraordinarios, deben dejar de estar bajo la más estricta legalidad.

Se debe verificar si hay planes **escritos y actualizados** para:

- Garantizar la seguridad del personal y la actividad de los contribuyentes.
- Asegurar la provisión continua y sostenible de los servicios críticos y los que establezca el Gobierno bajo emergencia, en un nivel aceptable.
- Brindar apoyo a una amplia gama de contribuyentes para sus relaciones en tiempos de crisis ya que estarán más afectados que la propia Administración.
- Disponer de procesos de toma de decisiones claros y oportunos en un entorno que cambia rápidamente, con estados futuros inciertos y en ausencia parcial del personal con competencia para dictarlos.
- Disponer de canales de comunicación claros y oportunos con los contribuyentes y el personal.

La bibliografía en la materia es muy extensa y en ella se denominan y describen muchos posibles planes. Cada metodología concede más importancia a unos frente a otros y los nombres varían. Entre ellos, sea cual sea su denominación, son muy relevantes, incluso imprescindibles:

- **Plan de continuidad del negocio (BCP):** un BCP es un plan detallado, pero de alcance y contenido amplio que describe los pasos que una organización tomará para volver a las funciones comerciales normales en caso de un desastre.
- **Planes de recuperación ante desastres (DRP):** de naturaleza más detallada que los BCP, los planes de recuperación ante desastres consisten en planes de contingencia sobre cómo las empresas protegerán específicamente sus sistemas de TI y datos críticos durante una interrupción debida a causas concretas como interrupciones masivas, desastres naturales, ataques de *ransomware y malware*, y muchos otros.

La **guía** no concede importancia a las denominaciones, sino que busca valorar si caso de suceder una crisis habrá que improvisar o no.

Acciones y actividades

En el indicador 1.3 distinguimos tres tipos de actividades:

- Redacción y actualización de normas y procedimientos.
- Capacitación y motivación.
- Certificación

Puede interesar en algunos casos certificar al personal o exigir a los consultores certificaciones[1]. El coste de obtenerlas oscila entre 500$ y 3.000$ y en la mayoría de los casos se requiere asistir a costes de formación. El examen en la norma ISO es de los más económicos.

La lógica subyacente es que hay que evaluar no solo las buenas intenciones, las normas y los planes sino la praxis y el conocimiento que la hace transformadora.

Ideas

El objetivo de este apartado es resumir noticias relativas a esta materia que hayan sido publicadas recientemente y que muestren las tendencias hoy existentes:

1. BCI[2] ha encontrado que, después de la pandemia, el 37,3% de los encuestados afirmó que se había creado y ocupado en su organización un rol, a nivel de junta directiva, responsable de promover y coordinar los esfuerzos de resiliencia. La *resiliencia operativa* ahora está regulada o se está regulando en muchas jurisdicciones para garantizar que los asuntos relacionados con la Continuidad se informen al *Director de Operaciones*. Incluso se ha nombrado "*Jefe de Resiliencia*", a un miembro definido de la junta directiva (CEO, COO o CRO) en algunos casos.
2. Tras el desarrollo de nuevas formas de trabajo, en parte estimuladas por la pandemia, alrededor del 96,7% de las organizaciones informan que "al menos parte del personal" ahora espera tener flexibilidad para trabajar desde casa durante parte del tiempo. Para aquellas organizaciones que introdujeron medidas durante la pandemia para aumentar la resiliencia y el trabajo ágil, estas incluyeron la instalación de

1 Certificate of the Business Continuity Institute 2. Certified Business Continuity Professional 3. ISO 22301 Certified Business Continuity Manager (CBCM) https://www.certifiedinfosec.com/services/certification-programs/22301-certifications/certified-iso-22301-business-continuity-manager. EC-Council Disaster Recovery Professional (EDRP)5. Certified Disaster Recovery Engineer (CDRE)6. Business Continuity and Resiliency Professional (BCRP)7. Certified Business Resilience Manager.

2 BCI launches Continuity & Resilience Report 2022.

fuentes de energía ininterrumpida en las oficinas en el hogar, pero también *tener centros más pequeños en todo el país donde los trabajadores puedan trabajar en un entorno de oficina si es necesario*.

3. Se ha encontrado que *es más probable que las habilidades sociales se prioricen frente a las calificaciones académicas* en el proceso de entrevista para un rol de Business Continuity y resiliencia. Ante un desastre total saber no hace daño, pero lo importante es resistir y motivar.

4. Al analizar los cambios en el sector durante los próximos cinco años, los encuestados sintieron que el cambio más probable era una mayor atención de la alta dirección a la continuidad y resiliencia del negocio, y el 88,3% creía que esto sería de "mucha más" o "más" importancia.

4.2. Visión

Propósito central de la evaluación del área

Existen estrategias en las que se privilegia la visión de nicho. Hay que hacer una cosa simple, hacerla bien y cumplir lo prometido. Basta con eso. Se hizo famosa la estrategia de las patatas fritas Lay en Estados Unidos. Freían buenas patatas y las transportaban a tiempo, incluso durante los huracanes, porque definieron así su misión. Existen otras actividades como la educación escolar en las que el objetivo es mucho más complejo y lo más importante no es que el alumnado memorice el libro y los maestros sean puntuales. La visión de lo que es la educación debe ser más amplia y la estrategia de una organización educativa más sutil.

En materia de Continuidad de Negocio en las AT también existen **visiones de nicho** y **visiones amplias**. Existen distintos grados de perfección en la comprensión de en qué consiste la continuidad de negocio y en el alcance concedido al contenido de la palabra "negocio". Puede además existir el error de definir mal, quién es el máximo responsable de la continuidad (que no es el responsable TIC). Este es responsable de que funcionen las TIC, pero no de que funcione la Administración Tributaria durante y después de una crisis.

Se puede concebir la continuidad, con visión de nicho tecnológico, literalmente, como término opuesto a la discontinuidad. Si es el caso, el problema queda reducido a prevenir interrupciones. Una forma más acertada consiste en aceptar que la continuidad no se altera por interrupciones sino por **acontecimientos**, por crisis, por lo que lo que hay que prevenir no es una detención, sino la ruina.

La metodología de la guía busca determinar en esta área si existe una adecuada **visión del problema**. Parafraseando a M.L King si alguien: "Ha tenido un sueño". La visión de la **guía** quiere ser amplia. En un

momento de crisis lo que hay que defender es al tejido económico y la recaudación del Estado. Es lo que se invita a visualizar y a observar en la consideración de tres indicadores. Son los de:

- Visión tecnológica
- Visión organizativa y procedimental
- Gestión de riesgo

Hace pocos años la mayor parte de la bibliografía sobre continuidad de negocio analizaba exhaustivamente los costes económicos y de reputación asociados a las caídas de IT, de las interrupciones, debatiendo sin límite sobre técnicas para pasar del 99,8% al 99,99% de nivel de servicio y los costes y beneficios asociados. Era una visión focalizada en TI, estrecha. Como consecuencia de la pandemia del COVID-19 el mundo cambió. Muchas organizaciones se han replanteado radicalmente su **estrategia de resiliencia** e incluso se han parado a pensar en qué consiste el término. Han ampliado su visión, conscientes de que se pueden dar situaciones en las que lo que esté comprometido sea la supervivencia.

Los elementos que deben ser considerados para evaluar la calidad de una visión son muchos, pues la visión será tanto más completa cuantos más elementos de la actividad abarque:

Periodo de tiempo. Tradicionalmente los analistas realizan estudios sobre los efectos económicos y reputacionales de interrupciones del servicio derivadas de eventos de duración limitada, horas y en el peor de los casos días, como las derivadas de los huracanes. Ahora el "*time frame*" en el que es necesario garantizar la resiliencia y gestionar una situación compleja es mucho mayor y puede ser de años.

Personal. Antes se prestaba atención a la seguridad de los responsables de sistemas para evitar un ataque y se diseñaban controles de acceso a los CPD con verificación de retina. Ahora el problema es garantizar el servicio con docenas o centenares de bajas.

Identificación de procesos críticos. Como consecuencia de los nuevos intervalos de riesgo, procesos que no eran críticos ahora pasan a serlo. Administraciones como la de Australia han creado **unidades para auxiliar a los contribuyentes y literalmente ayudarles a que sus negocios sobrevivan** en un entorno radicalmente alterado. La misión crítica puede llegar a ser salvar al contribuyente.

Escenarios de riesgo concatenado. Aparecen no solo nuevos riesgos asociados a las medidas paliativas como el trabajo remoto, sino que hay que pensar en "plagas sucesivas", tragedias naturales seguidas de epidemias, aprovechadas por ciberdelincuentes. En resumen, hay que planificar la resiliencia frente a combinaciones de problemas.

Objetivo de la estrategia. Hace unos años era la vuelta a casa (*on premises*) y retorno a la normalidad. El nuevo paradigma tiene que considerar opciones (en la nube) para cuando no sea posible el retorno y el retorno a la nueva normalidad.

Externalización frágil. El escenario actual hace plausible la existencia de fallos sistémicos en los que hasta los proveedores se vean **sistémicamente** afectados.

Doble capacitación del personal. No solo la tecnología debe tener back-up sino también el personal. Debería ser entrenado de forma dual para, apoyado en la documentación, poder prestar flexiblemente más de una tarea. La estrategia no es que exista personal duplicado en un lugar, sino que existan dos personas que sepan hacer dos cosas, al menos durante la situación de emergencia, de modo que se respalden.

Coordinación y liderazgo superior. Se han creado en ocasiones **jefes de resiliencia**.

Esquema de alerta o advertencia. Algunas organizaciones han establecido niveles de alerta, que activan progresivamente los recursos.

Comunicación. Interna y externa.

Esta metodología concede especial importancia a una **visión iluminadora**. Los filósofos diferencian el futuro, lo que inevitablemente sucederá como la muerte de todos y cada uno, del acontecimiento, en el que surge la novedad. El responsable de la Continuidad de Negocio **debe abrir a los ojos no a lo inexorable sino a lo venidero**. El verbo alemán *verhoffen* recoge este sentido. Se debe esperar *hoffen* como el perro del cazador, bebiendo el viento para saber qué dirección tomar. Nadie podía pensar hace años en una crisis derivada de un virus respiratorio. Muy pocas personas están pensando hoy en lo que será la siguiente crisis. Solo sabemos una cosa, que no será igual. Con este indicador se quiere evaluar hasta qué punto la visión impulsa **la innovación de tecnologías y métodos**, si hace todo lo posible para estar preparada.

Desarrollamos a continuación los indicadores.

Visión tecnológica

Los enfoques tradicionales, orientados a controlar las interrupciones, ponían una especial atención en los mecanismos de back-up y en la creación de infraestructuras robustas en entornos fuertemente centralizados. Se trataba de enfoques pasivos frente al tipo de incidencias: “algo se rompió o se quemó”.

La situación ha cambiado radicalmente y hoy en día es necesario invertir, además, en nuevas tecnologías por el motivo de que los problemas son más arduos, porque la tecnología es más compleja y porque existen ataques contra los intereses vitales de un Estado por múltiples motivos, que utilizan tecnología.

Se evalúa en el cuestionario tanto si existe innovación tecnológica 2.1.1, como procedimental, metodológica, 2.1.2 pues si el problema es cambiante las herramientas y los procedimientos deben cambiar.

Algunas de las herramientas tecnológicas en las que es posible invertir son: a) Herramientas automatizadas de gestión de la seguridad de datos; b) Back up en la nube; c) Servicios de recuperación de desastres basados en la nube; d) Virtual Machine Back up; e) and Recovery; e) Software para la planificación del BCP, etc.

Por lo que se refiere al segundo aspecto, se evalúa hasta qué punto existe un compromiso constante de actualización, de adecuación a las mejores prácticas, de imaginar con persistencia un futuro mejor, hasta qué punto no solo los técnicos, sino también los gestores se preparan para lo inesperado.

Visión organizativa y procedimental

La **guía** trata aquí dos aspectos culturales mediante dos factores, la **cultura orientada a la resiliencia** (2.2.1) y la **cultura orientada al servicio** (2.2.2), incluso después de una crisis y se pregunta si la AT tiene estos atributos.

Atendemos al primer factor. El concepto de resiliencia, que primero tuvo un contenido en la Física de los materiales se trasladó al ámbito de las ciencias sociales, primero en Psicología y luego a la Economía y las ciencias medioambientales. Después del éxito de la obra de James Rifkin “La era de la resiliencia”, ha cobrado tal difusión, que en el año 2020 fue una de las candidatas a “Palabra del año”. No es de extrañar que se aplique también en nuestro ámbito y que las normas de referencia contengan el concepto.

La palabra resiliencia en su origen tuvo dos acepciones:

- Capacidad de adaptación de un ser vivo frente a un agente perturbador o un estado o situación adversos.
- Capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido.

Apreciamos que para nuestro ámbito no son acepciones muy buenas porque, ni una AT es un ser vivo, ni es cierto que el objetivo después de un desastre deba ser estar igual de mal que como estábamos antes. En la

concepción de la **guía**, tras una crisis no hay que volver a donde se estaba, sino llegar a donde se deba estar, porque el estado de las cosas, el contexto, cambia durante la crisis.

La norma ISO 22316:2017 define la resiliencia organizacional como: *"La capacidad de una organización para absorber y adaptarse en un entorno cambiante que le permita cumplir sus objetivos y sobrevivir y prosperar".* ITIL 4 la define como: *"La capacidad de una organización para anticipar, prepararse, responder y adaptarse tanto a los cambios incrementales como a las interrupciones repentinas desde una perspectiva externa"*.

La resiliencia no debe considerarse como un atributo, al modo del "coeficiente de elasticidad", ni como la dureza, ni como la capacidad de absorber y disipar la energía de un impacto, ni como la estatura. **La resiliencia no es un "ser" ni un "estar" sino un hacerse**, un devenir resiliente. La resiliencia, como la cultura o como la resistencia en carrera surge de un proceso. El ciclo de vida de la resiliencia incluye un punto de vista adecuado, desde una visión adecuada, y un enfoque estructurado, un método, para establecer y mantener una organización resiliente. Una estrategia de resiliencia debe estar alineada con el liderazgo y alinearse con estándares como ISO22301, NFPA1600, ITIL, NIST.

En el indicador 2.2.1 la **guía** valora los elementos hasta ahora tratados, indicadores, normas, planes, la comunicación, los estándares, que se deben diseñar teniendo en cuenta el concepto de resiliencia, en el sentido de la norma ISO citada.

Hay que tener en cuenta que después del COVID-19 la cultura del trabajo cambió, se ha impuesto el trabajo a distancia junto con otras expectativas **y que la organización debe encontrar un punto nuevo de equilibrio**, incorporando la tecnología necesaria para soportarla y nuevas normas, muy especialmente las relativas a seguridad. ¿Cómo debe ser la organización para poder asimilar de manera flexible formas de trabajo **impuestas externamente por una crisis**? Solo con una organización de este tipo se reaccionará bien en circunstancias inesperadas.

Ahora bien, después de un desastre natural, por más que se recupere el suministro de agua y de electricidad, la predisposición a pagar impuestos (más allá de la capacidad) ha variado. La comunicación con el contribuyente debe restablecerse en cada caso en el nuevo contexto. **¿Cómo crear una organización que mantenga una relación resiliente con el ciudadano?**

Se aborda en este indicador más el aspecto cultural que el técnico, más el organizacional que el de los activos. Hay que tener en cuenta el impacto traumático de los desastres pues generan cambios físicos y psicológicos en personas **insustituibles**.

Hoy hay que pensar además en la **ciber resiliencia** y esto implica nuevas estrategias. Cada vez existen más intercambios de información en un devenir imparable. Se deben crear arquitecturas que mitiguen el riesgo de propagación de código malicioso en los centros de datos de recuperación. Para lograrlo, la resiliencia cibernética incorpora tecnologías de replicación avanzadas y bóvedas de datos cibernéticos aisladas para proteger los datos críticos. A las técnicas tradicionales hay que añadir – *Air-gapped storage* (Copias inmutables de datos críticos) y "*End point recovery solutions*". No debe olvidar el planificador que los futuros ataques utilizarán Inteligencia Artificial.

El segundo de los factores estudiado es la atención concedida al contribuyente (Política de ingresos) y al ciudadano (Política de gastos). La evolución de la tecnología hace que los ciudadanos dependan de una infraestructura tecnológica, que, en el caso de fallar, arrastra efectos en cadena. Mientras que en un modelo tradicional bastaba con mantener las oficinas abiertas al público, hoy en día en que la interacción se realiza a través de plataformas, es posible que el ciudadano, aunque quiera no pueda o que se vea afectado por efectos en cadena y necesite acogerse a medidas paliativas extraordinarias, para cuyo disfrute deberá ser auxiliado.

Gestión de riesgos

Muchas definiciones del concepto de riesgo son defectuosas. Por ejemplo, la que dice: *"[Riesgo es] una probabilidad o amenaza de daño, lesión, pérdida o cualquier otro suceso negativo causado por vulnerabilidades externas o internas, y que puede evitarse mediante una acción preventiva"*[3].

El riesgo es un **estado de cosas** en el que existe la **posibilidad** de que un suceso cause un impacto negativo. Su acaecimiento puede ser estimado en ocasiones. Existen casos como los juegos de azar en que es posible su cálculo usando la probabilidad. En otros no. Es bien conocida la distinción que Keynes estableció en su tesis doctoral entre probabilidad e **incertidumbre**. Pudiera ocurrir que cayera un meteorito y que sus efectos fueran la extinción de los caballos blancos. Como no podemos calcular los casos favorables entre los posibles, como dijo Keynes. "Simplemente no sabemos". El **responsable de continuidad es el guardián de la posibilidad y el gestor de muchas probabilidades**. Mediante su gestión se reduce la probabilidad de lo que es tal, se anticipa lo incierto y se mitigan los efectos de lo que sucede.

3 Fuente: ¿Qué es un riesgo? 10 definiciones de diferentes industrias y estándares https://www.stakeholdermap.com/risk/risk-definition.html

Entre las principales 10 definiciones de diferentes industrias y estándares[4], lo más común es definir el riesgo como el producto entre la probabilidad de ocurrencia de un hecho y el impacto que el mismo puede causar, lo que de nuevo es ilustrativo, pero filosóficamente impreciso.

La **gestión de riesgos**, según la **guía** ISO 73, es el conjunto de "actividades coordinadas para dirigir y controlar una organización en relación con el riesgo"[5]. La norma ISO 31000 define un marco y un proceso para ello.

La metodología que proponemos aborda cuatro actividades. Con ello nos alineamos con las prácticas de la industria (FFIEC, 2015): a) Análisis de Impacto; b) Valoración de los riesgos (en: *Risk Assessment*); c) Gestión de riesgo; d) Monitorización y prueba de las medidas paliativas.

Dijo Einstein que "**En tiempos de crisis la imaginación es más efectiva que el intelecto**" y en épocas como las actuales en que el cambio es muy rápido es importante verificar si los responsables imaginan las nuevas amenazas y ensayan nuevas formas de enfrentarlas, pues no existe para todo suceso amenazante estudio de la probabilidad asociada.

El responsable de un PCN no debe ser miedoso porque a las amenazas de objeto conocido hay que enfrentarlas reciamente. Ahora bien, no le perjudica ser **ansioso**, preocuparse por males no identificados, pues esto mueve a la acción. La seguridad total no existe, es algo imposible y la información, servicios y sistemas de cualquier organización siempre están expuestos a amenazas que pueden ser explotadas causando perjuicio en la misma. Muchas de ellas son en este momento inciertas o imprevisibles como fue el COVID -19 en 2018. Es por ello, que en la **guía** se singulariza el estudio de Análisis y Gestión de Riesgos, en el Área de "Visión", siendo algo fundamental y la base de una estrategia resiliente.

La **guía** presta atención a cuatro factores:

- **Identificación de los activos de la organización**

Decían los preceptores latinos: "Para comprender primero hay que atender". Mal planificaremos un remedio si no hemos identificado el riesgo y mal diseñaremos cómo enfrentarnos a dos si no sabemos cuál es el mal mayor. Mal podremos saber los daños lesiones o perdidas, si no sabemos cuáles son los objetos de nuestro interés y más aún si no reflexionamos sobre el hecho de que hay activos inmateriales de enorme valor, como

4 https://www.stakeholdermap.com/risk/risk-definition.html

5 Gestión de riesgos: un modelo de madurez basado en la norma ISO 31000. Disponible en: https://www.researchgate.net/publication/319218604_Risk_Management_A_Maturity_Model_Based_on_ISO_31000 [consultado el 29 de julio de 2024].

la reputación. Desde esta perspectiva el primer factor que se evalúa es hasta qué punto los activos materiales e inmateriales, relevantes, que se encuentran bajo amenaza han sido identificados.

- **Análisis de los riesgos**

El contenido actual del término tiene su origen en la Química, donde se utiliza para describir la descomposición de un compuesto en sus componentes elementales. De allí ha pasado a otras disciplinas como psicoanálisis con un contenido semántico opuesto al de síntesis. El **análisis de riesgos** es el proceso que permite a las organizaciones tener conciencia detallada y diferenciada de los riesgos y de sus componentes y de las consecuencias (impacto) que supondría su materialización. En base a este conocimiento preciso, se puede, a continuación, gestionarlos. Pongamos por ejemplo el riesgo de robo de datos a través de tercero colaborador. Se puede optar por reducir la probabilidad, que, además, suele ser muy baja de por sí, exigiendo medidas de seguridad, auditando los procesos y firmando penalizaciones leoninas. La estrategia alternativa consiste en analizar, desglosar los componentes y reducir el impacto esperable haciendo que el proveedor solo tenga unos datos básicos y una *password* que pueda ser anulada rápidamente. En cada caso hay que buscar la línea de acción más eficaz.

El análisis de riesgos es el proceso que permite a las organizaciones tener conciencia detallada y diferenciada de lo que es importante, descomponiendo la posibilidad en sus elementos constituyentes. Hay que comprender cuáles son las amenazas, las vulnerabilidades, jerarquizarlas, estimar la frecuencia y probabilidad de que sucedan dichas amenazas o calificar la incertidumbre existente y por último comprender las causas de los riesgos y de las vulnerabilidades.

A partir de este conocimiento preciso, se puede y debe llevar a cabo un proceso de gestión de los riesgos orientado a implantar las medidas (salvaguardas) que permitan el mantenimiento de un entorno controlad y con ello cumplir los acuerdos de nivel de servicio o compromisos existentes, modificando la degradación y/o la probabilidad del acontecimiento y en último término minimizando los riesgos hasta niveles aceptables.

- **Gestión de los riegos**

Se aborda su calidad en el indicador 2.3.3 en la que se investiga si “existe un ciclo de vida de la metodología”. Se pretende que el seguimiento de las medidas y salvaguardas propuestas se realice conforme al modelo PDCA u otro de gestión similar. Como sucede siempre, una cosa es que la AT gestione sus procesos y otra muy distinta que lo haga para bien, pues pudiera suceder que el proceso o el objetivo no fueran los adecuados. Si es el caso que la estrategia es la adecuada y la gestión correcta surge el éxito y la organización madura en vez de desintegrarse.

En la guía y para la totalidad de la Continuidad de Negocio se ha aplicado el concepto de madurez.

- **Profundidad de la visión**

En el cuestionario se intenta comprender en primer lugar si se evalúan todos los riesgos o la identificación es ingenua (letra a).

Es evidente que en la gestión de un riesgo hay distintos grados de perfección. Señalamos desde un primer momento en que es distinto "venir para verlo", para gestionarlo, que "verlo venir". Por eso se han incluido las preguntas del cuestionario referidas a este aspecto en el apartado "Visión".

La popularidad del concepto de Gestión de Riesgos ha venido acompañada por la difusión de sus herramientas conceptuales, entre ellas la "Matriz de Riesgos. Se trata de una idea simple que ha alcanzado gran difusión, quizás por ser tan simple. Antes de recomendar su uso recordamos la frase de Einstein cuando tuvo que explicar la gravedad como una deformación del espacio tiempo utilizando tensores. "La explicación de los fenómenos debe hacerse de modo tan simple como sea posible. Pero no más simple".

El uso de la matriz supone ordenar en una matriz de 3x3 o 4x4 o 5x5 los impactos de cada riesgo ordenados cualitativamente (Muy grave, grave, etc.) y en columnas la probabilidad (bien cualitativamente bien cuantitativamente). Como modo de ordenar el pensamiento tiene su utilidad. Su uso ingenuo nos lleva a una inmerecida autosatisfacción por asumir la idea evidente de lo que es muy probable y causa mucho impacto hay que atenderlo antes de lo que causa poco impacto y no suele suceder. ¡Claro que sí!

El problema surge cuando el sistema se utiliza, como sucede en muchos casos, para decidir inversiones o como en muchos casos para justificarlas una vez decididas con otros criterios. Por ejemplo ¿Cuál es el riesgo de que tengamos un problema de privacidad a través de un servicio prestado por un *third party*? ¿Cuál sería el impacto en términos económicos? ¿Cómo comparamos este riesgo con el de un deterioro de un rack de servidores del que no tengamos copia de seguridad? No es simple para los expertos: a) Obtener las probabilidades de riesgo y mucho menos la valoración de términos económicos de los impactos legales o reputacionales; b) Normalizar los valores en riesgos de muy distinta naturaleza.

No siendo repudiable en sí mismo, hay que denunciar que muchas organizaciones, por tener la presentación con la matriz en tres colores de una docena de grandes categorías, han gastado recursos valiosos en consultoría. Una máxima de organización alemana dice "Antes ser que parecer". Es mejor comprar antibióticos para la caja de las medicinas que un estuche de cuero.

La letra c) indaga si se ha realizado el esfuerzo de crear una matriz de riesgos que no sea trivial, **que haya sido minuciosamente creada** y que aporte a la organización un conocimiento que no tenía antes de realizarla.

Se indaga además para ver si se ha identificado para cada riesgo su **causa principal**. La mayoría de los fenómenos sociales y entre ellos muchos relacionados con la continuidad de negocio están **sobredeterminados**, suceden por una conjunción de causas. Frecuentemente se unen lo limitado de los presupuestos, las carencias de personal, las dificultades para realizar una formación adecuada en una combinación de efectos letales. No obstante, debe hacerse un esfuerzo por identificar la causa principal que se encuentra entre aquellas que amenazan a los requisitos que son necesarios.

Lecciones aprendidas

La pandemia de COVID-19 tuvo un impacto significativo en la gestión de riesgos, dejando patente su importancia y la necesidad de revisar los análisis existentes hasta el momento.

Según un informe de Deloitte, sólo el 49% de las empresas habían elaborado manuales pertinentes y realizado pruebas previas basadas en escenarios de emergencia relacionados con la pandemia. No es para reprocharlo, porque a nadie se le habría ocurrido, pero sí que es una lección para abrirnos a pensar en lo que no es inmediato. Su ansiedad, su visión había sido insuficiente.

Durante los últimos años se ha apreciado:

- Falta de conocimiento por parte de la alta dirección de los riesgos que **realmente** tiene y asume la organización. Los hindúes utilizaron para denominar un tipo de meditación el término sánscrito "*vipassana*", que significa "ver las cosas tal como son". El hecho de que la Alta Dirección no tenga conocimiento de los riesgos existentes o de que puede afirmar que no lo tiene, puede generar que no se proporcionen los recursos necesarios. Después de recordar lo peligroso que es "lo que no se conoce que no se conoce" hay que lograr que la Dirección conozca por interés suyo y de todos, el riesgo objetivo. El PCN debería ser un inductor del "**vipassana**".
- Falta de conocimiento y **visión de las dependencias entre los activos y servicios críticos**. El conocimiento debe versar sobre las causas, sobre la esencia y sobre las relaciones. Hay que evitar que se solventen las cosas parcialmente provocando otro incidente posterior, que el remedio sea peor que la enfermedad y que se tarde mucho más tiempo en solventar los incidentes ocurridos, por no tener presentes todos los aspectos implicados.
- **Falta de priorización y jerarquización de los servicios críticos.** Priorizar es algo fundamental cuando se tienen recursos y tiempo limitado, como sería el caso de un problema de continuidad. No tener claridad sobre qué aspectos priorizar, en qué invertir los recursos en caso de problemas de continuidad puede provocar dilatar la indisponibilidad durante un tiempo innecesario. Dicho lo anterior puede suceder

que un requisito crítico requiera otro de la misma naturaleza previamente activo. Por lo tanto, hay que determinar las prioridades de forma jerarquizada.

- **Falta de convenio entre los afectados.** Cada experto sabe de su negocio y aspectos que pueden parecer menos importantes para un área, pueden serlo para otras. Es por ello, que **consensuar**, escuchar y aceptar las opiniones de todos los afectados es algo determinante. Es fundamental que en la elaboración y propuesta del proceso de análisis y gestión de riesgos se incluyan representantes de todas las áreas de la organización. El diseño del PCN debe realizarse con ánimo amplio y visión amplia. Sin orejeras.
- **Falta de revisión del análisis y gestión de riesgos.** Los riesgos cambian rápidamente. Si no se revisa regularmente el análisis y gestión de riesgos, así como los planes y medidas implementadas la sensación de seguridad será falsa.

Estas deficiencias deben ser evitadas.

4.3. Recursos

Propósito central de la evaluación del área

El propósito de la Guía del CIAT en esta área es evaluar a) la suficiencia global, pues si los recursos son muy precarios cualquier impacto desestabilizará el sistema y b) evaluar en qué medida los recursos disponibles están orientados a la continuidad del negocio y son suficientes.

En esta Área se estudian ocho indicadores:

4.3.1. Marco organizativo

Propósito central en la evaluación del área

Etimológicamente la palabra organización tiene su origen en la palabra griega "*organon*" aquello con lo que se trabaja. En el ámbito de los sistemas de los organismos, un órgano es la estructura que realiza una función. En nuestro ámbito al referirnos al "marco organizativo" designamos el conjunto de elementos que hacen posible que se cumpla la función de continuidad de negocio.

Por ser un marco, el contenido del término incluye elementos inmateriales y otros materiales y entre estos últimos los personales. Se ha dicho que la organización es el factor que posibilita lograr un resultado

extraordinario mediante la colaboración de muchas personas que no lo son. De poco serviría una organización con una actitud extraordinaria y una visión profunda si no existieran entre sus recursos los humanos y organizativos que hacen posibles resultados extraordinarios, como lo es la continuidad del negocio en tiempos de crisis.

Para estudiar este marco se identifican los siguientes factores:

- Requisitos normativos y de buenas prácticas
- Recursos asignados al cumplimiento normativo
- Vigencia y transparencia de los planes
- Procedimientos de comunicación y coordinación con terceros

Requisitos normativos y de buenas prácticas

En áreas anteriores se ha tratado la existencia de normas y los planes. Aquí la Guía indaga más allá de si ha existido declaración expresa o no sobre los planes y se hayan elaborado normas.

En el apartado 3.1.1 se investiga si:

a) Existe una norma sobre el PCN y **una unidad organizativa con recursos para mantenerlo** y difundirlo, así como para realizar las tareas asociadas (Análisis de Impacto, Planes de Desastre o similares, etc.) Forman parte de ella las Normativas de Seguridad, la Política de Seguridad y las normas y procedimientos relativos a la materia. Lo fundamental aquí es saber si la Unidad tiene recursos para poder realizar su tarea y que normas y procedimientos no queden en letra muerta.

b) Se pregunta si existe una evaluación de *compliance* de la normativa en materia de Continuidad de Negocio realizada durante los dos últimos años. En ocasiones se realiza en coordinación con otras instituciones del Estado. Se pretende comprobar la **persistencia** en el propósito.

c) Existen **análisis** del cumplimiento o de la madurez en relación con algún estándar en materia de Continuidad de Negocio o con una norma externa de carácter nacional. Con ello se pretende verificar si existe una preocupación por el alineamiento con las normas internacionales y las mejores prácticas y si además de resumir la situación se ha realizado un análisis detallado.

d) **La Dirección** ha solicitado en el periodo de los dos últimos años o algún Comité de Seguridad u órgano **la ha informado** sobre los riesgos más graves existentes con propuesta de acciones de corrección. Con ello se pretende conocer el grado en que la Dirección conoce y por ello es partícipe de los riesgos asociados a la carencia de elementos necesarios para la continuidad del negocio. Se pretende averiguar si la Administración tiene como vigente el problema.

e) Existe alguna institución externa (oficial o contratada) que evalúe la calidad de la seguridad existente periódicamente. En las mejores prácticas existe una verificación externa de las evidencias.

Recursos asignados al cumplimiento normativo

La cuestión ahora es saber si se dispone de un recurso organizativo singular, de un área que tome el mando en caso de problemas. Se pretende evaluar si la AT ha aprobado formalmente el establecimiento de un Comité de Crisis (CC) y definido su composición y funciones. Se indaga sobre la existencia de "alguna estructura organizativa" (e.g.: Comité de Seguridad, de Continuidad de Negocio o similar) que se haya reunido al menos una vez al trimestre durante los dos últimos años e informado a Dirección. Las soluciones son tan diversas como las organizaciones, pero se busca la existencia de algo que pueda en rigor cumplir con una función rectora en materia de continuidad de negocio, y si existe documentación asociada a su funcionamiento (designación de participantes, convocatoria de reuniones, actas, etc.).

Vigencia y transparencia de los planes de emergencia

Con este factor se desea evaluar hasta qué punto el esfuerzo por garantizar la continuidad es una tarea en curso. Se evalúa si existe a) un esfuerzo para que normas y planes estén actualizados; b) si son transparentes) si las medidas se prueban; d) si las iniciativas se difunden, si son accesibles. Solo debería alcanzar la máxima calificación si esta cultura está presente.

Procedimientos de comunicación y coordinación con terceros

Se pretende evaluar si en el ámbito de la comunicación también existe una" tarea en curso", si en esta faceta se reacciona al cambio. Se averigua qué se ha hecho el último año.

Lecciones aprendidas

- **Es necesario preguntarse por el presupuesto posible y disponible.** El presupuesto dedicado a la seguridad varía dependiendo del tamaño de la organización, la tolerancia al riesgo y el sector de la Organización. **Históricamente los equipos de seguridad han tenido entre el 5% y el 7% del presupuesto de TI**, y esas cifras aumentan con la expansión del panorama de amenazas y la creciente complejidad de la seguridad. La revisión de la empresa *Vanta* en UK estimó una inversión media en seguridad del 9% del presupuesto de T.I. De esta cantidad un 6% se dedica a concienciar al personal. Algunos expertos recomiendan aumentar el gasto en seguridad organizacional entre un 10% y un 15%,

cubriendo programas de seguridad, cumplimiento y continuidad del negocio. Es razonable que la cifra oscile entre el 7% y el 10% del presupuesto de TI.

Se aprecia en los últimos años:

- **Aumento presupuestario:** Los presupuestos de ciberseguridad (2024) crecen globalmente a un ritmo del 6%. El ritmo es inferior al de años anteriores.
- **Aumento proporcional de los presupuestos de TI:** Los presupuestos de seguridad, como porcentaje de los presupuestos generales de TI, tienen una tendencia al alza, habiendo aumentado del 8,6 % al 11,6 % desde 2020 y siguen creciendo más en 2024.
- **Motivos del aumento presupuestario:** el 63% de los encuestados recibieron un aumento presupuestario y los ajustes anuales de rutina representan el 20% de los casos.
- **Dotación de personal y remuneración:** Los costes de personal y consultoría ascienden al 38% y son mayores el caso de que se operen en la nube.

Una pregunta relevante es: Si el gasto medio de seguridad en TI es del 7% de su presupuesto **¿Cuál debería ser el porcentaje del presupuesto de la AT que se asignase a la continuidad? La respuesta es difícil, pero mueve a impulsar que pongamos este gasto en relación con otros de la organización**.

- **Es necesario disponer de un Comité de Crisis y conveniente que un miembro de la Alta Dirección lo presida.** Debe estar claramente diferenciado del Comité de Seguridad sin perjuicio de que miembros de este participen en aquel. Es preciso Identificar a todos los interesados y afectados (*stakeholders*) internos y externos cuyas acciones u omisiones pueden generar la imposibilidad ante una crisis de ofrecer la solución planificada. Deben participar en el proceso de Planificación pues solo así pondrán de manifiesto los obstáculos existentes y actuarán coordinada y eficientemente en el caso necesario.

- **La voluntad de implantar principios de "Gobernanza" es insuficiente.** La gobernanza es el proceso de tomar y hacer cumplir decisiones dentro de una organización, Estado o sociedad. Es necesario que se tomen decisiones en materia de Continuidad de Negocio y que, llegado el caso, se ejecuten, pero es necesario además que sean las adecuadas: La Teoría de la Organización en la actualidad (Paton, 2019) destaca la importancia radical del aspecto organizativo. Las capacidades de resiliencia organizacional (OR) y de sostenibilidad organizacional (OS) tienen una importancia conocida desde antiguo (Ates y Bititci, U., 2015) pero actualmente se concede una especial importancia como principios inspiradores de un PCN de forma que se pueda responder a situaciones disruptivas adecuadamente (UN, 2015).

- **Unidades críticas.** Los modelos organizativos son muy variados ya que las necesidades son muy distintas en cada tipo de negocio. No son las mismas las necesidades de la Administración Tributaria que las de una Universidad o una empresa industrial. Existen ciertas estructuras que son necesarias en todo caso a los que para facilitar las consultas nombramos en inglés.

a. *Business Continuity Management (BCM) Steering Committee.* Es el grupo principal que adopta las decisiones en materia de Continuidad de Negocio. Aprueba y revisa la estrategia, Esta presidido por un miembro de la alta gerencia y en él están representados todas las áreas funcionales y de soporte principales. Autoriza el uso de recursos, desarrolla cronogramas y define responsabilidades para el programa BCM.

b. *Business Continuity Planning Team. Asume la dirección técnica.* Elige las metodologías y estándares y estudia las mejores prácticas. Sobre estas bases planifica e informa al Comité Director.

c. *Crisis Management Team (CMT)*. Solo actúa una vez declarada la crisis

d. *Emergency Response Team (ERT).* Se congrega en una crisis en cada oficina de la organización con el personal planificado o sus sustitutos, si es el caso.

4.3.2. Infraestructuras

Propósito central en la evaluación del área

A diferencia de otros indicadores, el actual no requiere de una amplia explicación. En cualquier Plan de Continuidad de Negocio global se deberá tener en cuenta la necesidad de mantener abiertas las oficinas, disponer de respaldo de personal imprescindible, información recuperable, etc. Dado el grado de digitalización alcanzado, el Centro de Proceso de Datos (CPD), supone un punto clave. Es por ello que este indicador se centra en la continuidad de las **infraestructuras físicas** relacionadas con el CPD.

Si bien no es frecuente, salvo por desastre natural una disrupción total y prolongada de un CPD, aunque la probabilidad sea baja, el impacto es muy elevado. El número de desastres naturales de todo tipo se ha multiplicado por cinco en los últimos 25 años y por diez en los últimos cien. Si se mantiene esta aceleración en el periodo entre este momento y el 2050 sufriremos diez veces más que en las últimas décadas lo que no deja de ser preocupante. Entre 2000 y 2019 se han contabilizado 7.000. No porfiamos en una predicción, pero parece razonable esperar en los próximos 15 años 30.000 desastres. Siendo cierto que no hay que ponerse en lo peor, lo que no hay duda es que hay que enfrentar incidentes, cuya frecuencia es mucho más alta.

A continuación, se muestran los principales tipos de incidentes producidos en los Centros de Proceso de Datos (CPD) en 2023, así como las causas de estos:

1. **Fallas de Hardware:** 25%. Estas incluyen fallos en componentes físicos como servidores, discos duros, y otros equipos críticos del CPD.

2. **Errores humanos:** 20%. Errores cometidos por el personal, ya sea por falta de capacitación, fallos en procedimientos operativos o decisiones incorrectas durante la gestión de sistemas. Se estima, además, que este tipo de errores va en aumento.
3. **Ciberataques:** 15%. Incidentes de seguridad cibernética como ataques de denegación de servicio (DDoS), *malware*, *ransomware* y otras amenazas que comprometen la disponibilidad y seguridad de los datos y servicios.
4. **Fallas de Software:** 15%. Problemas relacionados con el software, incluyendo *bugs*, fallos en actualizaciones, y errores en las aplicaciones que afectan el funcionamiento del CPD.
5. **Desastres naturales:** 10%. Eventos como terremotos, inundaciones, tormentas, y otros desastres que pueden dañar la infraestructura física del CPD y causar interrupciones prolongadas.
6. **Cortes de energía:** 8%. Interrupciones en el suministro eléctrico que afectan la operación continua del CPD, a menudo debido a problemas en la red eléctrica externa o fallos en los Sistemas de Alimentación Ininterrumpida (SAI). Este problema es sutil porque no es lo mismo una caída de minutos, que se alivia con la conexión de los SAI, que una más larga. Según los datos de *Uptime Institutes*, con una encuesta realizada a 850 CPDs, en 2023, el 55% de los CPD habían tenido al menos un *outage* en los últimos tres años. Suponía una mejora frente a las cifras reportadas de un 60% en 2022, 69% en 2021, y 78% en 2020. Estas paradas tienen un coste elevado. Al 54 % les supuso un impacto de más de $100,000. A un 16%, les supuso un coste de más de un millón de dólares. Estas cifras pueden ser utilizadas por quienes, con todas las prevenciones que señalamos, decidan calcular una matriz de riesgos.
7. **Problemas de red:** 5%. Fallos en la conectividad de red, incluyendo problemas con los *routers*, *switches*, o proveedores de servicios de internet que impiden la comunicación entre los sistemas.
8. **Mantenimiento planificado:** 2%. Paradas programadas para llevar a cabo tareas de mantenimiento, actualizaciones y mejoras en la infraestructura del CPD. Aunque planificadas, estas paradas pueden ocasionalmente extenderse más allá del tiempo previsto debido a problemas imprevistos.

Como puede observarse, más del 50% de los principales incidentes se corresponderían con problemas en las infraestructuras físicas.

La metodología de la **guía** considera varios factores

- Instalaciones de respaldo
- Suministros como corriente eléctrica
- Resiliencia de la infraestructura frente a desastres naturales
- Resiliencia de la infraestructura frente a ataques intencionados.

El factor 3.2.1 indaga por la existencia de las medidas más tradicionales en este área: El factor 3.2.2 indaga por la existencia de medidas de back up, el 3.2.3 por las medidas que previenen los desastres naturales y el 3.2.4 frente ataques vandálicos.

Lecciones aprendidas

Se enumeran recomendaciones encontradas en la bibliografía:

- **Instalación y mantenimiento de sistemas de protección eléctrica (SAI, grupos electrógenos).** Es más oportuno ser **proactivos** y anticipar **medidas que permitan** en su momento garantizar la continuidad que tener que ser **reactivos** por necesidad Se deberá disponer de **sistemas de protección eléctrica** que entren en funcionamiento en caso de caída. Pueden ser **Sistemas de Alimentación Ininterrumpida (SAI)**, los cuales entran en funcionamiento instantáneamente para garantizar la continuidad durante los primeros momentos, o grupos electrógenos, que requieren de un tiempo para ponerse en funcionamiento, pero permiten garantizar un mayor tiempo de continuidad.
- **Identificación e inventariado de los recursos alternativos, tales como compañías eléctricas y compañía de comunicaciones.** Este aspecto se encuadra en la relación con terceros proveedores. Algunos servicios dependen de terceros proveedores, tales como compañías eléctricas y de comunicaciones. En este caso hay que tener convenientemente identificados e inventariados los proveedores que suministran el servicio, el contrato de continuidad suscrito y los proveedores alternativos que podrían garantizar la continuidad en caso del proveedor principal. Debe definirse la estrategia de comunicación con los mismos y la de conmutación entre los diferentes proveedores si fuera necesaria.
- **Instalación, mantenimiento y monitorización de sistemas ambientales, sistemas de detección y extinción de incendios.** Se debe verificar regularmente el buen funcionamiento de los sistemas de detección temprana en caso de incidente de humedad, vertidos humo o incendios.
- Instalación de sistema de **control de accesos físico**. Es **imprescindible contar con seguridad física** que evite las intrusiones.
- **Instalación, mantenimiento y monitorización de circuitos de cámaras.** Deben existir **circuitos de cámaras monitorizados** ya que el objetivo es poder detectar si está ocurriendo algún incidente en el menor tiempo posible.
- **Personal de seguridad física.** Su actuación debe regirse por protocolos de manera que no tenga que improvisar y debe estar prevista la comunicación con otros Cuerpos y Fuerzas de seguridad del Estado.
- **Inventario básico para cubrir los servicios mínimos.** Se debe planificar con qué mínimo de activos se podría seguir dando el servicio. Se considerará personal, dependencias, equipos hardware y software.

- **Formación y concienciación.** Se requiere la **definición y pruebas periódicas de protocolos y planes de actuación ante incidentes**. Los protocolos deben priorizar la seguridad del personal y **dirigir al personal fuera de las instalaciones a lugares seguros**. Sus responsables **deben ser conocidos** y deben poder ser **fácilmente reconocibles**, por ejemplos con chalecos de colores, **disminuyendo el desconcierto**.
- **Sistemas o medios directos y periódicos de comunicación con centros de alertas medioambientales.** Es cada vez más importante para que la organización se pueda preparar ante un posible fenómeno extraordinario.
- **Garantizar que se cuenta con los medios necesarios para contactar con las personas involucradas.** Aun siendo este aspecto general en cualquier Plan de Continuidad de Negocio, se hace hincapié de que, en caso de contingencia total del CPD, es importante contar con los medios humanos que garanticen el servicio en el centro de respaldo, incluyendo traslados.

4.3.3. Salvaguarda de información

Propósito central en la evaluación del área

Los datos son un recurso imprescindible para el correcto funcionamiento de los procesos de negocio. El propósito general de la salvaguarda de información en un PCN es garantizar que los datos y la información siempre estén disponibles.

En general, los procedimientos de salvaguarda de información deben garantizar:

- **Disponibilidad.** Garantizar que la información esté accesible cuando se necesite, incluso durante un incidente en el que fallen los sistemas de información.
- **Integridad.** Asegurar que la información requerida para reaccionar en una crisis sea precisa y completa, evitando cualquier modificación no autorizada.
- **Confidencialidad.** Proteger la información sensible y confidencial contra accesos no autorizados.
- **Cumplimiento normativo.** Garantizar que la organización cumpla con la normativa aplicable relacionada con la protección de datos.

Principales riesgos

Los principales riesgos identificados en este ámbito son:

- **Ciberataques:** Amenazas como *malware*, *ransomware*, ataques de denegación de servicio y otros ataques cibernéticos. Según el informe de Sophos "The State of Ransomware 2024", en 2024 los ataques de ransomware siguen siendo una amenaza significativa para las empresas a nivel mundial. Un 59% de las organizaciones reportaron haber sido víctimas de ransomware en el último año, una ligera disminución respecto al 66% reportado en años anteriores. Sin embargo, el coste de recuperación ha aumentado respecto a otros años. En promedio, los costes de recuperación sin incluir el pago del rescate ascendieron a $2.73 millones, un aumento del 50% comparado con los $1.82 millones del año anterior. Más de la mitad de las organizaciones afectadas (56%) pagaron el rescate para recuperar sus datos, y muchas usaron múltiples métodos de recuperación, como el pago del rescate combinado con el uso de respaldos.

  Un 32% de los ataques comenzaron con una vulnerabilidad sin parchear, destacando la importancia de la gestión de vulnerabilidades y la actualización regular de sistemas. Se espera que los ataques de *ransomware* evolucionen, con un aumento en la explotación de infraestructuras de nube y VPN, y un mayor uso de inteligencia artificial generativa para mejorar las tácticas de ataque, como campañas de *phishing* más sofisticadas.

- **Errores humanos. Accidentes como la eliminación accidental de datos, malas configuraciones de sistemas, o divulgación involuntaria de información pueden causar pérdida de la confidencialidad y disponibilidad de los datos.**

- **Desastres naturales.** Eventos como incendios, inundaciones, terremotos, y tormentas pueden dañar infraestructuras físicas y sistemas de información.

- **Fallos técnicos.** Problemas como fallos de hardware, errores de software pueden interrumpir el acceso a la información crítica.

La **guía** considera tres factores:

- Política y procedimientos de **copia** de seguridad
- Protección de las copias de seguridad
- Pruebas de los procedimientos de seguridad

Todos ellos son bien conocidos por los responsables de informática y no procede un desarrollo especifico.

Lecciones aprendidas

Se deben gestionar los siguientes aspectos:

- **Política y procedimientos de copia de seguridad.** Es necesario, en primer lugar, conocer cuál es la información que hay que proteger para el correcto funcionamiento de la AT y comprender la mejor forma de hacerlo. Se requiere una política de seguridad donde se definan los procesos de salvaguarda. Es necesario disponer de procedimientos claros en los que se defina la forma de realizar las copias de seguridad, la periodicidad, el tiempo de retención, los responsables y al alcance de estos procesos. Deberán incluir las normas relativas al registro de copias de seguridad que incluya todos los detalles de cada copia: identificador, tipo de copia, fecha, lugar de almacenamiento, etc.

- **Cumplimiento normativo.** Es necesario conocer y cumplir con todos los requisitos normativos de protección de datos, tanto en los datos almacenados en sistemas informáticos como en las copias de seguridad.

- **Redundancia.** Para poder garantizar el correcto funcionamiento de los sistemas informáticos frente a un incidente, es necesario que los datos están redundados y al menos una de las copias de seguridad esté almacenada en un lugar diferente. Si se dispone de los medios suficientes, sería recomendable disponer de los datos redundados en al menos 2 CPDs, de tal modo que, en caso de incidencia en uno de los CPDs, la recuperación fuese inmediata dando servicio en el CPD de respaldo. Es recomendable disponer también de una tercera copia de seguridad en una ubicación física diferente, por si la segunda se deteriorase durante la recuperación.

- **Protección y disponibilidad de las copias de seguridad.** Se debe conciliar la protección de la confidencialidad de los datos almacenados en las copias de seguridad con la necesidad de que las copias estén disponibles de forma inmediata cuando se necesita disponer de ellas.

- **Pruebas y mejora continua de los procedimientos de copia de seguridad.** Es muy recomendable disponer de un plan de pruebas de los procedimientos de copia de seguridad y restauración, y al menos anualmente realizar una prueba de disponibilidad y recuperación a partir de las copias de seguridad.

- **Nivel de servicio.** Las compañías áreas tienen regulado la cantidad de combustible con la que despega un avión. No dejan decidirlo al piloto. Los responsables de continuidad de negocio deberían exigir al responsable de IT una respuesta concreta a la pregunta por el *Recovery Time Objective RTO*. ¿Si detectásemos ahora un virus o que nuestros datos están contaminados y si su origen se ha localizado por ejemplo hace una semana ¿Cuál es el tiempo que necesitaríamos para ir a una copia con datos de calidad y retornar a donde deberíamos estar? Si la demora no nos convence deberemos indagar el coste de que el tiempo sea el adecuado. Las autoridades de la Administración tributaria deben saber si caso de un desastre, recuperarán todo si o no. Si es así, en cuanto tiempo y si el tiempo es asumible cuántas horas de trabajo extraordinario y de quiénes, habrá que emplear.

4.3.4. Servicios de terceros

Propósito central en la evaluación del área

La Gestión de Riesgos de Terceros (*Third-Party Risk Management, TPRM*) es el proceso mediante el cual las organizaciones supervisan las relaciones con sus terceros asociados, con el fin de evaluar el comportamiento, desempeño y los riesgos relacionados con cada uno de ellos.

La idea de la externalización es antigua, pero en las Administraciones Tributarias, por motivos legales y culturales no ha prosperado, siendo el modelo autogestionado de las TIC el más generalizado. No obstante, el surgimiento de los servicios en *cloud* y la dificultad en captar técnicos, ha hecho que las Administraciones Tributarias también, se están valiendo de terceros proveedores para proporcionar servicios. La Guía ha querido prestar especial atención a este aspecto.

A finales del siglo XX, se extendió el uso del concepto de *outsourcing* tras las iniciativas de empresas como Kodak y Schweppes. La idea básica radicaba en concentrar la actividad de la empresa en las tareas en que tenían ventaja competitiva y contratar a terceros las demás tareas, como el transporte, eligiendo quienes las ofrecieran conforme a las mejores prácticas. Mientras que en algunos casos la determinación de lo que es fundamental (*core competencies*) y lo que no lo es (por ejemplo, la vigilancia o la atención del comedor de la empresa) no admite mucha discusión, en otros, como sucede con la totalidad de los servicios TIC, es más problemático.

Las teorías sobre los criterios a utilizar han sido estudiadas extensivamente, pero, en último término, los criterios para la decisión se basan más en la intuición del empresario que en un cálculo racional.

En el puro ámbito de las TIC, la tercerización es una práctica en constante crecimiento cuyos tres componentes más importantes son la administración de sistemas, el *outsourcing* de aplicaciones y el *web hosting*. Incluso organizaciones con un fuerte apego al desarrollo en sus instalaciones han considerado conveniente e incluso se han visto forzadas a utilizar plataformas para ofrecer servicios continuos en la red, a emplear factorías de software para poder cumplir los plazos de desarrollo o a la tercerización de servicios en materia de ciberdefensa, por no mencionar los despliegues en la nube de los que nos ocuparemos más adelante.

Este proceso evolutivo de largo alcance se ha visto alterado por el cambio tecnológico y organizativo que ofrecen y permiten los servicios en la nube. La pandemia de la COVID 19 forzó a muchas empresas a adoptar

la decisión. Según un estudio de la Función Telefónica, el 90% de las empresas españolas aumentó su uso de herramientas digitales durante la pandemia, lo que es extrapolable al resto de los países. Concretamente, la nube pasó de ser un espacio principalmente de almacenamiento a convertirse en un espacio de trabajo.

La globalización y los avances tecnológicos de los últimos años hacen que la dependencia entre distintas instituciones, empresas y proveedores sea inevitable. Esto arrastra una serie de ventajas, pero implica riesgos.

Según una encuesta realizada por Deloitte, el 28% de las organizaciones encuestadas habían tenido un incidente grave causado por sus proveedores, el 26,2% habían sufrido daño reputacional por las acciones de sus proveedores y el 21% habría vivido brechas de datos sensibles por esta misma causa.

Asimismo, la organización ISC, que gestiona el *Certified Information Systems Security Professional (CISSP)* ha publicado que 1/3 de sus 709 clientes en IT y ciberseguridad en la encuesta de noviembre de 2023 habían sufrido una vulneración. De ellos, el 54% había ocasionada por un socio de gran tamaño y el 46% por un socio de pequeño tamaño. Conviene recordar también el incidente de Crowdstrike y Windows en el mes de julio de 2024, que con la “pantalla azul de la muerte” dejó colapsados a millones de usuarios.

Cada vez más empresas están registrando, midiendo y notificando las interrupciones en la cadena de suministro que afectan a su rendimiento, pero según un informe de BCI (*Business Continuity Institute*) sólo el 25% de las empresas han creado un registro coordinado en toda la organización que permitan conectar unas con otras dando un sentido al conjunto.

Las instituciones financieras han atendido desde hace muchos años a la urgencia del problema y han elaborado información y guías cuya lectura recomendamos (Basel, 2024; Federal Reserve, 2024).

Adicionalmente, las grandes consultoras han realizado recientes informes sobre cómo gestionar este tipo de riesgos (Ernst & Young, 2023; PwC, 2023, KPMG, 2023). Las Administraciones Tributarias no tienen motivo alguno para prestar a esta cuestión menos atención que las financieras.

Principales riesgos

Si bien existen ventajas significativas cuando las organizaciones se valen de proveedores externos, esta decisión implica una serie de riesgos adicionales, que hay que tener presentes.

A continuación, se exponen los principales riesgos identificados:

- **Dependencia.** Falta de oferta de proveedores por ser el mercado estrecho y cautivo. Por un lado, esto supone un riesgo de dependencia de un proveedor específico, dificultando la transición a otros proveedores o soluciones. Por otro, supone riesgo para la continuidad, ya que reduce las alternativas en caso de fallo del proveedor principal.

  De hecho, según un informe realizado por BCI (*Business Continuity Institute*), el 53% de las organizaciones entrevistadas ven éste como uno de los principales problemas.

- **Cumplimiento legal.** Siendo en muchos casos los proveedores multinacionales, se puede correr el riesgo de que apliquen normativas menos estrictas que las que deseamos. En Europa, este problema tiene especial virulencia en materia de privacidad de datos. La normativa europea de protección de datos es restrictiva en cuanto a la ubicación de los servidores desde los que se ofrece el servicio, debiendo proporcionar los países en los que se ubican las mismas condiciones que las exigidas por el Reglamento Europeo. Por último, sucede que muchos de los contratos ofertados son prácticamente de adhesión y aportar la carga de la prueba de los daños sufridos en otras jurisdicciones es muy complicado.

- **Calidad del servicio y requisitos de seguridad.** Hay que tener presente que la responsabilidad final del servicio es de la organización y que, tras un fallo, poco se remedia encontrando un culpable o un chivo expiatorio. Si bien es cierto que, no puede evitarse el riesgo de que cualquier proveedor pueda sufrir un incidente grave que afecte al servicio, es importante que la selección de los proveedores sea lo más exigente posible. Es necesario, podría decirse obligatorio, que se le exija al proveedor que va a proporcionar el servicio que sea transparente con el servicio ofrecido, con las medidas de ciberseguridad y protección de datos que proporciona, con las estrategias de continuidad que ofrece y que todo ello quede claro y reflejado en el contrato. Deberá figurar cómo se medirá el impacto de forma inequívoca y qué actuaciones de mitigación le son exigibles de manera que no haya dudas acerca de lo que podemos y debemos exigir.

- **Reputacional.** Relacionado con lo anterior, existe el riesgo asociado a la mala reputación de la organización en el caso de que los servicios contratados no tengan la debida calidad.

- **Ambigüedad por contratos y SLAs no definidos correctamente.** La definición incorrecta de lo que se espera es un riesgo grave. Un proveedor válido puede ofrecer distintos niveles de servicio y no puede asumirse que vaya a garantizar algo que no se haya indicado explícitamente. Por ello, es muy importante especificar todos los requisitos que se requieren y definir los SLAs que puedan garantizar la continuidad del servicio según las necesidades de la organización.

- **Continuidad en caso de incidente del proveedor.** Los proveedores de servicio no están exentos de sufrir un problema de continuidad, independientemente del SLA que tengamos contratado. Por ello, hay que considerar posibles alternativas en el caso de que un proveedor deje de dar el servicio.

- **Posible camino sin retorno.** La sabiduría tradicional ha buscado "asegurar el camino de retorno en la tercerización" y se cita como ejemplo de la posibilidad el caso de la AFIP en Argentina que le permitió no renovar su contrato con una UTE. Mariana Mazzucato, en un excelente libro "El gran engaño" en el que aborda el problema de la consultoría, alerta, en el capítulo llamado "La infantilización de las organizaciones" sobre los perniciosos efectos de la pérdida de conocimiento actualizado, que atrapa en un círculo vicioso a algunas organizaciones. La estrategia más recomendable no es en absoluto evidente. La propia autora dice "Hoy resulta difícil creer que en su momento los gobiernos gestionaran y mantuvieran por ellos mismos gran parte de sus infraestructuras de TI, pero fue así en el siglo XX:..". Muchos países, aun haciéndolo por fases están evolucionado a nubes híbridas y dado que según el Gartner Group la vida media de las nuevas tecnologías que ahora están siendo implantadas es de dos años y medio, será más fácil cambiar a un proveedor alternativo que disponer de los conocimientos y los recursos para volver a la antigua instalación.

  En su carta a los accionistas de 2017, el fundador de Amazon Jeffrey Bezos explicó que el éxito de Amazon se había basado en su estrategia para la toma de decisiones: "Algunas decisiones son transcendentales e irreversibles, o casi irreversibles (puertas de un solo sentido), y hay que tomarlas con meticulosidad, esmero y lentitud, tras deliberarlo y consultarlo mucho". La tercerización parcial de los recursos TIC es casi imprescindible, pero una radical es una decisión profundamente estratégica y hay que tener la seguridad, como buscan los escaladores de que si no se puede volver a donde se estaba, al menos, si soltamos una mano tengamos asidero en otro lugar. Esta búsqueda sistemática de opciones alternativas es un principio inspirador de la Guía.

- **Falta de conocimiento de los riesgos reales.** La mentalidad en que se ha venido basando la Continuidad de Negocio ha sido la del "*Just In Time*", donde el mayor esfuerzo se orientaba en entregar cada producto y servicio en el momento adecuado y se procuraba garantizar que las interrupciones fueran las mínimas posibles asegurándolas con ciertos SLAs.

  Ahora el trabajo no es individual sino colectivo como en un quirófano. La pregunta del cirujano no es qué hay que prever hacer para acabar la intervención segura a una hora sino qué hacer si el anestesista falla. Con la potenciación de los servicios prestados por terceros, hemos pasado del "*Just in Time*" al "*Just in Case*". La tarea es difícil. Existe el sentimiento generalizado de que los datos tanto internos como externos en esta materia son de poca calidad, o muy vagos. Nadie tiene muy claro qué haría si una de las grandes tuviera una caída seria. ¿Qué sucedería si un incidente como el de *Crowdstrike* en vez de ser fortuito hubiera sido provocado y la interrupción del servicio durara días? Nadie tiene claro qué datos habrían

podido solicitar a Microsoft o cómo se podrían cambiar las licencias. Como siempre se debe gestionar este riesgo, sabiendo que es singular y distinto a otros.

En el estudio de este indicador se analizan tres factores:

- Proveedores
- Cloud
- Cadena de suministro

En el primero de los factores se investiga el grado de exigencia de la organización con los proveedores, el segundo se indaga la exigencia de un tipo de servicios que ha pasado a ser crítico y en el tercer lugar la atención de la AT a un elemento que, siendo novedoso, ha pasado a ser relevante, la **cadena de suministro** en sí.

Lecciones aprendidas

En este apartado se indican las acciones indispensables para gestionar los riesgos en los proveedores.

- **Inventariar los proveedores.** No se puede gestionar algo que no se conoce o sin información. Se deben inventariar todos los proveedores de servicio y la cadena de suministro que constituyen. Hay que conocer qué proveedores dan servicio al proveedor principal, la llamada cadena de suministro y tener en cuenta que no todos ellos han sido contratados a iniciativa del Departamento de Informática.

- **Identificar claramente lo que cada proveedor ofrece y no dar cosas por supuesto.** Tan importante como conocer los proveedores que nos suministran servicio es conocer qué alcance tiene dicho servicio, qué se ha exigido del mismo y qué se puede esperar de dichos proveedores en caso de incidentes.

- **Comunicación con los proveedores.** La comunicación debe estar garantizada en todo momento. De manera recurrente para conocer el estado del servicio, para explorar con transparencia qué hacer "*Just in case*", y por último en caso de incidente. Se debe disponer de un protocolo claro sobre la comunicación / notificación en caso de incidentes que incluya el tiempo en el que debe realizarse, vía de comunicación, etc. y mantenerlo actualizado.

- **Selección de los proveedores.** Para ello se puede y debe contar con la experiencia de otras organizaciones y no es desaconsejable promover reuniones de los servicios TIC de distintas instituciones del Estado y grandes organizaciones como las bancarias para compartir experiencias de éxito y malas experiencias. Además, se deberá disponer de un checklist con los requisitos mínimos exigibles en función del servicio que se ofrezca para reflejarlo y pedirlo en los Requerimientos de los concursos. Estos

requisitos cubrirán aspectos como certificaciones, estándares, ubicación de los servidores, políticas de backup, condiciones de la cadena de suministro, etc.

- **Monitorización de los proveedores.** Se debe hacer seguimiento de la evolución de los proveedores, revisar SLAs, revisar si las penalizaciones exigibles han sido exigidas, auditar algún aspecto relativo a seguridad o calidad de estos, si se ve necesario. Mediante la explotación de los registros de incidentes, los servicios jurídicos y de contratación, deben exigir sistemáticamente las penalizaciones existentes, pues la resistencia frente a las de menor importancia es indicador de otras mayores cuando la penalización sea grave y adiestrará a la organización en los obstáculos que se interponen.

- **Pruebas periódicas.** Hay llevar a cabo pruebas de continuidad considerando que un proveedor falla. De esta manera se pueden sacar conclusiones claras y mejoras de cara a afrontar una situación real.

- **Integrar la gestión de la continuidad de los terceros proveedores.** En la encuesta Global TPRM de Deloitte de 2023, la idea más difundida es que hay que considerar la continuidad de terceros proveedores como un aspecto dentro de los planes de continuidad de negocio. Así lo realiza la Guía.

- Dicho lo anterior, cuando existen varios *outsourcing*, en el sentido fuerte del término, cada uno de ellos debe tener su Plan de Continuidad diferenciado.

4.3.5. Infraestructura TI (hardware, software y comunicaciones) – alta disponibilidad

Propósito central en la evaluación del área

En el ámbito de tecnologías de la información y las comunicaciones, el concepto de **disponibilidad** se refiere a la capacidad de un servicio, conjunto de datos o sistema, de ser operable y accesible en el periodo de tiempo determinado en el que son requeridos. Para garantizar la operación son necesarias medidas y mecanismos que permitan al sistema de información mantener su estado de operatividad y accesibilidad.

La determinación del grado de **alta disponibilidad** requerido de la infraestructura TI, es un elemento esencial de un plan de continuidad de negocio. Los conceptos de alta disponibilidad de los recursos TIC, tolerancia a fallos y redundancia están relacionados.

En la metodología de la Guía se distinguen los siguientes factores:

- Políticas y procedimientos relacionados con la disponibilidad de los sistemas TI

- Arquitectura y operación
- Monitorización
- Evaluación y mejora continua

El factor 3.5.1 indaga en los procedimientos existentes buscando conocer hasta qué punto al diseñar las políticas, al realizar los inventarios, al crear los procedimientos, etc., se ha tenido en cuenta el factor de alta disponibilidad. El factor 3.5.2 indaga hasta qué punto se ha considerado la alta disponibilidad en el diseño de arquitectura.

Se describen a continuación los distintos modelos existentes para garantizar la alta disponibilidad, así como el comportamiento de sus nodos en caso de fallo.

- **Modelo de equilibrio de carga (activo-activo).** Tanto el nodo primario como el secundario son activos y procesan las solicitudes del sistema en paralelo. Los datos se replican de forma bidireccional en función de los servicios del sistema. El tiempo de recuperación en caso de fallo de un nodo en este modelo es cero.
- **Modelo de espera caliente.** Ambos nodos disponen del software instalado y disponible. El nodo secundario se encuentra activo y en ejecución, pero no procesa de forma activa datos hasta que falla el nodo primario. En este caso, el tiempo de recuperación es de pocos segundos.
- **Modelo de espera templada.** En este modelo, los nodos disponen del software instalado y disponible, pero el nodo secundario no está ejecutándolo. En caso de fallo en el nodo primario, mediante un gestor de clúster, el nodo secundario inicia los componentes de software. Los datos se replican regularmente en el nodo secundario o se almacenan en un disco compartido. El tiempo de recuperación en caso de fallo es de pocos minutos.
- **Modelo de espera fría.** El nodo secundario dispone de la misma configuración que el primario, pero se encuentra apagado. Solo se enciende y entra en acción en caso de fallo en el nodo primario. Los datos pueden ser copiados en un sistema de almacenamiento y restaurados en el nodo secundario en caso necesario. Es el modelo más lento y puede tardar unas horas en recuperarse.

La Alta Dirección debe conocer expresamente cuál es el caso. En los casos donde se requiera la contratación de recursos TI externos para el desarrollo de las actividades de la organización, es necesario establecer un Acuerdo de Nivel de Servicio en lo que se refiere a La disponibilidad de forma contractual. Este acuerdo debería incluir las características del servicio prestado, lo que debería entenderse como “servicio mínimo admisible”, así como la responsabilidad del prestador del servicio y las consecuencias para este en caso de incumplimiento.

En lo que se refiere específicamente a los sistemas de telecomunicaciones, se debe disponer de:

- Redundancia de los propios dispositivos empleados para llevar a cabo las comunicaciones, tales como Switches y Routers. Lo más habitual es disponer de elementos redundados y emplear los mecanismos de red disponibles para garantizar la recuperación automática frente a fallos, como por ejemplo VRRP (*Virtual Router Redundancy Protocol*), de tal modo que cuando se produce un fallo en uno de los dispositivos de enrutamiento, otro dispositivo lo sustituye de forma automática, logrando que no se produzca una degradación del servicio.
- Redundancia de los canales de comunicación. En este caso, se logrará mediante la duplicación de los propios canales de comunicación. En el caso de redes internas, una red de cableado interna alternativa, disponible en caso de fallo en la red principal. En el caso de redes externas proporcionadas por un tercero, una red externa alternativa contratada con un Operador distinto al que suministre red principal. De tal forma que, en caso de problema con el Operador principal, se disponga de una contingencia inmediata.

En el factor 3.5.3 se valora la monitorización de la disponibilidad. Un enfoque proactivo y bien planificado para garantizar la disponibilidad de los sistemas TI de la organización ayuda a resistir y recuperarse rápidamente de incidentes disruptivos, minimizando el impacto en sus operaciones.

Para monitorizar la disponibilidad y poder seleccionar las medidas de seguridad que será necesario aplicar, se dispone de distintas métricas que miden la disponibilidad y la fiabilidad de los servicios.

Las principales métricas a tener en cuenta son:

- **MTTF (Mean Time to Failure).** Es la medida que estima el tiempo entre fallos en los sistemas en su operación normal. Se puede calcular como la media aritmética entre fallos de un sistema.
- **MTTR (Mean Time to Recover).** Es la medida que indica el tiempo medio que le llevará al sistema volver a una situación de normalidad tras haberse provocado un incidente.
- **Disponibilidad.** El cálculo del porcentaje de disponibilidad del sistema se calcula mediante la fórmula: Disponibilidad = MTTF / (MTTF + MTTR).
- **RTO (Recovery Time Objective) o Tiempo de recuperación.** Es el tiempo que un proceso del sistema TI permanecerá detenido antes de que su funcionamiento sea restaurado. En función del nivel de disponibilidad requerido por el sistema, se deberá establecer un RTO máximo para los distintos procesos de la organización.
- **Tiempo máximo tolerable de caída o MTD (Maximum Tolerable Downtime).** Es el tiempo que un proceso del sistema TI puede permanecer inoperativo antes de que se produzcan consecuencias críticas para la organización.

- **Nivel mínimo de recuperación de servicio o ROL (Revised Operating Level).** Es el nivel mínimo de operación que debe tener una actividad para ser considerada como recuperada, aunque el nivel de servicio no sea el óptimo. En la metodología del CIAT se indaga hasta qué punto el proceso para garantizar la disponibilidad mejora con el tiempo.

Principales riesgos

Tal como se ha comentado en este punto del manual, los sistemas de información y las comunicaciones son imprescindibles para el desempeño de las labores de una administración tributaria. Los principales riesgos que pueden afectar a la disponibilidad de los sistemas son:

- **Riesgos físicos**
  - Desastres Naturales: Terremotos, inundaciones, incendios, etc.
  - Interrupciones de Energía: Cortes de electricidad, fluctuaciones de voltaje.

- **Riesgos técnicos**
  - Fallos de Hardware: Problemas con servidores, discos duros, y otros componentes físicos.
  - Fallos de Software: Errores en aplicaciones, sistemas operativos y bases de datos.
  - Fallos de servicios de terceros, en caso de que la administración tributaria tenga dependencias de ellos para desarrollar sus actividades.
  - Fallos en los servicios de telecomunicaciones, tanto la red interna como las comunicaciones con redes de terceros e Internet.

- **Problemas de red**
  - Caídas de la red interna, problemas de conectividad, fallos en routers y switches.
  - Fallos en los servicios de telecomunicaciones de terceros, que proporcionan la comunicación con redes de terceros e Internet.

- **Riesgos humanos**
  - Configuraciones incorrectas, eliminación accidental de datos, negligencia.
  - Ataques Internos: Sabotaje por empleados descontentos, accesos no autorizados.

- **Riesgos de seguridad**
  - Ciberataques: Malware, ransomware, DDoS (ataques de denegación de servicio), hacking.
  - Fugas de datos: Accesos no autorizados, pérdida de datos sensibles.

- **Riesgos operativos**
  - Mantenimiento programado: Actualizaciones y paradas planificadas.
  - Capacidad y rendimiento: Sobrecarga de sistemas, falta de recursos.

Lecciones aprendidas

En este apartado se indican las acciones indispensables para gestionar los riesgos asociados a la infraestructura TI (*Hardware*, *Software* y Comunicaciones) y garantizar la alta disponibilidad de los sistemas.

- **Crear una política de disponibilidad y procedimientos orientados a garantizar la alta disponibilidad de los sistemas TI.** Es necesario tener claro cuáles son los sistemas críticos y definir los tiempos asumibles de inactividad para los mismos

- **Disponer de redundancia de sistemas y comunicaciones.** En la mayoría de los casos, disponer de infraestructura redundada es la única forma de cumplir con los objetivos de la organización frente a incidentes que afecten al CPD principal o las telecomunicaciones.

- **Monitorizar sistemas y comunicaciones.** La monitorización sistemática permite identificar problemas en tiempo real **o incluso antes de que ocurran**. Esto incluye fallos en el hardware, problemas de rendimiento, errores de software, comunicaciones etc. Se debe impulsar **la transparencia, haciendo visibles las indisponibilidades y con ello creando conciencia de la existencia de un problema, si es el caso**.

- **Evaluar para mejorar.** Se debe recopilar información suficiente sobre los incidentes que hayan afectado a la disponibilidad de los sistemas, **analizarlos** y no solo registrarlos y con los resultados de este análisis implementar todas las mejoras que sea posible. Se deben realizar simulacros para probar los procedimientos de recuperación y las medidas implantadas. Se deben revisar periódica y sistemáticamente las políticas y procedimientos relacionados con la disponibilidad de los sistemas, para adaptarlos a los posibles cambios tecnológicos de la organización. Los cambios en la tecnología desplegada son oportunidades para simplificar mejorar o reenfocar las estrategias.

4.3.6. Gestión de la seguridad y respuesta frente a ciberincidentes

Propósito central en la evaluación del área

En el contexto de un plan de continuidad, la gestión de seguridad y la respuesta ante ciberincidentes son actualmente fundamentales para garantizar el servicio en las administraciones tributarias.

En el PCN del CIAT se evalúan en este indicador

a) Políticas y procedimientos relacionados con la seguridad

b) Gestión y monitorización

c) La respuesta ante ciberincidentes

d) La evaluación y mejora continua

El conjunto de todos ellos no encierra novedad conceptual, sino que indaga por la existencia de prácticas que no son especialmente complejas, pero buscando que explícitamente se desarrollen en el ámbito de la ciberseguridad.

La guía incluye un indicador en esta materia porque en numerosos informes se aprecia la tendencia creciente del número de amenazas y ciberincidentes. El informe del CCN-CERT (Centro Criptológico Nacional, perteneciente al Centro Nacional de Inteligencia de España) del año 2023, muestra que los incidentes más comunes han sido:

1. **Phishing y suplantación de identidad:** Representan un 35% de los incidentes. Este tipo de ataque sigue siendo predominante debido a su efectividad en engañar a los usuarios para que revelen información sensible.
2. **Ransomware:** Ha afectado a un 25% de las empresas, con un notable incremento en la sofisticación de los ataques y las demandas de rescate.
3. **Ataques de denegación de servicio (DDoS):** Conforman un 20% de los incidentes reportados, dirigidos principalmente contra infraestructuras críticas y grandes corporaciones para interrumpir sus servicios.
4. **Vulnerabilidades y explotación de software:** Aproximadamente el 15% de los incidentes han sido resultado de la explotación de vulnerabilidades no parcheadas en sistemas y aplicaciones.
5. **Robo de datos:** Afecta a un 5% de las empresas, con ataques dirigidos que buscan obtener información confidencial y valiosa.

Principales riesgos

- **Ciberataques avanzados:** Amenazas sofisticadas como *ransomware*, ataques de día cero y campañas de *phishing* dirigidas, que pueden evadir las defensas tradicionales.
- **Errores humanos:** La falta de capacitación y conciencia entre los empleados puede resultar en errores que faciliten la ocurrencia o empeoren los efectos de un incidente.
- **Amenazas internas:** Empleados descontentos o negligentes que puedan causar incidentes de seguridad intencional o accidentalmente.
- **Fallos de detección de incidentes:** Sistemas de detección y monitorización inadecuados que no identifican actividades sospechosas a tiempo.
- **Respuesta inadecuada:** Procesos de respuesta mal diseñados o ejecutados que no logran contener o mitigar efectivamente los incidentes.
- **Falta de recursos:** Insuficiencia de personal, herramientas y tecnología para gestionar y responder adecuadamente a los incidentes.
- **Dependencia de proveedores externos:** Riesgos asociados a la seguridad de los proveedores de servicios y su capacidad para manejar incidentes.
- **Fallos en la comunicación:** Comunicación ineficaz durante y después de un incidente, lo que puede agravar la situación y retrasar la recuperación.
- **Incumplimiento normativo:** Sanciones y repercusiones legales debido al incumplimiento de leyes, normativas y regulaciones de seguridad.
- **Políticas y procedimientos de seguridad desactualizados:** Políticas y procedimientos obsoletos que no reflejan las amenazas y tecnologías actuales.

En la actualidad sabemos la necesidad de:

Políticas y procedimientos específicamente relacionadas con la ciberseguridad. En estos procedimientos se deberían describir claramente todas las cuestiones relacionadas con la gestión de la ciberseguridad, de tal forma que se minimicen las posibilidades de sufrir incidentes por ciberataques y estén definidos los mecanismos de detección y respuesta cuando se produce un incidente.

Actualizar los sistemas de gestión de vulnerabilidades. Constantemente se descubren nuevas vulnerabilidades en los sistemas informáticos, que se suelen solucionar aplicando los parches que

proporciona el fabricante. Es necesario disponer de “disparadores” de procedimientos que se activen ante la recepción de las noticias oportunas por los proveedores, socios u otras instituciones del Estado. Herramientas y procedimientos de gestión de parches y actualizaciones de seguridad. Es altamente recomendable disponer de mecanismos para analizar los sistemas en busca de vulnerabilidades, de tal forma que se puedan detectar y solucionar con la mayor rapidez posible, reduciendo así la ventana de tiempo en la que se pueda sufrir un incidente de seguridad o incluso realizar acciones de *hacking* ético.

Controlar las prisas. El responsable de seguridad debe estar en el primer nivel de la organización, desde luego en el Área de Informática, y el Director le debe conceder plenos poderes para detener una implantación o servicio en caso de riesgo.

Prevención de intrusiones. No basta con disponer de sistemas de detección, sino que hay que configurarlos y actualizarlos correctamente, así como monitorizar los resultados que proporcionan.

Detectar incidentes. Hay que contar con las herramientas adecuadas, como por ejemplo un SIEM que recopile los eventos de los sistemas, y mediante correlación sea capaz de detectar posibles comportamientos anómalos que puedan ser un indicio de un incidente de seguridad. No se deben regatear esfuerzos en disponer de un equipo de personal adecuado, tanto para configurar estas herramientas y dotarlas de utilidad como para revisar y gestionar e interpretar los avisos y alertas que proporcionan.

Responder ante incidentes. Una vez que se ha producido un incidente, es muy importante tener claro los pasos que hay que seguir para minimizar el impacto y recuperar la normalidad de la operación de la administración tributaria. Existen distintos aspectos que es muy importante tener en cuenta en la respuesta ante incidentes.

- *Personal cualificado.* Es necesario disponer de recursos humanos cualificados y suficientes, para llevar a cabo la respuesta ante incidentes. Lo más habitual es contar con un centro de operaciones de seguridad (SOC) que esté especializado en la detección y respuesta ante incidentes y que opere en horario 24x7.
- *Procedimientos y protocolos de respuesta ante incidentes.* Para gestionar correctamente la respuesta ante un incidente, es necesario que se hayan definido protocolos y procedimientos de actuación frente a los posibles incidentes. De igual forma es imprescindible contar con los mecanismos de comunicación internos y con terceros para gestionar los incidentes, así como de escalado a la dirección cuando sea necesario.
- *Automatización de respuesta ante incidentes.* Para mejorar la seguridad y minimizar el impacto que pueda tener un incidente, es recomendable disponer de mecanismos automatizados de mitigación de amenazas a través de las herramientas de las que disponga la administración tributaria. Un ejemplo sería el bloqueo

automático de una cuenta de usuario, cuando en el SIEM se detecta un comportamiento anómalo de dicho usuario. En muchas ocasiones, este tipo de acciones automatizadas, evitan incidentes de seguridad.

La **guía** concede importancia a la evaluación de la seguridad y **mejora continua**. Se indaga en el factor 3.6.4.

Para desarrollar un proceso de mejora continua, es recomendable recopilar y analizar todos los datos relacionados con incidentes de seguridad, para detectar e implementar posibles mejoras y que se haga una revisión periódica de todos los procedimientos y documentación asociados a la gestión de seguridad, detección y prevención de incidentes.

Formación. Muchos de los incidentes de seguridad son originados por los comportamientos, en muchos casos involuntarios, de los usuarios internos. Se debe desarrollar un plan de formación con nociones básicas de seguridad y capacitación para los empleados lo cual ayuda notablemente a reducir los riesgos de sufrir un incidente. También se debe capacitar de forma más específica en materia de seguridad del personal encargado de la detección y respuesta ante incidentes, así como el resto de personal TI que pueda tener alguna responsabilidad sobre la seguridad de los sistemas.

Lecciones aprendidas

Las primeras **48 horas son críticas**. En un primer momento hay que:

- Apagar los servidores no imprescindibles y aislar los segmentos críticos de red.
- Limitar el acceso remoto salvo a los usuarios imprescindibles.
- Coordinar con expertos internos y externos en ciberseguridad.
- Notificar la incidencia a usuarios y proveedores para generar confianza.
- **Registrar y anotar todo.** Ayude a la posible investigación penal ulterior, con todos los datos de contexto posibles.
- Valorar los daños.
- **Evitar que participe todo el que quiera ayudar.** El más caracterizado debe tomar el mando.
- **Incrementar al máximo la prevención.** Actúe, pues es muy fácil que suceda, que el primer ataque sea una distracción y esté preparado un segundo mientras los técnicos recuperan.

4.3.7. Recursos humanos

En la actualidad la misión de Recursos Humanos ha evolucionado. Son ideas relevantes las siguientes:

En tiempos de crisis, las organizaciones confían en sus departamentos de RR.HH. para que les proporcionen una dirección estratégica y garanticen el bienestar de su fuerza laboral. Los profesionales de RR.HH. han pasado de realizar actividades transaccionales a ser socios estratégicos que guían a la empresa en tiempos de turbulencia. Colaboran con la alta dirección para desarrollar planes de respuesta a las crisis, centrándose en la seguridad de los empleados, las estrategias de comunicación y la asignación de recursos.

Propósito central en la evaluación del área

En el apartado 4.3.1 se ha abordado el aspecto organizativo. Ahora abordamos un aspecto que complementa el anterior, los aspectos subjetivos, personales y los factores de contexto como los motivacionales o los asociados a los riesgos laborales.

Prestamos especial atención a las tareas que debe desempeñar el Departamento de Recursos Humanos.

Se identifican tres indicadores

- Necesidades: roles y habilidades
- Existencia de equipos de respuesta
- Formación y entrenamiento

Roles y habilidades

Siendo evidente que no es la misma estructura en una organización de gran tamaño que en otra de tamaño reducido, lo que se intenta evaluar es si el rol de la continuidad de negocio se delega implícitamente sin más consideración al Director/a de Informática, si se designa a un “hombre orquesta” o si simplemente no se diferencian y asignan roles.

Lo que se pretende evaluar es si los roles, sean cuales sean, están diferenciados, se potencian las habilidades necesarias y los expertos están organizados.

Algunos posibles roles son:

- **Comité de auditoría o de riesgos y/o continuidad.** La supervisión de las medidas relativas a la continuidad se delega normalmente al comité de auditoría. A veces, otro comité tiene esta responsabilidad, como un comité de operaciones o de gobernanza.
- **Gerencia ejecutiva.** Cada miembro del equipo ejecutivo conserva la supervisión y la responsabilidad final de la planificación de la continuidad en su área específica de operaciones.
- **Patrocinador ejecutivo o propietario de un área del negocio.** Es común designar al director de informática o al de tecnología o un gerente o subdirector. Supervisan la gestión diaria de las actividades de planificación de la continuidad.
- **Miembros del comité directivo de continuidad.** El comité directivo de continuidad empresarial, cuando existe, es normalmente un equipo interdisciplinario de seis a ocho personas, se reúne trimestral o anualmente para garantizar que el programa de continuidad empresarial esté alineado con la estrategia y los objetivos corporativos y que madure y avance hacia las metas anuales.
- **Gerente del programa de continuidad.** Puede crearse en las grandes organizaciones este puesto singular. Si no es el caso, es conveniente asignar la responsabilidad a alguien en el Comité de Dirección.
- **Responsables de los distintos aspectos de la continuidad.** Compatible con otras tareas.

La **guía** indaga en la existencia de equipos de respuesta y en la formación y entrenamiento, sobre lo que no nos extendemos por no incluir conceptos técnicos específicos.

Lecciones aprendidas

Recuerda que:

- **La seguridad integral del personal es fundamental.** En tiempos de crisis, las AT deberían lograr que sus departamentos de RR.HH. les proporcionen una dirección estratégica y establezcan las normas que garanticen la seguridad y en lo posible el bienestar de su fuerza laboral. Los profesionales de RR.HH. guían a la empresa en tiempos de turbulencia y definen la estrategia de comunicación.
- **La comunicación eficaz es una piedra angular del PCN.** Recursos Humanos debe tomar la iniciativa en la difusión de información precisa y oportuna a los empleados, fomentando un sentido de transparencia y confianza. Deben impulsar iniciativas para apoyar el bienestar mental y emocional de los empleados.
- **Hay que garantizar la productividad.** La pandemia de COVID-19 ha impulsado el despliegue de modalidades de trabajo ágiles. **Se deben crear las herramientas que permitan garantizar que estas facilidades no causen una reducción de la productividad** o generen absentismo.

- **Gestión del talento.** RR.HH. debe facilitar e incluso impulsar la búsqueda de talento y facilitar e impulsar mediante carreras de formación **la versatilidad** pues la extrema especialización no es deseable durante una crisis prolongada o después de un desastre.
- **Definición de nuevos roles.** Las situaciones de crisis exigen una adaptación rápida, y RR.HH. debe alinear la estrategia de gestión del talento con el PCN. Los profesionales de RR.HH. redefinen **los roles laborales y sus retribuciones**, identifican las carencias de habilidades e implementan programas de capacitación y actualización de habilidades para equipar a los empleados ante las demandas cambiantes.
- **RR.HH. como gestor de recursos psicológicos.** RR.HH. debe ofrecer a los empleados **apoyo psicológico y recursos** para ayudar a los empleados a afrontar el estrés y el impacto de una crisis.

4.3.8. Precariedad

Propósito central en la evaluación del área

La carencia de los recursos necesarios para realizar el trabajo supone un compromiso no solo para la continuidad sino para la mera actividad. En los análisis convencionales esta carencia de recursos de todo tipo se analiza como un riesgo, pero en trabajos previos del CIAT se ha singularizado su importancia. Por esa razón se le concede un apartado singular.

En todos los ámbitos existe una tendencia a compararse con las mejores prácticas, pero en este ámbito no es posible.

En Física se estudia el concepto de magnitudes extensivas como la masa e intensivas, como la temperatura. El número de contribuyentes es una magnitud aditiva mientras que las variables de continuidad de negocio no lo son. Si tenemos una masa de un kilo y traemos otra tendremos dos kilos. Si necesitamos controlar mil contribuyentes en un lugar y mil en otro necesitamos controlar dos mil contribuyentes. La ratio de inspectores por contribuyente es extensiva. Si queremos controlar con igual precisión el doble de contribuyentes necesitamos el doble de inspectores.

Los recursos asociados a la informática son extensivos. Hace falta prácticamente el mismo programa para despachar un millón de documentos de importación que dos. Las organizaciones gestionan cada año más potencia y Data Lakes más grandes con las mismas personas.

Por este hecho mientras que el análisis del número de efectivos en una organización a través de tablas como las de ISORA o de la OCDE en el ámbito de la gestión tributaria y del control tributario son muy útiles, aquí lo son menos.

La evaluación que aquí se realiza es prácticamente binaria. En el factor 3.8.1 y bajo el principio de que el servicio se deja por causa de la carencia del recurso más escaso se pregunta simultáneamente por capacidad instalada, de desarrollo, de presupuestos de personal, asumiendo que si hay carencia de uno solo de ellos la situación deviene precaria.

Las métricas habituales no son aplicables a una AT. El gasto en recuperación de desastres en las empresas financieras y comerciales se correlaciona con el costo promedio del tiempo de inactividad de una empresa, como puso de manifiesto un estudio de 2016 realizado por Cloud Endure. El problema que la determinación del coste de inactividad por hora o día de una Administración Tributaria es muy especulativa.

La implantación de las medidas diseñadas en una guía de continuidad de negocio es costosa y no se hacen en los ratos libres. En ocasiones se tiende a enfocar la planificación de la continuidad de negocio que es realizada por algunas personas junto con otras tareas administrativas atendiendo a las prioridades existentes en cada momento. No debe ser así.

El PCN **debe incluir un presupuesto** que refleje todos los recursos necesarios desde el inicio del proyecto BCP hasta el final. El presupuesto puede incluir lo siguiente:

- Capacitación en BCP (cursos internos o públicos)
- Software especializado en BCP
- Consultores externos
- Infraestructuras
- Servicios externos prestados para respaldar el BCP
- Gastos de viaje

Puede utilizarse como referencia el Capítulo 16 del libro *Managing Your Business Continuity* (Goh, 2021).

Los factores identificados son:

- Precariedad por escasez de recursos

- Precariedad por rigidez
- Precariedad por contexto

En el primero se investiga si la situación de fragilidad tiene su origen en lo material, por la carencia de recursos, en el segundo si se deriva de la estructura y en la tercera si tiene su origen en el contexto

Lecciones aprendidas

La situación de precariedad es un estado en el que una persona o una organización se encuentra arrojado. Pues sus causas son muy diversos sus remedios son muy distintos, pero existe un corpus de conocimiento, que, adaptándolo, puede ser utilizado. Adapte estándares ante la escasez de recursos de consultoría. BS 25999-2:2007 es una norma británica que proporciona los requisitos que debe satisfacer una buena gestión orientada a la continuidad de negocio (BCM). Su idea fundamental es que BCM tiene como objetivo gestionar diversos tipos de riesgos poco comunes que tendrían un enorme impacto en una empresa. La norma, como esta guía, requiere la implementación de un sistema de gestión de acuerdo con el ciclo PDCA como sucede en otras normas, como ISO/IEC 27001, ISO/IEC 20000, ISO/IEC 9001 e ISO/IEC14001. Sin embargo, esas normas describen sólo qué hacer en lugar de como hacerlo. Es una buena práctica revisar críticamente estas normas y construir materiales anticipando cómo se debería reaccionar en caso de desastre favoreciendo con ello tanto la reflexión como la capacitación.

4.4. Madurez

Concepto de madurez y CMM

En este apartado abordamos el aspecto más avanzado de la Continuidad de Negocio. A medida que la tecnología y la misión de las administraciones tributarias evolucionan, los Planes de Continuidad de Negocio se hacen a su vez cada vez más complejos y es más difícil su gestión. Implementan procesos, aprueban normas, realizan actividades que, en este ámbito, con el transcurso del tiempo, constituyen un “marco de trabajo” (en: *business continuity framework*). No tienen por qué ser iguales en todos los países pues sus necesidades son distintas. Como dijo Confucio “cada uno es el mejor a su manera”, pero, dicho lo anterior, hay grados en el ser mejor.

Lo que aquí nos ocupa es un “constructo”, como la calidad, no una variable directamente observable como la existencia o no de normas o el monto de las inversiones. La palabra madurez (en: *maturity*) en primera aproximación tiene asociada la idea de llegar a ser todo lo bueno que se puede ser, llegar al acmé, en el

ámbito de los procesos. Se sitúa en el campo semántico de "*capability*", recogiendo la idea de tener la capacidad para hacer algo, todo lo mejor que podemos hacer, fluidamente cuando sea necesario.

El factor 4.1.1 indaga sobre si existe en la organización un **modelo de madurez**. Describiremos ahora el concepto.

Los modelos de madurez describen una serie de estados cualitativamente ordenados de esa madurez, "*niveles*", y un camino, "*path*" "*roadmap*", para ir alcanzándolos sucesivamente. El estar situado en los más elevados ofrece a la propia organización y a los interesados, la capacidad de ofrecer calidad y la confianza de poder ejecutar procesos similares en sus efectos a los de las mejores prácticas.

La idea de concebir que el mundo se puede organizar en niveles jerárquicos (*hieros archos*), lo que no tiene por qué ser verdad ni es evidente, la popularizó, dentro lo que cabe, en la teología, Dionisio el Areopagita. Se empezó a popularizar en las ciencias sociales los años 50, en Psicología, con Maslow y sus niveles. La idea fue recogida en los años 70, ya como madurez, en el mundo del proceso de datos (e.g.: Crosby Quality Management Maturity Grid -QMMG).

Alcanzó popularidad en los años 90 con el desarrollo del *Capability Maturity Model (CMM)* por el *Software Engineering Institute (SEI)* en la Carnegie Mellon (1993). Fue pensado como un instrumento a utilizar por el *Department of Defense (DoD)* de EE.UU. para evaluar a sus proveedores y su capacidad para entregar productos de calidad de forma consistente. Esencialmente era una técnica de *Supply Chain Management* que ayudaba a mitigar los riesgos de un proyecto impulsando la calidad en los procesos de los suministradores. A muchos les interesó que el concepto fuera aceptado, entre ellos a los que comercializaban el *outsourcing* del desarrollo por empresas en la India, ponderando que ofrecían estar situadas en el nivel 5 (máximo) de madurez del CMM.

Thorsden y Bick (2023) han indagado sobre la real utilidad y alcance de la idea, más allá de la publicidad de quienes ofrecen consultoría sobre estos métodos.

El CMM, que es probablemente el más conocido de los modelos de madurez en TI define el término *madurez* (Paulk, 1995) como 'la medida en la que un proceso especifico está exactamente definido, gestionado, medido, está controlado y es efectivo'.

La idea de que existe en cualquier ámbito, la Continuidad de Negocio, una escala por niveles de perfección, lleva implícitamente asociada que nuestros niveles y procesos son comparables con los de otros. Pero ¿Qué otros?

En 1997, Jerry Klawitter en J.P. Morgan Chase pensó en crear un *Business Continuity Management* para su empresa, una financiera, tomando como ejemplo los modelos desarrollados para la creación de Software, lo que hizo tras contactos con Virtual Corporation (Corporation, 2007). Así se creó BCMM con seis niveles de madurez.

A partir de aquí proliferaron muchos modelos, existiendo una cierta voluntad comercial en que fueran generales, lo que no oculta al lector que los hace adolecer de cierta vaguedad. Son ejemplos de ellos el *SMIT* (Smit, 2005, Randeree et al., 2012), *Gartner*, *RSA*, *BCM Gartner Security Process Maturity Model* (Dang Van Mien, 2001), el *KPMG World Class IT model* (Delen, 2000), el *IT service CMM* (Niessink, Clerc and Van Vliet, 2002), el de Desarrollo de Sw CMM (Paulk, 1995), el INK-model (Titulaer, 200, Self-Assessment (Gallagher, 2003) el *Complete Public Domain Business Continuity Maturity Model SM* (Virtual Coorporation Inc., 2004), el *Gartner BCP Maturity Model* (Mingay, 2002), *BCMS Capability* (Sheth, 2007), Program Metrics (Strong, 2010).

Para una revisión sistemática (Tarhan et als., 2016). En el año 2008 ya existían 135 modelos de madurez en el ámbito del desarrollo del Sw en un esfuerzo que se acabó condensando en la ISO 22301. Sobre esta última existen publicaciones gratuitas[6]. Esta norma se ha creado buscando la generalidad por lo que puede ser implantada por cualquier organización con independencia de su línea de negocio o tamaño. Utiliza el modelo Plan-Do-Check-Act (PDCA) como principio operativo.

En el caso de las Administraciones Tributarias no es fácil la comparación, si no es por mera analogía, con empresas como Netflix o con grandes bancos, y aunque la comparación se facilita porque ya hay estándares como ISO, es importante comprender juiciosamente qué características deben tener los niveles en los que se debe estar.

Objetivos de los modelos de madurez en BC

La utilización de cualquiera de estos modelos ofrece una mera guía para proporcionar respuesta a las siguientes preguntas de las autoridades tributarias:

1. ¿Dónde estamos ahora en términos relativos?
2. ¿Dónde queremos estar en el futuro para estar mejor?
3. ¿Dónde deberíamos estar más adelante, a continuación?

6 ISO - ISO 22301 - Business continuity

Para valorar la madurez de una organización conviene considerar los siguientes aspectos:

1. **Definición previa de los niveles de madurez**
   Es preciso que los niveles definidos tengan dos características: a) que ofrezcan información suficiente y comparable. De poco serviría crear tres niveles, por ejemplo, malo medio y bueno, más aún cuando en el nivel medio estaría la mayoría en circunstancias muy distintas b) Bien ordenados. El continuo de las empresas debe distribuirse adecuadamente en ellos pues si los niveles fueran tales que el 90% estuviera en uno de ellos la información sería poco útil, c) Informativos. La contestación a los cuestionarios debe informarnos no solo del nivel correspondiente alcanzado sino del camino de evolución al siguiente.

2. **Criterios de valoración**
   Las preguntas que se realizan para situar a la empresa en el nivel de madurez debido la sitúan en relación con las mejores prácticas. Estas son distintas en una administración tributaria que, en un hospital, por lo que los cuestionarios deben estar adaptados. En el caso del modelo del CIAT a una realidad tributaria regional.

3. **Áreas e indicadores (KPIs)**
   Estos modelos fraccionan la actividad estudiada, en nuestro caso los procesos orientados a la continuidad del negocio en áreas (en el modelo del CIAT son cuatro) e indicadores para poder disponer de una métrica de los avances.

4. **Mejores prácticas y mejora continua**
   Conviene que exista una referencia a las mejores prácticas que es lo que se pretende aportar en el presente manual.

5. **Cambios organizacionales**
   Escalar en los niveles del modelo de madurez viene acompañado de cambios estructurales y culturales en la organización.

En el diseño de la Guía se identifican tres niveles. Hay modelos con más. Se ha seleccionado un valor pequeño por hacer su evaluación simple teniendo en cuenta además que no es razonable pensar que después de la epidemia del COVID 19 exista alguna administración tributaria que no haya tomado medida alguna en materia de continuidad y que la mejor práctica es un ideal

- **Iniciado.** Se trata del nivel básico. Una organización en esta situación realiza actividades dispersas, hace copias de seguridad, actúa reactivamente, existen documentos, pero no hay un plan definido. Se asume que el Departamento de IT es en lo fundamental el único responsable.
- **Planificado.** Se ha superado la situación anterior porque existe un Plan de Continuidad de Negocio, existen normas y responsables. Existe conciencia del problema y decisión de actuar.

- **Implementado.** El Plan o planes con mayor o menor perfección son gestionados. La administración tributaria como conjunto gestiona la continuidad del negocio.

Esta **guía** incluye este apartado porque indaga sobre un proceso, el de Gestión de la Continuidad. Recomienda hacer un esfuerzo para situar inicialmente la organización en uno de tres niveles, los indicados a continuación y luego disponer de una metodología que impulse una progresiva escalada en estos niveles.

- **Emergente.** Práctica inicial y reactiva.
- **Controlado.** Se ha implantado el ciclo PDCA. Existen objetivos anuales, un ciclo de retroalimentación y la gestión de este proceso es "*business as usual*" como la de otros. Se presta tanta atención a este proceso como al de cumplir los objetivos de los procesos financieros.
- **Optimizado.** Ha pasado a formar parte de la cultura organizacional y existe un esfuerzo continuo por mejorar este proceso como pudiera suceder con la atención al usuario o el sistema de información. Se han alcanzado las mejores prácticas y se ha pasado de imitar a liderar.

Los factores 4.2.1 y 4.3.1 indagan si se realizan ciertas acciones que hacen progresar en el nivel de madurez.

Mejores prácticas

- Comprenda en primer lugar, antes de hacer nada en este aspecto, en profundidad lo que es un modelo de madurez[7].
- Valore su actual estado de madurez con una herramienta actualizada[8].
- Cuantifique, adaptando a su caso materiales como "BCI White Paper Q3: How to measure BCM programme Maturity".

7 https://www.virtual-corp.com/bcmm
https://www.techtarget.com/searchdisasterrecovery/tip/Business-continuity-maturity-model-An-at-a-glance-guide
https://www.agilityrecovery.com/article/key-aspects-mature-business-continuity-program
https://www.linkedin.com/pulse/ey-common-challenges-business-continuity-management-karam-%D8%A3%D8%AD%D9%85%D8%AF-%D9%83%D8%B1%D9%85

8 https://kpmg.com/ae/en/home/services/advisory/risk-consulting/kpmg-governance-regulatory-compliance/business-continuity-management/bcm-maturity-assessment-tool.html

5. Diseño de un plan

5.1. Filosofía de la metodología empleada

Un plan de continuidad de negocio deber ser concebido como un documento vivo. Tiene por objeto la continuidad de distintos "negocios", que realmente son áreas de responsabilidad y por ello de interés. Son en nuestro caso los objetivos de las AT. Son satisfechos en cada momento con procesos que evolucionan ante nuevas necesidades o con la incorporación de nuevas tecnologías.

El documento PCN que se diseñe y elabore bajo los principios de esta **guía** deberá tener sucesivas versiones. El diseño del propio plan debe atender esta característica y en esta metodología se recomienda la creación de una versión anual.

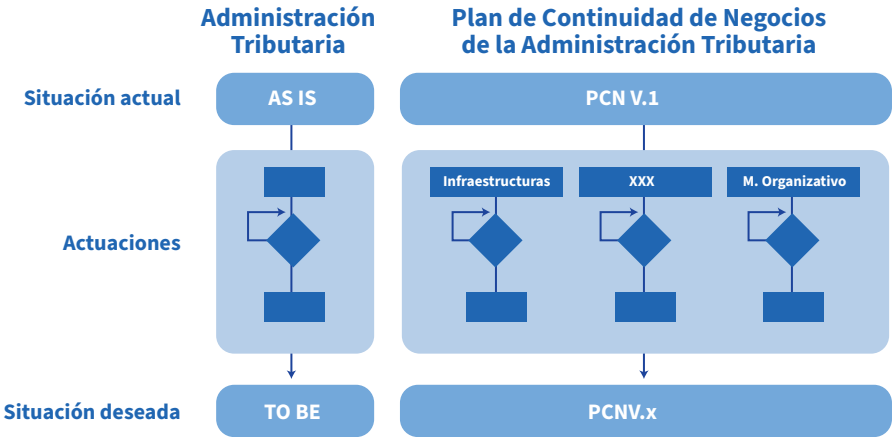
La metodología de diseño que describimos utiliza un ciclo de actividad mediante el que el PCN se actualiza y perfecciona:

$$\text{PCN}_{\text{actual}} = \text{PCN}_{\text{año anterior}} + \text{Cambios en cuatro Planes de Actuación Trimestrales}$$

El ciclo de gestión PDCA puede tener muchos objetos de interés, tantos como se gestionen. En la Figura 4 se pone de manifiesto su utilización en dos de ellos. El principal de ellos es aquel mediante el que la AT evoluciona desde su situación actual hasta la deseada. Otro, necesario pero muy distinto, del que aquí nos ocupamos, es el ciclo mediante el que se tiende a garantizar que la AT continúe su negocio, que idealmente puede ser bueno, pero que puede ser en parte malo.

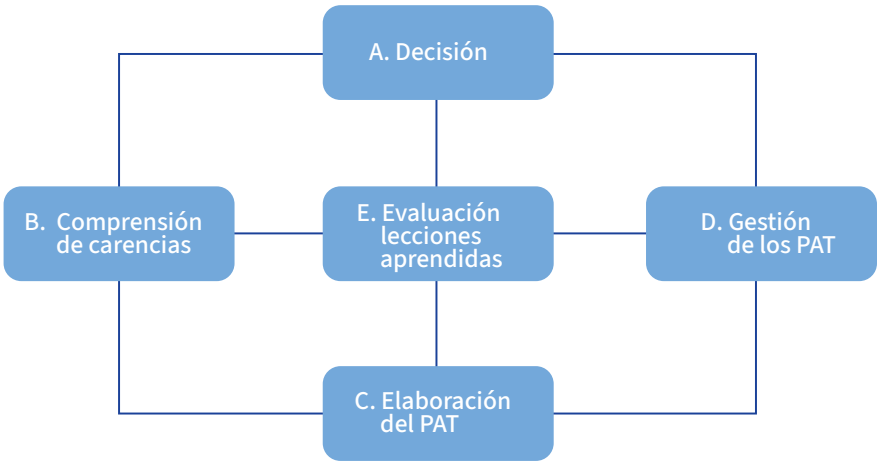
Para garantizar la continuidad de todos los procesos y servicios el Plan de Continuidad debe atender, entre otros, a datos, información, servicios, e infraestructuras. Los más importantes están recogidos en el cuestionario. Mediante Planes de Actuación Trimestrales (PAT), se logrará que el PCN se perfeccione y con ello se mejorará, en parte, la gestión de la AT.

Figura 3. Estructura y ciclo del PCN usando PDCA



Siguiendo la estrategia PDCA recomendada por el CIAT, el ciclo de actividades se muestra en la *Figura 5*.

Figura 4. Ciclo trimestral



5.2. Ciclo de actividades

El punto de partida de toda actividad es la manifestación de propósito de la institución, que hace visible su actitud. Se adopta una decisión porque existe una visión y la actitud adecuada. Este propósito se debe sostener en el tiempo. El desarrollo de las tareas a realizar se desglosa a continuación.

5.2.1. Decisión de la alta dirección

El punto de partida para iniciar el diseño debe ser la decisión expresada por la Alta Dirección que, en su Plan Estratégico o por otros medios, anuncia su interés y compromiso por garantizar la Continuidad de Negocio y señala una Unidad responsable.

Después y no antes de que exista el mandato y una persona o unidad responsables se inicia la actividad ejecutando las siguientes tareas del ciclo.

5.2.2. Comprensión de carencias

Puede suceder que en administraciones tributarias de pequeños y medianos ingresos no exista un PCN (CIAT, 2024). Dicho lo anterior, todas las organizaciones tributarias tienen una tradición de siglos y una experiencia informática de décadas, por lo que sin duda existen, en todos los casos, prácticas razonables y medidas informáticas relacionadas con la seguridad, aunque puede que las acciones de los distintos departamentos no contengan elementos que propicien de forma sistemática la continuidad.

La Unidad o persona encargada deberá recabar la información necesaria para elaborar el plan y para ello debe cubrir las siguientes fases:

- **Recabar conocimiento de la situación.**
  - Obtención de conocimiento experto local.
  - Autoevaluación mediante un cuestionario.
  - Síntesis de los cuestionarios.
  - Identificación de los servicios críticos.
  - Priorización de los servicios.
  - Identificación de las amenazas.
  - Gradación de las amenazas.
- **Elaboración de Estado de Situación (AS IS).**
- **Identificación del Estado deseable (TO BE).**
- **Análisis de las carencias.**
- **Segmentación de riegos y acciones.**
  - Diseño del plan.

Recabar conocimiento de la situación

Obtención de conocimiento experto local

- **Riesgos conocidos singulares.** Cada AT es consciente de riesgos que le son propios.
- **Riesgos emergentes.** Riesgos que aún no se han manifestado pero que podrían tener un impacto significativo en el futuro, tales como nuevas tecnologías, cambios regulatorios o amenazas locales. Es necesario revisar periódicamente los riesgos. Donald Rumsfeld dijo: "Los informes que dicen que algo no ha sucedido siempre me resultan interesantes, porque, como sabemos, hay cosas que se saben, cosas que sabemos que sabemos. También sabemos que hay cosas que se desconocen, es decir, que sabemos que hay algunas cosas que no sabemos. Pero también hay cosas que no sabemos que no sabemos". Coincidimos con él. Existen amenazas como las relacionadas con la ciberseguridad en las que al menos sabemos lo que no sabemos y buscamos expertos que nos ayuden, pero para problemas como garantizar que daremos el servicio suceda lo que suceda, para ser resilientes ¿Cómo sabremos lo que no sabemos?
- **Interdependencias.** Hay que valorar no de forma abstracta, sino particularizadamente la repercusión que un riesgo de un tercero, a priori, ajeno, puede implicar en la organización. Por ejemplo, hay países en los que solo una o dos factorías de software tienen el tamaño necesario para atender a la AT. ¿Qué se puede hacer si quiebran o incumplen?

  En el aspecto funcional, la participación de la AT en servicios complejos como la Ventanilla Única genera, por ejemplo, que la Aduana no pueda otorgar el levante a las mercancías sin que los sistemas de los servicios para-aduaneros o de los puertos estén activos. El Plan de Continuidad de Negocio deberá prever sistemas de despacho alternativos.

  El filósofo francés Gilles Deleuze mostró que es más adecuado para describir el mundo de hoy el concepto de rizoma que el de jerarquía. Todo está relacionado con todo. Todos somos dependientes de todos. Los *third-party risks* son complejos porque cada uno de nuestros partners son dependientes. La única defensa que tenemos es comprender que las redes complejas son más resilientes si están poco acopladas.
- **Resistencia al cambio.** Los presupuestos en las AT son continuistas. Conseguir recursos para satisfacer en vez de necesidades visibles, por ejemplo, el mantenimiento de edificios, para priorizar amenazas inciertas requiere vencer legitimas resistencias. Muchas organizaciones han reconocido que, a diferencia de otras responsabilidades para cuya satisfacción prima la excelencia técnica, para impulsar un PCN es preciso otro tipo de perfil. Debemos pensar que la misión de líder es llevar una organización desde donde estaba a donde nunca ha estado y no la de saber lo que casi nadie más sabe.
- **Activos invisibles.** Hay que tener presentes todos los activos con los que se cuenta, para poder determinar problemas y vulnerabilidades que puedan ocasionarse en cada uno de ellos, teniendo en cuenta la dependencia de los mismos. Aunque parezca algo obvio, según un informe de Gartner,

aproximadamente el 30% de las organizaciones no tienen una visibilidad adecuada de sus activos TI. Y sobre todo recuerde que los activos inmateriales (e.g: el conocimiento) son invisibles.

Autoevaluación con el cuestionario

Con esta práctica y con la ayuda del **cuestionario** que la Guía contiene en su anexo, se cuantifica la situación inicial. La persona encargada impulsará proactivamente que sea cumplimentado el cuestionario por tantas personas y unidades como considere razonable. El cuestionario será cumplimentado por los responsables de Tecnologías de la Información (TI), sin duda, pero también por los de contratación, recursos humanos, asistencia al contribuyente y por quienes la Unidad que impulse la actividad considere aconsejable. Es muy posible que muchos de ellos puedan responder a algunas de las secciones del cuestionario, lo que es aceptable y muy útil.

Síntesis de los cuestionarios. Utilizando la hoja de cálculo se crearán tantos bloques de columnas de puntuación como encuestados. Al final se obtendrá la media de las puntuaciones normalizadas y con ellas se obtendrán los diagramas de araña.

Figura 5. Visualización de las carencias

Área	Indicador	Factor		Respuesta	Resultado	Normalizado	
						Resultado	Objetivo
1. ACTITUD	1.1. Liderazgo y Normas	1.1.1	Organizativos	A	12	0.67	1.00
		1.1.2	Procedimientos	A			
	1.2. Planes	1.2.1	Actuaciones	B			
	1.3. Actividades	1.3.1	Impulso	C			
2. VISIÓN	2.1. Visión tecnológica	2.1.1	Innovación tecnológica	A	21	0.54	1.00
		2.1.2	Innovación metodológica	B			
	2.2. Visión organizativa y procedimental	2.2.1	Cultura de Resiliencia	B			
		2.2.2	Enfoque en la atención al contribuyente y/o ciudadano	A			
	2.3. Gestión del riesgo	2.3.1	Activos de la organización	A			
		2.3.2	Análisis de riesgos	C			
		2.3.3	Gestión de los riesgos	C			
		2.3.4	Profundidad	C			

Identificación de los servicios críticos, los activos que los sustentan y los compromisos

Para prestar un servicio, es necesario utilizar recursos (personal, instalaciones, información, dispositivos hardware, software, etc.). Los activos se utilizan para prestar servicios.

Priorización de los servicios. Es preciso ordenar los servicios por prioridad comprendiendo los que son críticos y los activos que los soportan. El problema actual es que todo está relacionado y demasiadas cosas son críticas, porque si cae una caen todas. El "*assessment*" por ello debe ser sistemático. Se debe inventariar juiciosamente todos los activos de que se dispone. El indicador 2.3.1 indaga sobre su existencia reclamando que sea "por tipos", esto es considerando también los inmateriales, preguntándose si se trata de un inventario "vivo" con responsables de "mantenimiento" o una mera lista de aquello que se ha comprado.

Se debe determinar qué tiempo de pérdida de cada servicio podría ser "asumible", pues su **magnitud es un indicador de su prioridad**. Se prestará especial atención a la existencia de plazos objetivos, como los establecidos por las normas para las devoluciones o para presentación de declaraciones.

Identificación de las amenazas

A continuación, se realizará un inventario, **con imaginación** moderada por el realismo, de las amenazas existentes. Las preguntas del indicador 2.3.2 investigan si existe una clasificación "jerárquica" de la relación entre los riesgos y amenazas. Su existencia permitirá relacionar la jerarquía de los riesgos con la de los servicios y activos.

La perspectiva debe ser amplia, la del negocio y no la más focalizada de las TIC, por lo que aspectos como los servicios de comunicación con los contribuyentes son básicos.

Gradación de las amenazas

Las amenazas deben ser graduadas por impacto. Sus tipos son muchos: catástrofes naturales, fuego, fallos en el suministro eléctrico, ataques terroristas, interrupciones organizadas o deliberadas, cuestiones legales, huelgas de empleados, conmoción social o disturbios, virus, amenazas y ataques informáticos, etc., e incluso como hemos experimentado recientemente que las grandes plataformas experimenten incidentes serios. Su naturaleza y frecuencia dependerán de muchos factores: situación del Centro de Procesos de Datos (CPD), ubicación del país, actividad sísmica de la zona, actividad volcánica de la zona y factores personales como el resentimiento de los empleados o la indignación de los contribuyentes. Esto hace que el análisis cuantitativo basado en frecuencias observadas sea muy difícil pues no hay bibliografía de casos comparables.

Elaboración del estado de situación (AS IS)

Con los elementos de información anteriores es posible elaborar un documento que describa de forma adecuada el estado de las cosas al que denominamos **Estado de Situación AS IS**.

Elaboración del estado deseable (TO BE)

Utilizando la información de los expertos y la ayuda proporcionada por el cuestionario, que pone de manifiesto las carencias se redacta el Estado Deseable (TO BE), en el cual se deben considerar los elementos descritos a continuación.

Análisis de las carencias

El análisis de carencias o GAP análisis pondrá de manifiesto los componentes del camino que habrá que recorrer y que deberá tener en cuenta el diseño del Plan de Continuidad.

Se valorará, primero de forma global y luego por áreas de interés (Informática, atención al contribuyente, recaudación), las carencias detectadas.

Las deficiencias se aprecian de dos formas, gráfica y numérica, como se muestra en la *Figura 6*.

a) De forma numérica, por la diferencia entre la puntuación normalizada en la hoja de cálculo.

b) De forma visual por la diferencia entre la circunferencia exterior, situación de máxima puntuación y la observada. En ella se aprecia de forma inmediata las áreas en las que la diferencia es mayor.

Segmentación de riesgos y acciones

Se creará un inventario de acciones a realizar con los datos de la *Figura 7*.

Figura 6. Segmentación de medidas

Medida	Identificador		Viabilidad	Resultado	Max
Obtener estadísticas de incidencias por tipo	1	Alta	Medio	1.3.1	B-->A
Crear el documento "existe un documento formalmente aprobado donde se indiquen planes y proyectos..."	2	Alta	Medio	2.3.3	B-->A

Se realizará una estimación de costes, en jornadas y económico que permitirá conocer la viabilidad de las medidas y **segmentarlas** por impacto y viabilidad.

Figura 7. Segmentación para crear una matriz de riesgo

Viabilidad / Impacto	Baja	Media	Alta
Alta	1	4,6	5,7,9
Media		2	8
Baja	3	10	11

De la matriz de riesgo y oportunidad construida se deduce cuál es el orden racional. Se deberá comenzar por las medidas de alta viabilidad (las que se pueden hacer con los recursos disponibles) y que tendrán alto impacto, siendo menos interesantes a aquellas que sirven para poco y no hay recursos para hacerlas.

Se deberá determinar un tiempo de ciclo para las actuaciones, de forma que el control periódico sea eficaz. Recomendamos tres meses.

Los atributos de cada actuación son:

- Descripción de las tareas
- Asignación de responsables
- Fijación de criterios de finalización.

Materialización del plan en un documento

1. Se realizará la versión del PCN V.0. Llegados a este punto de disponer de los materiales para materializar el Plan. Existen muchos modelos en las referencias bibliográficas contenidas en esta Guía. Se sugiere usarlos solo como referencia pues lo fundamental es que el Plan sea estudiado y aprobado. Para ello

Utilice como formato uno que sea habitual.

Incluya un resumen ejecutivo de no más de dos hojas en el que incluya:

- Los resultados de la evaluación
- Haga referencia al documento diseñado
- Describa los objetivos que se deberían cubrir en el primer ejercicio, **sus costos** y los beneficios que supondrían para la AT.
- Solicite que se asignen responsables
- Solicite que se apruebe formalmente el documento.
- Incluya como Anexo el PCN

2. Se comunicará a la Alta Dirección.

3. Se solicitará su aprobación. Si es aprobado, después de **incorporar las correcciones necesarias se dispone de un PCN V.1 que nos sitúa en la cúspide** de la *Figura 4*.

4. En este momento el PCN se socializa. Se comenzará la tarea de evolucionar desde la situación actual creando normas, unidades y realizando actividades para lo que inicia el ciclo de gestión con Planes Trimestrales. Comienza el Ciclo de Gestión descrito puesto que ya se dispone de un objetivo, cumplir un mandato de la Alta Dirección.

5.2.3. Creación de los Planes de Actuación Trimestral (PAT)

Se creará el cronograma del Plan de Actuaciones Trimestral, tenido en cuenta que puede suceder que una persona o Unidad deba desarrollar más de una tarea y que es posible que no pueda hacerlo simultáneamente. Conviene calificarlas en grupos: a) Preventivas. Ejemplo de este tipo de medidas sería ubicar el CPD en una planta segunda o tercera, de manera que se evite que pueda inundarse en caso de subida de un río que pase cerca, b) Reactivas. Medidas y salvaguardas en el momento en el que ocurre el desastre, de manera que mitiguen el impacto; c) Restauradoras.

5.2.4. Gestión de los PAT

Durante cuatro trimestres se realizarán las actuaciones de control, seguimiento e impulso que parezcan aconsejables y al final del cuarto hay que:

1. Determinar los riesgos residuales.
2. Identificar medidas y salvaguardas para reducir el riesgo residual y aceptación de un riesgo objetivo.

5.2.5. Evaluación

Al finalizar el año se evaluará el resultado pues no todas las actuaciones habrán sido un éxito. Siempre quedará un remanente de riesgos y de tareas por hacer cuyo control será objetivo para el siguiente ciclo de la fase de gestión (PDCA).

Es necesario iterar estos pasos de manera periódica porque cualquiera de los componentes que lo forman pueden variar: servicios, activos, amenazas, salvaguardas, nivel de riesgo aceptado, etc. Asimismo, deberá realizarse esta revisión siempre que se produzcan cambios importantes, de forma que se pueda adaptar el nivel de riesgo a las circunstancias cambiantes que toda organización aborda en el cumplimiento de su misión.

Con las lecciones aprendidas o bien se modificará el Plan o se perfeccionarán los modos de gestión o de actuación.

6. Referencias

Ali, Q. S. A., Hanafiah, M. H., & Mogindol, S. H. (2023). en "Systematic literature review of Business Continuity Management (BCM) practices: Integrating organisational resilience and performance in Small and medium enterprises (SMEs) BCM framework. *Publicada En International Journal of Disaster Risk Reduction,(99) Ofrecen Una Revision Complete y Global de La Literatura Sobre Continuidad de Negocio*.

Arenas, A. E., Massonet, P., Ponsard, C., & Aziz, B. (2015). *Goal-Oriented Requirement Engineering Support for Business Continuity Planning*. Goal-Oriented Requirement Engineering Support for Business Continuity Planning.

Ates, A., Bititci, U. (2011). Change process: A key enabler for building resilient SMEs. Int. J. Prod. Res. 2011, 49, 5601–5618.

Aven, T. (2010a). *Misconceptions of risk*. Chichester, Wiley.

Aven, T. (2010b). On how to define, understand and describe risk. *Reliability Engineering & System Safety*, 95(6), 623-631.

Aven, T. (2011). *Quantitative Risk Assessment: The Scientific Platform*. Cambridge University Press.

Aven, T. (2012). The risk concept-historical and recent development trends. *Reliability Engineering & System Safety*, 99, 33-44.

Aven, T. (2014*). Risk, Surprises and Black Swans: Fundamental Ideas and Concepts in Risk Assessment and Risk Management*. Routledge.

Aven, T. (2015a). Implications of black swans to the foundations and practice of risk assessment and management. *Reliability Engineering & System Safety*, 134, 83-91.

Aven, T. (2015b). *Risk Analysis* (2nd ed.). Wiley.

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, 253(1), 1-13.

Aven, T., Ben-Haim, Y., Andersen, H., Cox, T., Droget, E., Greenberg, M., Guikema, S., Kroger, W., Renn, O., Thompson, K., & Zio, E. (2018).

Bailey, D. (2015). Business continuity management into operational risk management: Assimilation is imminent resistance is futile. *Journal of Business Continuity & Emergency Planning*, 8(4), 290-294.

Bakar, Z. A., Yaacob, N. A., & Udin, Z. M. (2015). The effect of business continuity management factors on organizational performance: A conceptual framework. *International Journal of Economics and Financial Issues*, 5(1S), 128-134.

Baldwin, S. (2019). Business continuity management as an operational risk service provider: An approach to organizational resilience. *Journal of Business Continuity & Emergency Planning*, 13(2), 102-110.

Banking Supervision Consultative Document, B. C. (2024). *Principles for the sound management of third party risk Issued for comment by*.

Bankole, F. O. (2016). *A Normative Process Model for ICT Business Continuity Plan for Disaster Management in Small, Medium and Large. A Normative Process Model for ICT Business Continuity Plan for Disaster Management in Small, Medium and Large Benefits and Bottom Lines on Backups*. (2019). How to Choose a Data Recovery Solution.

Bernstein, P. L. (1996). *Against the gods: The remarkable story of risk*. Wiley New York.

Bhimanprommachak, V. (2020). *Leading Your Team through a Crisis* (harvardbusiness.org)

Botha, J., & Solms, R. V. (2004). A Cyclic Approach to Business Continuity Planning. *Information Management & Computer Security*, 12(4), 328-337.

Butkovic, M. J., & Caralli, R. A. (2013). Advancing Cybersecurity Capability Measurement Using the CERT ®—RMM Maturity Indicator Level Scale. En *Advancing Cybersecurity Capability Measurement Using the CERT ®—RMM Maturity Indicator Level Scale*.

Chapman, R. (2021). *Simple tools and techniques for enterprise risk management* (2nd ed.). Wiley.

Charoenthammachoke, K., Leelawat, N., Tang, J., & Kodaka, A. (2020). Business continuity management: A preliminary systematic literature review based on science direct database. *Journal of Disaster Research*, 15(5), 546-555. https://doi.org/10.20965/jdr.2020.p0546

C.O.R.E. (s. f.). *Risk Analysis on the development of a Business Continuity Plan*. https://core.ac.uk/download/pdf/159125441.pdf

Corporation, E. (2015). *RSA® ARCHER® MATURITY MODEL: BUSINESS RESILIENCY. RSA® ARCHER® MATURITY MODEL. BUSINESS RESILIENCY*.

Corporation, V. (2007). *Business Continuity Maturity Model*.

Crue, C., & Francis, K. L. (2020). As the field of emergency management evolves, is it time to enhance its training methods? *Journal of Business Continuity & Emergency Planning*, 14(1), 65-74.

Curtin, T., Hayman, D., & Husein, N. (2005). The Crisis Management Team. En Managing a Crisis. Palgrave Macmillan. https://doi.org/10.1057/9780230509306_12

Dekker, S., Hollnagel, E., Woods, D., & Cook, R. (2008). *Resilience engineering: New directions for measuring and maintaining safety in complex systems* [Final report.].

Deloitte. (2023). *Navigating the headwinds*.

Disaster safety. *Preparing Your Business for a Severe Weather Emergency*. (2020).

Dreyfus, S. E. (2004). The five-stage model of adult skill acquisition. *Bull. Sci. Technol. Soc*, 24(3). https://doi.org/10.1177/0270467604264992

Edimburgo, U. (s. f.). *Business Continuity Management and Framework*.

Ernst & Young. (2023). . *In an uncertain world, how do you see every angle? 2023 EY Global Third-Party Risk Management Survey* https://www.ey.com/content/dam/ey-unified-site/ey-com/en-gl/insights/risk/documents/ey-global-third-party-risk-management-survey-v3.pdf.

Fagel, M. J., Fulmer, K. L., & Rothstein, P. J. (2014). *Crisis Management and Emergency Planning*. CRC Press.

Fischbacher-Smith, D. (2017). When organizational effectiveness fails: Business continuity management and the paradox of performance. *Journal of Organizational Effectiveness: People and Performance*, 4(1), 89-107. https://doi.org/10.1108/JOEPP-01-2017-0002

Flin, R. (1996). *Sitting in the hot seat: Leaders and teams for critical incident management*. Wiley.

Gallagher, M. (2003). *Business Continuity Management*. Business Continuity Management.

Goh, M. H. (2021). Managing Your Business Continuity Planning Project. Business Continuity Management Planning Series (3rd ed.). Singapore: GMH Pte Ltd.

Gottschalk, P., & Solli-Sæther, H. (2005). *Critical success factors from IT outsourcing theories: An empirical study*. Industrial Management and Data Systems.

Guía de verificación de cumplimiento del Esquema Nacional de Seguridad 808. (s. f.-a). https://www.ccn-cert.cni.es/es/800-guía-esquema-nacional-de-seguridad/518-ccn-stic-808-verificacion-del-cumplimiento-de-las-medidas-en-el-ens/file.html

Guía de verificación de cumplimiento del Esquema Nacional de Seguridad 808. (s. f.-b). https://www.ccn-cert.cni.es/es/800-guía-esquema-nacional-de-seguridad/518-ccn-stic-808-verificacion-del-cumplimiento-de-las-medidas-en-el-ens/file.html

Guía de verificación de cumplimiento del Esquema Nacional de Seguridad 808. (s. f.-c). https://www.ccn-cert.cni.es/es/800-guía-esquema-nacional-de-seguridad/518-ccn-stic-808-verificacion-del-cumplimiento-de-las-medidas-en-el-ens/file.html

Hambrick, D. C., & Mason, P. A. (1984). Upper Echelons: The Organization as a Reflection of Its Top Managers. *The Academy of Management Review*, 9(ue 2), 193-206.

Hancox, M., & Hackney, R. (2000). IT outsourcing: Frameworks for conceptualizing practice and perception". *Information Systems Journal*, 10(3), 217-237.

Harrison, C. (2008). *Blog-The Effects of a Power Outage on a Business*.

Herramienta PILAR del Centro Criptológico Nacional (CCN)—Incluyendo Manual de Usuario. (s. f.). https://pilar.ccn-cert.cni.es/index.php/pilar/pilar

Hiles, A. (2012). *Definitive Handbook of Business Continuity Management*.

Hiles, A., Merna, T., & Al-Thani, F. F. (2010). The definitive handbook of business continuity management. John Wiley & Sons.

Hollnagel, E. (2011). Epilogue: RAG-The Resilience Analysis Grid. En E. Hollnagel, J. Pariès, J. Wreathall, & D. D. Woods (Eds.), *Resilience engineering in practice: A guidebook* (pp. 275-296). Ashgate.

Hollnagel, E. (2014). Becoming resilient. En P. C. Nemeth & E. Hollnagel (Eds.), *Resilience engineering in practice*. Volume 2,: *Becoming resilient* (pp. 179-192). Ashgate publishing.

I.S.O. (2018). *Risk management*.

I.S.O./Guide. (s. f.). *Risk management—Vocabulary*.

J., & Helsloot, I. (2020). Organisational resilience: Shifting from planning-driven business continuity management to anticipated improvisation. *Journal of Business Continuity & Emergency Planning*, 14(2), 102-109.

Junttila, J. (2014). *A Business Continuity Management Maturity Model. A Business Continuity Management Maturity Model*.

Korsten, G., Ozkan, B., Aysolmaz, B., Mul, D., & Turetken, O. (2024). Understanding Capability Progression: A Model for Defining Maturity Levels for Organizational Capabilities. En H. Aa, D. Bork, R. Schmidt, & A. Sturm (Eds.), *Enterprise, Business-Process and Information Systems Modeling*. BPMDS EMMSAD 2024 2024. *Lecture Notes in Business Information Processing* (Vol. 511). Springer. https://doi.org/10.1007/978-3-031-61007-3_26

K.P.M.G. (2023). https://assets.kpmg.com/content/dam/kpmg/sg/pdf/2023/10/cyber-brochure-managed-third-party-risk-management-services.pdf https://assets.kpmg.com/content/dam/kpmg/sg/pdf/2023/10/cyber-brochure-managed-third-party-risk-management-services.pdf

Linnenluecke, M. K. (2017). Resilience in business and management research: A review of influential publications and a research agenda: Resilience in business and management research. *International Journal of Management Reviews*, 19(1), 4-30. https://doi.org/10.1111/ijmr.12076

Mehravari, D. N. (2016). *Everything You Always Wanted to Know About Maturity Models*. Carnegie Mellon University.

Mingay, S. (2002). *Outlining the Gartner BCP Maturity Model*. Gartner INC.

Paton, D.; Buergelt, P. (2019). Risk, transformation and adaptation: Ideas for reframing approaches to disaster risk reduction. Int. J. Environ. Res. Public Health.

Patriarca, R., DiGravio, G., Costantino, F., Falegnami, A., & Bilotta, F. (2018). An analytic framework to assess organizational resilience. Safety and Health at Work, 9(3), 265-276. https://doi.org/10.1016/j.shaw.2017.10.005

Pinto, D., Fernandes, A., Silva, M. M., & Pereira, R. (2022). *Maturity Models for Business Continuity.A Systematic Literature Review Instituto Superior Técnico, INOV*. Instituto de Engenharia de Sistemas e Computadores Inovação.

Poeppelbuβ, J., Niehaves, B., Simons, A., & Becker, J. (s. f.). Maturity Models in Information Systems Research. Literature Search and Analysis, "*Communications of the Association for Information Systems*, 29,2011.

Por sus siglas en inglés será de aplicación a partir del 17 de febrero de 2024.
PwC Third-party risk management. (s. f.). https://www.pwc.in/assets/pdfs/risk-consulting/managing-third-party-risks-in-the-energy-and-infrastructure-sector.pdf

R.A, C., Falkenburg, J., White, T. P., & Tracy, D. K. (s. f.). Crisis teams: Systematic r eview of their effectiveness in practice Hayes, Erika Leading Teams in Crisis Situations: From Chaos to Extraordinary Performance. https://jamesandwooten.com/wp-content/uploads/2020/04/Leading-Teams-in-Crisis.pdf

Randeree, K., Mahal, A., & Narwani, A. (2012). *A Business Continuity Management Maturity Model for the UAE Banking Sector. A Business Continuity Management Maturity Model for the UAE Banking Sector*.

Renn, O., Laubichler, M., Lucas, K., Kröger, W., Schanze, J., Scholz, R.W. and Schweizer, P.-J. (2022), Systemic Risks from Different Perspectives. Risk Analysis, 42: 1902-1920. https://doi.org/10.1111/risa.13657

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. (s. f.-a). https://boe.es/buscar/act.php?id=BOE-A-2022-7191

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. (s. f.-b). https://boe.es/buscar/act.php?id=BOE-A-2022-7191

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. (s. f.-c). https://boe.es/buscar/act.php?id=BOE-A-2022-7191

Release, F. F. I. E. C. P. (2015). *The Federal Financial Institutions Examination Council (FFIEC)*. https://www.ffiec.gov/press_2015.htm

Reserve, F. (2024). *Third-Party Risk Management A Guide for Community Banks*. https://www.occ.gov/news-issuances/news-releases/2024/pub-third-party-risk-management-guide-for-community-banks.pdf

Risk Management: A Maturity Model Based on ISO 31000. (s. f.-a). https://www.researchgate.net/publication/319218604_Risk_Management_A_Maturity_Model_Based_on_ISO_31000

Risk Management: A Maturity Model Based on ISO 31000. (s. f.-b). https://www.researchgate.net/publication/319218604_Risk_Management_A_Maturity_Model_Based_on_ISO_31000

Röglinger, M., & Pöppelbuß, J. (2011, junio). What makes a useful maturity model? A framework for general design principles for maturity models and its demonstration in business process management. *In Proceedings of the 19th European Conference on Information Systems*.

Sahebjamniaa, N., Torabi, S. A., & Mansouri, S. A. (2014). Integrated Business Continuity and Disaster Recovery Planning: Towards Organizational Resilience. *Integrated Business Continuity and Disaster Recovery Planning: Towards Organizational Resilience*, 13.

SAMA Business Continuity Management and Framework. (s. f.).

Sandercock, L. (2003). Out of the closet: The importance of stories and storytelling in planning practice. *Planning Theory & Practice*, 4(1), 11-28. https://doi.org/10.1080/1464935032000057209

Shah, L. S., A, & Vernadat, F. (2009). Maturity assessment in risk management in manufacturing engineering. *IEEE Syst. Conf*, 296-301.

Smit, N. (2005). *Business Continuity Management. A Maturity Model*. Snedaker, S.

Standardization, I. O. F. (2011). *ISO 22320 security and resilience—Emergency management—Guidelines for incident management*.

Tangenes, T., & Steen, R. (2017). *The trinity of resilient organisation: Aligning performance management with organisational culture and strategy formation* (Vol. 7). International Journal of Business Continuity and Risk Management.

Tarhan, A., Turetken, O., & Reijers. (2016). H.A.: Business process maturity models: A systematic literature review. *Inf. Softw. Technol*, 75, 122-134. https://doi.org/10.1016/j.infsof.2016.01.010

Thekdi, S., & Aven, T. (2019). An integrated perspective for balancing performance and risk. *Reliability Engineering & System Safety*, 190, 106525. https://doi.org/10.1016/j.ress.2019.106525

Thordsen, T. & Bick. (s. f.). M.: A decade of digital maturity models: Much ado about nothing? *Inf. Syst*. https://doi.org/10.1007/s10257-023-00656-w

Tuffley, A. (2007). Comparing Maturity Models. *PMOZ Conference*, 10.

United Nations Office for Disaster Risk. Sendai Framework for Disaster Risk Reduction 2015–2030; 2015. Available online: https: //www.preventionweb.net/files/43291_sendaiframeworkfordrren.pdf (accessed on 13 July 2021)

Vegt, G. S., Essens, P., Wahlström, M., & George, G. (2015). Managing risk and resilience. *Academy of Management Journal*, 58(4), 971-980. https://doi.org/10.5465/amj.2015.4004

Weick, K. E. (1993). The collapse of sensemaking in organizations: The Mann Gulch disaster. *Administrative Science Quarterly*, 38(4), 628-652. https://doi.org/10.2307/2393339

Zou, P., Chen, Y., & Chan, T. (2010). *Understanding and Improving Your Risk Management Capability: Assessment Model for Construction Organizations* (August, pp. 854-864,).

Guías y normas

Atlassian – Buenas prácticas para respuesta ante incidentes https://www.atlassian.com/es/incident-management/incident-response/best-practices#one-more-thing

CCN - ENS. Guía de implantación (Copias de seguridad) https://www.ccn-cert.cni.es/es/series-ccn-stic/800-guía-esquema-nacional-de-seguridad/505-ccn-stic-804-medidas-de-implantancion-del-ens/file?format=htmlENS. Guía de implantación

CCN guía para procedimiento de generación de copias de respaldo y recuperación de información https://www.ccn-cert.cni.es/es/series-ccn-stic/800-guía-esquema-nacional-de-seguridad/540-ccn-stic-822-procedimientos-de-seguridad-anexo-iii/file?format=html

Criterios de seguridad para productos de copia de seguridad https://www.ccn-cert.cni.es/es/pdf/guías/series-ccn-stic/guías-de-acceso-publico-ccn-stic/3983-guía-140-anexo-f-5-copias-de-seguridad/file?format=html

INCIBE- Guía de copias de seguridad https://www.incibe.es/sites/default/files/contenidos/guías/guía-copias-de-seguridad.pdf

Informes sobre tendencias en problemas de ransomware https://news.sophos.com/en-us/2024/04/30/the-state-of-ransomware-2024/ https://www.techtarget.com/searchsecurity/feature/Ransomware-tren

CCN-TEC 010 - La disponibilidad de los sistemas TIC https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/boletines-pytec/496-ccn-tec-010-la-disponibilidad-de-los-sistemas-tic/file

CCN - ENS. Guía de implantación https://www.ccn-cert.cni.es/es/series-ccn-stic/800-guía-esquema-nacional-de-seguridad/505-ccn-stic-804-medidas-de-implantancion-del-ens/file?format=htmlENS. Guía de implantación

ISO/IEC 27001 - Sistemas de Gestión de Seguridad de la Información: International Organization for Standardization. (2013). ISO/IEC 27001:2013 - Information technology – Security techniques – Information security management systems – Requirements. Norma que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI), que incluye aspectos de alta disponibilidad.

Uptime Institute. (2023). Global Data Center Survey Results. Recuperado de Uptime Institute. Informe anual que proporciona estadísticas sobre la disponibilidad y resiliencia de los centros de datos a nivel global.

RFC-3768 Virtual Router Redundancy Protocol. https://www.rfc-editor.org/rfc/rfc3768

CCN-STIC-820- Protección contra denegación de servicio https://www.ccn-cert.cni/es

Guía de gestión de ciberincidentes del CCN-CERT https://www.ccn-cert.cni.es/es/comunicacion-eventos/comunicados-ccn-cert/3921-actualizada-la-guía-de-gestion-de-ciberincidentes.html

Gestión de crisis para ciberincidentes https://www.ccn-cert.cni.es/es/informes/informes-de-buenas-practicas-bp/6936-ccn-cert-bp-29-gestion-de-crisis-para-ciberincidentes-en-entidades-locales/file.html

Ciberamenazas y tendencias https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/7188-ccn-cert-ia-3523-ciberamenazas-y-tendencias-edicion-2023/file.html

Esquema Nacional de seguridad España https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-7191

Computer Security Incident Response Team (CSIRT) Services Framework https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

7. Anexo

Cuestionario de autoevaluación base para formular el plan de continuidad de negocio

Acceda al cuestionario aquí.

Para ayudar a los que cumplimenten el cuestionario se recomienda que quienes lo coordinen:

a) Lean previamente la Guía.

b) Lean los criterios que califican una evidencia como aceptable antes de asignar la calificación a las preguntas.

c) Hagan cumplimentar el cuestionario por al menos tres personas situadas en funciones distintas de la Administración de modo que se puedan comparar a través de los resultados sus visiones sobre la Continuidad del Negocio.

En la parte inicial del cuestionario se ha incluido:

- Relación de objetos de interés para el cuestionario, sobre los que debe existir evidencia.
- Diccionario de términos técnicos utilizados.

El cuestionario para la evaluación del Plan de Continuidad de Negocio tiene la estructura que se muestra en la *Tabla1*.

Se hace observar que en el diseño del cuestionario la puntuación de las respuestas es:

A. 4 puntos

B. 3 puntos

C. 1 punto

Esta circunstancia se tiene en cuenta al obtener las puntuaciones normalizadas.

Tabla 2. Relación de indicadores y factores que deben ser avaluados

Área	1	ACTITUD	Preguntas
Indicador	1.1	Liderazgo y normas	
Factores	1.1.1	Organizativos	7
	1.1.2	Procedimientos	5
Indicador	1.2	Planes	
Factor	1.2.1	Actuaciones	5
Indicador	1.3	Actividades	
Factor	1.3.1	Impulso	5

Área	2	VISIÓN	Preguntas
Indicador	2.1	Visión tecnológica	
Factores	2.1.1	Innovación tecnológica	3
	2.1.2	Innovación metodológica	4
Indicador	2.2	Visión organizativa y procedimental	
Factores	2.2.1	Cultura de resiliencia	5
	2.2.2	Enfoque en la atención al contribuyente y/o ciudadano	7
Indicador	2.3	Gestión del riesgo	
Factores	2.3.1	Activos de la organización	6
	2.3.2	Análisis de riesgos	6
	2.3.3	Gestión de los riesgos	6
	2.3.4	Profundidad	3

Área	3	RECURSOS	Preguntas
Indicador	3.1	Marco organizativo	
Factores	3.1.1	Requisitos normativos y buenas prácticas	6
	3.1.2	Recursos asignados al cumplimiento normativo	3
	3.1.3	Vigencia y transparencia de los planes de emergencia, contingencia y recuperación	5
	3.1.4	Procedimientos de coordinación y comunicación con terceros	5

Indicador	3.2	Infraestructuras	
Factores	3.2.1	Instalaciones de respaldo	6
	3.2.2	Suministros	8
	3.2.3	Resiliencia frente a desastres naturales	6
	3.2.4	Resiliencia frente a ataques intencionados	3
Indicador	3.3	Salvaguarda de la información	
Factores	3.3.1	Políticas y procedimientos de copia de seguridad	7
	3.3.2	Protección de copias de seguridad	5
	3.3.3	Pruebas de los procedimientos de copia de seguridad y recuperación	3
Indicador	3.4	Servicios de terceros	
Factores	3.4.1	Proveedores	7
	3.4.2	Cloud	7
	3.4.3	Cadena de suministro	6
Indicador	3.5	Infraestructura TI (Hardware, Software y comunicaciones) - Alta disponibilidad	
Factores	3.5.1	Política y procedimientos relacionados con la disponibilidad de los sistemas TI	4
	3.5.2	Arquitectura y operación	5
	3.5.3	Monitorización	3
	3.5.4	Evaluación y mejora continua	5
Indicador	3.6	Gestión de la seguridad y respuesta ante ciberincidentes	
Factores	3.6.1	Política y procedimientos relacionados con la ciberseguridad	3
	3.6.2	Gestión y monitorización	3
	3.6.3	Respuesta ante ciberincidentes	5
	3.6.4	Evaluación y mejora continua	8
Indicador	3.7	Recursos humanos	
Factores	3.7.1	Análisis de necesidades: roles y habilidades	5
	3.7.2	Equipos de respuesta	3
	3.7.3	Formación y entrenamiento	4

Indicador	3.8	Precariedad	
Factores	3.8.1	Por escasez	5
	3.8.2	Por rigidez	4
	3.8.3	Por contexto	6

Área	**4**	**MADUREZ**	**Preguntas**
Indicador	4.1	Cobertura	
Factor	4.1.1	¿Existe modelo BCM@M?	7
Indicador	4.2	Pruebas	
Factor	4.2.1	De actuación	5
Indicador	4.3	Gestión cuantitativa	
Factor	4.3.1	Herramientas cuantitativas	5

7.1. Objetos a los que se refiere la evidencia

El cuestionario ha sido diseñado para ofrecer una información más fiable y conclusiones más exactas que las que se podrían obtener de meras apreciaciones subjetivas. Además, se desea facilitar la comprensión de la realidad regional y la posibilidad de compartir experiencias.

La evaluación ha sido diseñada para solicitar respuestas relativas a “objetos de interés”. Es necesario que los interesados puedan discernir lo que es apariencia frente a lo que es existencia a través de la evidencia sobre realidades relevantes para un Plan de Continuidad de Negocio.

En este apartado se ofrecen criterios no exhaustivos para que los encuestados puedan evaluar la información de que disponen, favoreciendo que los resultados obtenidos tengan validez externa, esto es, puedan ser interpretados de modo uniforme y unívoco por cualquiera dentro o fuera de la Administración Tributaria.

En el área **ACTITUD** se han identificado los siguientes objetos de interés para el análisis. Para cada uno de ellos se explica el alcance de cada término.

- **Normas.** Circulares, instrucciones y otras normas aprobadas por la Dirección que son de obligado cumplimiento en toda la organización. No son consideradas normas las directrices verbales, los modos de trabajo tradicionales, las reglas de sentido común asumidas, etc.

- **Planes.** Lineamientos y estrategias de actuación que, aunque puedan tener un contenido voluntarista y orientativo establecen metas y objetivos que deben ser alcanzadas por responsables conocidos en un cierto periodo. Incluyen los estratégicos, los anuales, los operativos, etc., con un horizonte temporal. Se consideran tales los realizados por ejemplo por las unidades TI o de atención a los contribuyentes para un cierto periodo que son comunicados a la Dirección o a Terceros. No se consideran planes las ideas meramente expresadas en declaraciones, ruedas de prensa, presentaciones o documentos internos y cuyo incumplimiento no genera repercusiones.
- **Actividades.** Cualesquiera acciones planificadas en las que se pueda identificar un responsable de la ejecución, la fecha en que fueron realizadas y existan efectos, productos o entregables.

En el área **VISIÓN** se identifican los siguientes objetos de interés:

- **Presupuestos, inversiones, gastos.** No se presta atención a la diferencia contable entre inversión y gasto. Solo se pretende atestiguar si la organización ha asignado recursos escasos, materiales o financieros a un proyecto.
- **Metodologías, mejores prácticas, guías.** Se entiende como tales las metodologías documentadas y estandarizadas, pero no las formas propias de trabajar consuetudinarias. Son mejores prácticas las reconocidas oficialmente por un organismo multilateral (OECD, CIAT) o por los Ministerios o Instituciones, pero no las consideradas como tales por un responsable técnico sin más aval que su criterio. Guías son documentos detallados.
- **Centros de soporte y contacto.** Se consideran como tales las unidades organizadas cuya existencia y funciones figuran en las páginas WEB de las instituciones o en sus trípticos de asistencia y que disponen de herramientas de soporte, pero no las meras centralitas o puntos cuya única misión sea trasladar sin más responsabilidad las cuestiones suscitadas a terceros.

Dentro del indicador **RIESGOS**, del área **VISIÓN** se consideran tres factores sobre los que versa su gestión:

- **Activos.** Con este factor se quiere valorar si se gestionan los riesgos asociados a la destrucción, obsolescencia o pérdida de los activos materiales o inmateriales. Un elemento importante es la calidad del inventario (registro cualificado por atributos necesarios de los activos), ya que un elemento básico para poder gestionarlos y mantenerlos es tener conocimiento de cuáles son y sus atributos (e.g: marca, modelo, versión, fechas relevantes, etc.).
- **Análisis.** La palabra “análisis”, se sitúa en el campo semántico de “dividir”, “diferenciar” como en Química y se opone a Síntesis. Se quiere cuantificar aquí el nivel de detalle alcanzado en la consideración de las amenazas a la continuidad de negocio y por tanto la posible precisión de las respuestas en su caso.

- **Gestión de riesgos.** Con este factor se quiere poner de manifiesto si existe un modelo de gestión, como el conocido PDCA. Si es el caso la organización no solo prevé o reacciona a los riesgos, sino que gestiona los procesos orientados a lograr la resiliencia.

En el área **RECURSOS** se identifican los siguientes:

- **Estadísticas.** El resultado de contabilizar de modo sistemático datos de interés para obtener información agregada que ayude a la toma de decisiones.
- **Inventario.** Registro de bienes o productos sea cual sea su forma.
- **Inventario de activos seguros.** Inventario de los bienes no declarables como obsoletos y servicios que se ofrecen con licencias en vigor, actualizadas.
- **Relación de servicios cloud cruzada.** Inventario de los servicios prestados en *cloud* entregado por los servicios jurídicos o de contratación y la relación presentada por los responsables de IT, cuando coinciden exactamente.
- **Sistemas.** Conjunto de cosas organizadas entre sí que la AT considera cumplen eficazmente su propósito. Por ejemplo, un sistema de gestión de incendios solo será tal si existe la convicción razonable de que caso de producirse el incendio lo extinguirá.
- **Políticas.** Cursos de acción diseñados para la solución de un problema o para la consecución de un objetivo. No lo serán por tanto las meras declaraciones de intenciones.
- **Procedimientos.** Son procesos establecidos por un órgano administrativo con competencias, en los que se señalan responsables, medios y reglas de actuación.
- **Monitorización.** Supervisión constante que hace conocer al responsable si la evolución de los acontecimientos es la correcta. Puede estar o no basada en la tecnología, pero es imprescindible que estén definidas las variables que deben ser observadas y a quiénes se transmiten las desviaciones.
- **Documentación.** Textual, gráfica o numérica en cualquier soporte.
- **Protocolos de orientación a la mejora.** Formados por el conjunto de reglas que indica las actuaciones que deben ser realizadas y en qué orden, para garantizar el cumplimiento de un objetivo.
- **Cultura.** Orientación a la mejora. Está asociada a la transparencia. Se manifiesta en la existencia de publicidad de los incidentes y demoras y de las lecciones aprendidas. Se dispone de cuadros de mando en los que se ofrecen de modo realista, los avances y los fallos.

En el ámbito de **MADUREZ**:

- **Cobertura.** El proceso por el que se alcanza la madurez supone una planificación y un esfuerzo continuado conforme a un plan. Con este factor se pretende cuantificar la existencia y el alcance de ese plan, en otros términos, su extensión.
- **Cloud.** Con esta dimensión se quieren particularizar los proveedores de servicios *cloud*, esto es en la denominada "nube", teniendo en cuenta implicaciones legales que pueda suponer, tales como la ubicación de servidores, medidas de seguridad que se garantizan, ...
- **Cadena de suministros.** Es todo el proceso que envuelve al producto, desde la compra inicial hasta la resolución final, es decir, la entrega de este artículo al cliente. Se utiliza para poner de manifiesto si se tienen identificadas las cadenas de suministro de los proveedores que dan servicio, así como las condiciones que dicha cadena de suministros supone y sus implicaciones en caso de contingencia.

7.2. Actitud

Área		**1. ACTITUD**
Indicador		**1.1. Liderazgo y Normas**
Factor		**1.1.1. Organizativos**
A	Se cumplen los siguientes requisitos:	
	a)	Existe un Plan de Continuidad de Negocio (PCN).
	b)	Existe un responsable del PCN en el Comité de Dirección o bien en el Plan Estratégico de la Organización se define explícitamente el compromiso con la continuidad o la resiliencia.
	c)	Hay una persona o grupo cuya tarea es actualizar y difundir el PCN.
	d)	Existe una norma que define los componentes del Comité de Crisis y sus roles en caso de desastre.
	e)	Están definidas cuántas y cuáles son las Misiones Esenciales y las Actividades de Soporte Básicas.
	f)	Están definidos los Niveles de Servicio de las Misiones Esenciales y Actividades de Soporte Básicas y sus métricas.
	g)	Existe una unidad externa a IT (e.g: AUDITORIA) que al menos una vez por año audita la seguridad de IT.
B	Se dan al menos tres requisitos del apartado anterior.	
C	Se dan dos o menos de los requisitos del apartado primero.	

Factor	1.1.2. Procedimientos
A	Existen normas aprobadas por la Dirección que podrá activar el Comité de Crisis en las siguientes materias:
	a) De Gestión Tributaria (Acuerdos con entidades bancarias, aplazamientos).
	b) Presentación de documentación en papel fuera de los cauces habituales.
	c) Actuaciones bajo servicio IT degradado por motivos de seguridad o hacking.
	d) Gestión remota y asignación de nuevas competencias a otros órganos.
	e) Existen normas sobre reconocimiento de la situación de desastre y cómo escalar medidas en caso de emergencia y ausencia de las autoridades competentes ordinarias.
B	Se dan al menos dos requisitos del apartado anterior.
C	Se da uno o ninguno de los requisitos del apartado primero.

Indicador	1.2. Planes
Factor	1.2.1. Actuaciones
A	Existen planes que preven el uso de recursos identificados y habilitados en caso de crisis
	1 EXTERNOS proporcionados por terceros, para facilitar el cumplimiento del contribuyente y auxiliarlo en caso de desastre o de una declaración de crisis.
	2 INTERNOS para garantizar:
	a) La seguridad del personal.
	b) Proporcionar los niveles de servicio establecidos incluso en otros locales, incluso con otro personal
	c) La toma de decisiones sin demora.
	d) Mantener informado al personal y a los contribuyentes con canales alternativos
	e) Existe un Plan de Continuidad de Negocios y otro de Recuperación de Desastres o el combinado de ambos y en los dos últimos años se ha realizado alguna actuación para difundirlo o mejorarlo.
B	Se dan al menos tres casos de los indicados en el apartado anterior.
C	Se dan dos menos de los requisitos del apartado primero.

Indicador	1.3. Actividades
Factor	1.3.1. Impulso
A	Se cumplen los siguientes requisitos:
	a) En el último año se han actualizado planes relacionados con la continuidad y existe una planificación de las futuras acciones.
	b) Se han realizado acciones formativas o se ha contratado consultoría en la materia.

	c)	Se dispone de estadísticas actualizadas al último trimestre de incidencias por tipo.
	d)	Existe al menos una evaluación global documentada durante los últimos tres años de las incidencias acaecidas.
	e)	Existe una política de comunicación de incidentes y escalado categorizados por riesgo.
	f)	Se impulsa la obtención de certificaciones del personal interno y su exigencia al externo.
B	Se dan al menos tres requisitos del apartado anterior.	
C	Se cumplen al menos dos o menos requisitos del apartado primero.	

7.3. Visión

Área	**2. VISIÓN**	
Indicador	**2.1. Visión tecnológica**	
Factor	**2.1.1. Innovación tecnológica**	
A	Se cumplen los siguientes requisitos:	
	a)	La AT tiene reservado un presupuesto específico de I+D para tecnologías asociadas a la Continuidad de Negocio.
	b)	Se han realizado planes, estudios de casos de uso, etc., que cubran alguno de los aspectos del Plan de Continuidad.
	c)	Se ha actualizado la tecnología disponible en aspectos relacionados con la Continuidad de Negocio por una cuantía que supere el 25% del valor de lo instalado antes del Covid 19 en los dos últimos años.
	d)	Se ha realizado en los dos últimos años al menos un informe sobre alguna necesidad tecnológica relacionada con la continuidad tecnológica que haya sido remitido a la Alta Dirección o que se haya adquirido.
B	Se dan al menos dos de los requisitos del apartado anterior.	
C	Se da uno o menos.	

Factor	**2.1.2. Innovación metodológica**	
A	Se cumplen los siguientes requisitos:	
	a)	Se utilizan metodologías reconocidas o estándares en los procesos de Análisis y Gestión de Riesgos de continuidad.
	b)	La AT ha participado en estudios comparativos de las mejores prácticas con otras AT en los últimos tres años, o ha contratado consultorías.

	c) Se ha asistido a cursos o seminarios o realizado visitas institucionales para mejorar los procedimientos actuales.
	d) Se sigue o intenta seguir formalmente una metodología concreta y se evalúa el grado de cumplimiento.
B	Se da al menos el requisito a) del apartado anterior, o el b) o c) pero aplicados a Continuidad del Negocio.
C	No se da el requisito a) del apartado primero.

Indicador	**2.2. Visión organizativa y procedimental**
Factor	**2.2.1. Cultura de Resiliencia**
A	Se cumplen los siguientes requisitos:
	a) Existen indicadores y métricas sobre aspectos relacionados con la Continuidad de Negocio que se hayan incorporado a los Cuadros de Mando de la organización o a sus Memorias Anuales o a sus Planes Estratégicos.
	b) Los planes de formación de la organización incluyen formación en procesos y actividades que mejorarán la resiliencia.
	c) Se realizan campañas de concienciación en materia de resiliencia.
	d) Existe en el Plan de Objetivos del último año alguno relacionado con mejorar la resiliencia.
	e) Se sigue algún estándar como ISO 22301, ITIL o NIST.
B	Se da el requisito a) del apartado anterior como mínimo y además el b) el c) o el d).
C	Solo se da un requisito o menos del apartado primero.

Indicador	**2.2. Visión organizativa y procedimental**
Factor	**2.2.2. Enfoque en la atención al contribuyente y/o ciudadano**
A	Se cumplen los siguientes requisitos:
	a) La AT dispone de planes de comunicación en caso de interrupción del servicio que incluye la comunicación a los contribuyentes y ciudadanos.
	b) Existen guías internas de atención al contribuyente y/o ciudadano que incluyen protocolos relacionados con cómo gestionar la interrupción del servicio.
	c) Está prevista la existencia de un Centro de Soporte para auxilio del contribuyente en caso de desastre.
	d) Los contactos del Centro de Soporte del apartado c) figuran en la WEB de la AT y el soporte telefónico los conoce.
	e) Existen estadísticas públicas del Nivel de Calidad de Servicio de los servicios ofrecidos y encuestas de satisfacción que se actualicen al menos cada dos años.

	f) Existe una relación de los grandes contribuyentes de los que depende la mayor parte del ingreso y un responsable y procedimiento para convocarlos a través de contactos conocidos en caso de desastre.
B	Se dan al menos tres requisitos del apartado anterior, entre ellos el a) y c).
C	Si no se da el requisito a) del apartado primero.

Indicador	**2.3. Gestión del riesgo**
Factor	**2.3.1. Activos de la organización**
A	Se cumplen los siguientes requisitos:
	a) Existe un inventario de activos clasificados por tipos, soportado por una aplicación informática y con los atributos necesarios para gestionar su mantenimiento y reposición a lo largo del ciclo de vida de los mismos.
	b) Existe una norma que asigna responsabilidades en el mantenimiento del inventario a lo largo del ciclo de vida de los activos, tales como alta, baja y modificación de los activos.
	c) Existen normas escritas con criterios deseables de reposición (por ejemplo de los equipos informáticos).
	d) Existen un documento donde se identifiquen las relaciones de dependencia entre los activos, de manera que se reconozcan los activos más críticos.
	e) Existe un control sobre la existencia de riesgos laborales que no deben ser asumidos.
	f) Existe un procedimiento para la aprobación de la documentación anterior y para el control de sus versiones.
B	Se cumplen al menos tres requisitos del apartado anterior, entre ellos el a), d) y e).
C	Si se da al menos el requisito a) del apartado primero.

Factor	**2.3.2. Análisis de riesgos**
A	Se cumplen los siguientes requisitos:
	a) Existe una clasificación jerárquica de todos los riesgos y amenazas que puedan afectar a la continuidad de la organización, desde los asociados a desastres naturales, epidemias, amenazas humanas intencionadas y no intencionadas, incluyendo los ciberataques.
	b) Existe al menos un documento con una definición aproximada de los tiempos que podría soportar la organización con el servicio de TI degradado por función, especialmente considerando la recaudación.
	c) Existe al menos un informe en los dos últimos años que muestre las mayores urgencias, lo que debe ser mejorado y el coste que supondría incluyendo más elementos que los propiamente informáticos.
	d) Se conoce para cada tipo de riesgo, especialmente en el caso de ciberataques cuáles serían las instituciones que darían soporte y a qué coste.

	e) Se revisa el análisis al menos cada dos años y en los últimos tres se ha incorporado algún riesgo nuevo.
	f) Existe un procedimiento para la aprobación de la documentación anterior y para el control de sus versiones.
B	Se dan al menos tres requisitos del apartado anterior.
C	Se da al menos un requisito del apartado primero.

Factor	**2.3.3. Gestión de los riesgos**
A	Se cumplen los siguientes requisitos:
	a) Existen protocolos de colaboración o contratos con las empresas o instituciones que darían soporte en caso de desastre.
	b) Existe una unidad con la misión de gestionar el ciclo de vida de la metodología utilizada que trate aspectos distintos a los informáticos.
	c) Existen acuerdos sindicales o con las organizaciones profesionales .
	d) Existen informes cuantificados anuales como: a) Incidencias por tipo b) Equipos sin licencia obsoletos o desactualizados; c) instalaciones inseguras y la Dirección conoce la evolución de estas variables.
	e) Existe un documento formalmente aprobado donde se indiquen planes y proyectos para mitigar los riesgos y amenazas identificadas, que incluye la relación entre qué planes y proyectos mitigan qué riesgos y amenazas, que incluya los responsables de los mismos y se realiza un seguimiento documentado con actas de dichos planes/proyectos. Entre ellas y muy especialmente, la operación con productos sin licencia actualizada u obsoletos o desarrollados en tecnologías inmantenibles.
	f) Se ha informado a Dirección de los riesgos existentes y el coste que supondría su mitigación.
B	Se da el requisito e) y cualesquiera otros dos requisitos más del apartado anterior.
C	No se da el requisito del apartado anterior.

Factor	**2.3.4. Profundidad**
A	Se cumplen los siguientes requisitos:
	a) Se ha estudiado la reacción frente a riesgos clásicos IT (infraestructura, comunicaciones, servicios, etc.), disturbios sociales y amenazas internas y otros propios del país.
	b) Se ha estudiado para cada riesgo su causa principal y el tipo de remedio más eficaz (presupuestario, organizativo, normativo, etc).
	c) ¿Existe una matriz de riesgos minuciosamente creada?
	d) ¿Se ha incluido algún riesgo nuevo en el inventario de riesgos o en la matriz de riesgos durante los dos últimos años?
B	Se ha estudiado la reacción frente a 6 o más dimensiones del área RECURSOS, pero no frente a disturbios sociales o amenazas internas.
C	No se da el requisito del apartado anterior.

7.4. Recursos

Área	**3. RECURSOS**
Indicador	**3.1. Marco organizativo**
Factor	**3.1.1. Requisitos normativos y buenas prácticas**
A	Se cumplen los siguientes requisitos:
f)	Existe una norma sobre el PCN y una unidad organizativa con recursos para mantenerlo y difundirlo así como para realizar las tareas asociadas (Análisis de Impacto, Planes de Desastre o similares, etc.)
g)	Existe una evaluación de compliance de la normativa en materia de Continuidad de Negocio realizada durante los dos últimos años, esto es se ha evaluado la gestión que se realiza de este Plan y reflejado el resultado en un informe.
h)	Existen análisis del cumplimiento o de la madurez en relación con algún estándar en materia de Continuidad de Negocio o con una norma externa de carácter nacional.
i)	La Dirección ha solicitado en el periodo de los dos últimos años o algún Comité de Seguridad u órgano la ha informado sobre los riesgos más graves existentes con propuesta de acciones de corrección.
j)	Existe alguna institución externa (oficial o contratada) que evalúe la calidad de la seguridad existente periódicamente.
k)	Existe algún análisis de brechas frente a las mejores prácticas.
B	Se da el requisito a) y cualesquiera otros dos requisitos más del apartado anterior.
C	Si no se da el requisito a) del apartado primero.

Factor	**3.1.2. Recursos asignados al cumplimiento normativo**
A	Se cumplen los siguientes requisitos:
a)	La AT ha aprobado formalmente el establecimiento de un Comité de Crisis (CC) y definido su composición y funciones.
b)	Existe alguna estructura organizativa (e.g. Comité de Seguridad, de Continuidad de Negocio o similar) que se haya reunido al menos una vez al trimestre durante los dos últimos años e informado a Dirección.
c)	Existe documentación asociada al funcionamiento normal del CC o de las instituciones de gobernanza (designación de participantes, convocatoria de reuniones, actas, etc.).
d)	Se pueden identificar tres recursos asignados específicamente a la Continuidad de Negocio.
B	Se da el requisito a) y cualquier otro requisito más del apartado anterior.
C	Si no se da el requisito a) del apartado primero.

Factor	3.1.3. Vigencia y transparencia de los Planes de emergencia, contingencia y recuperación
A	Se cumplen los siguientes requisitos:
a)	En el último año se han elaborado nuevos planes o actualizado o validado tras una revisión critica, al menos el 20% de los planes de emergencia, contingencia y recuperación.
b)	En el último año se han realizado y documentado ensayos de algún elemento (eg: desalojos, phising) de elementos de al menos 20% de dichos planes o más de cinco.
c)	Se dispone de un registro de las pruebas de aplicación de los planes que detalle su puesta en marcha y resultado(“lecciones aprendidas”).
d)	Se dispone de estadísticas actualizadas de aplicación de dichos planes o métricas de los incidentes o alguna otra expresión de que se realiza gestión cuantitativa basada en la evidencia.
e)	Existe al menos una evaluación global documentada durante los últimos tres años que confirme la adecuación a la normativa sobre emergencias estatal de dichos planes.
B	Se cumplen al menos los requisitos c), d) y e) del apartado anterior.
C	Se cumplen dos o menos requisitos del apartado primero.

Factor	3.1.4. Procedimientos de coordinación y comunicación con terceros
A	Se cumplen los siguientes requisitos:
a)	En el último año se han revisado y, si fuese necesario actualizado, los planes de comunicación y coordinación.
b)	En el último año se ha verificado la validez de los contactos para la coordinación de emergencias, se han actualizado los cambios y difundidas las copias o situadas en un repositorio accesible en una crisis.
c)	En el último año se han mantenido reuniones de coordinación con fuerzas de seguridad, emergencias o sanitarias u otras implicadas en los PCN.
d)	El plan de comunicación incluye una guía con ejemplos prácticos para la gestión de la comunicación con los empleados y los contribuyentes.
e)	Se dispone de herramientas y canales de comunicación con los empleados.
B	Se cumplen al menos tres requisitos del apartado anterior.
C	Se cumplen dos o menos requisitos del apartado primero.

Indicador	3.2. Infraestructuras
Factor	**3.2.1. Instalaciones de respaldo**
A	Se cumplen los siguientes requisitos:
a)	Existencia de una instalación de respaldo.
b)	La instalación de respaldo dispone del equipo (tanto Hardware como Software) para garantizar la continuidad y cubrir los servicios esenciales.

	c)	Existe un Inventario de activos necesarios para cumplir las misiones básicas.
	d)	Se tiene identificada la normativa que establezca y autorice restricciones a considerar en la instalación de respaldo.
	e)	Todos los servicios de terceros, especialmente los servicios cloud tienen SLR , penalizaciones por la prestación de servicios deteriorados y cláusulas para el caso de desastre tanto de la AT como del propio proveedor.
	f)	Disponibilidad por el CC de contratos y condiciones exigibles a terceros.
B	Se dan al menos los requisitos a), b) y d) del apartado anterior.	
C	Si no se da el requisito a) del apartado primero.	

Factor	**3.2.2. Suministros**	
A	Se cumplen los siguientes requisitos:	
	a)	Inventariado de recursos alternativos y condiciones de solicitud y uso.
	b)	Contrato y acometida en su caso con compañías eléctricas diferentes para garantizar el suministro.
	c)	Contrato con compañías de comunicaciones diferentes para garantizar el suministro.
	d)	Se cuenta con Sistemas SAI (Sistemas de Alimentación Ininterrumpida) de potencia suficiente para garantizar un SLA mínimo mientras se ponen en funcionamiento los grupos electrógenos y para garantizar un apagado ordenado.
	e)	Se cuenta con grupos electrógenos.
	f)	Se cuenta con el certificado periódico de mantenimiento de los sistemas indicados.
	g)	Se han realizado pruebas de los elementos anteriores con éxito.
	h)	Se cuenta con planes de mejora consecuencia de los resultados de las pruebas realizadas.
B	Se dan al menos los requisitos b), d) y f) del apartado anterior.	
C	No se dan los requisitos del apartado anterior.	

Factor	**3.2.3. Resiliencia frente a desastres naturales**	
A	Se cumplen los siguientes requisitos:	
	a)	Se cuenta con sistemas de mantenimiento de temperatura y humedad.
	b)	Se cuenta con sistemas de alerta y extinción de incendios adecuados al riesgo de cada zona.
	c)	Se cuenta con sistemas de detección y alerta de líquidos y humedad, con medios de achique en su caso.
	d)	Se cuenta con el certificado de revisión anual de dichos sistemas.
	e)	Se cuenta con sistemas o medios directos y periódicos de comunicación con centros de alertas medioambientales aprobados en un protocolo.

	f)	Se cuenta con protocolos documentados de actuación ante desastres naturales: incendios, terremotos, etc.
B	Se dan al menos los requisitos a), b), c) y d) del apartado anterior.	
C	Se dan al menos los requisitos a) y b) del apartado primero.	

Factor	**3.2.4. Resiliencia frente a ataques intencionados**	
A	Se cumplen los siguientes requisitos:	
	a)	Se cuenta con sistemas de monitorización del estado de los distintos sistemas TI, de manera que se detecte de manera precoz cualquier fallo en los mismos.
	b)	Se cuenta con videocámaras, las cuales están monitorizadas.
	c)	Se cuenta con tornos, tarjetas u otros sistemas de control de acceso físico.
	d)	Se cuenta con un contrato de personal de seguridad física.
B	Se cumplen al menos dos requisitos del apartado anterior.	
C	Se cumple solo uno o ninguno de los requisitos del apartado primero.	

Indicador	**3.3. Salvaguarda de la información**	
Factor	**3.3.1. Políticas y procedimientos de copia de seguridad**	
A	Se cumplen los siguientes requisitos:	
	a)	Existe una política de seguridad que define los procesos de copia de seguridad necesarios para garantizar el funcionamiento de los procesos críticos de la organización. En caso de uso de cloud previsiones adecuadas para el caso de desastre, litigio o cancelación o finalización del contrato.
	b)	Existen procedimientos de copia de seguridad, donde se definen todos los aspectos necesarios para la ejecución de las copias de seguridad: la frecuencia de las copias, requisitos de almacenamiento, controles de acceso, responsables, tiempo de retención, etc.
	c)	Existe un registro de copias de seguridad donde se indican todos los detalles de cada copia: identificador, tipo de copia, fecha, lugar de almacenamiento, responsable, etc.
	d)	La política y los procedimientos de copia de seguridad incluyen tanto las copias de seguridad de información como de configuración de sistemas, necesarios para ofrecer los servicios críticos para la organización.
	e)	Se cumple la normativa vigente sobre datos personales.
	f)	La Dirección actual de la AT conoce con un informe escrito de las limitaciones existentes en los sistemas de recuperación y el coste que supondría alcanzar el nivel requerido para garantizar los servicios en caso de crisis.
	g)	Existen al menos dos equipos de personas capaces de reiniciar las instalaciones desde el centro de respaldo.
B	Se da el requisito a) y cualesquiera otros dos requisitos más del apartado anterior.	
C	No se alcanza el nivel B.	

Factor	3.3.2. Protección de copias de seguridad
A	Se cumplen los siguientes requisitos:
a)	Al menos, una de las copias de seguridad se almacena de forma separada en lugar diferente, de tal manera que un incidente no pueda afectar tanto al repositorio original como a la copia.
b)	Las copias de seguridad se almacenan en un lugar seguro, con las medidas de seguridad suficientes para garantizar su confidencialidad, integridad y disponibilidad. Existe tercera copia para el caso de desastre durante la recuperación.
c)	Existe un registro de control de acceso a las copias de seguridad.
d)	La política de copias de seguridad abarca tanto la información corporativa como aquella existente en servidores, redes locales y puestos de trabajo que permiten trabajar desde el domicilio, que serían necesarios en caso de desastre.
e)	Las copias de seguridad tienen asignado un responsable de su custodia y existe un histórico a efectos judiciales y estadísticos.
f)	Se toman precauciones para evitar el deterioro provocado de la información con medios magnéticos.
B	Se cumple el requisito a) y b) del apartado anterior.
C	Se cumple el requisito a) o b) del apartado primero.

Factor	3.3.3. Pruebas de los procedimientos de copia de seguridad y recuperación
A	Se cumplen los siguientes requisitos:
a)	Se dispone de un plan de pruebas de los procedimientos de copia de seguridad y restauración.
b)	En el último año, se han revisado y actualizado si fuese necesario los procedimientos y la política de copia de seguridad.
c)	En el último año se ha realizado al menos una prueba de disponibilidad y recuperación a partir de la copia de seguridad.
B	Se cumplen al menos dos requisitos del apartado anterior.
C	Se cumple al menos el requisito a) del apartado primero.

Indicador	3.4. Servicios de terceros
Factor	**3.4.1. Proveedores**
A	Se cumplen los siguientes requisitos:
a)	Se dispone de un inventario de proveedores, indicando servicio suministrado, condiciones de disponibilidad contratadas y contacto del mismo.
b)	Existen algunos requisitos exigidos a los proveedores de forma estandarizada para mejorar la resiliencia (e.g. Acuerdos de nivel de servicios, penalizaciones etc).
c)	Entre los criterios de adjudicación se ha valorado alguna vez durante los dos últimos años criterios relacionados con la resiliencia.

	d)	Existen para los contratos algunas exigencias en los Pliegos de Cláusulas Administrativas o en Licitaciones que garanticen la reacción debida del suministrador en caso de declaración de desastre.
	e)	Se exige para las empresas adjudicatarias de servicios o para las fábricas de Sw o para la asistencia técnica algún modo de control de la fiabilidad del personal aportado y de responsabilidad frente a daños físicos o reputacionales.
	f)	Se ha realizado durante el último ejercicio un control sistemático de si los niveles de servicios acordados por los proveedores ha sido el señalado en los SLA y en caso contrario se han exigido las penalizaciones correspondientes.
	g)	Se exigen a los proveedores certificaciones relacionadas con la seguridad o la resiliencia.
B	Se dan al menos tres requisitos del apartado anterior.	
C	Se da al menos el requisito a) del apartado primero.	

Factor	**3.4.2. Cloud**	
A	Se cumplen los siguientes requisitos:	
	a)	Se dispone de un inventario de los servicios cloud, incluyendo los proveedores que proporcionan el servicio, condiciones del servicio suministrado, contactos e interlocutores en caso de crisis.
	b)	Se dispone de documentación donde se identifiquen e indiquen restricciones legales en relación con la cloud (por ejemplo, ubicación de servidores) y la forma de soslayarlos en caso de emergencia.
	c)	Se dispone de un Check list de requisitos exigidos a los proveedores cloud, incluyendo los necesarios en caso de crisis.
	d)	El contrato de suscripción de los requisitos exigidos prevee la operación en condiciones de desastre y establece SLA.
	e)	Certificaciones de los proveedores verificadas por el Órgano de Contratación.
	f)	Existen documentos precumplimentados para comunicar incidencias.
	g)	Se han realizado pruebas de operación y decisiones sobre los datos y aplicaciones de la nube en caso de desastre con operación por terceros. El Comité de Crisis dispone de las password y autorizaciones para operar en caso de ausencia irremediable de los técnicos de la AT.
B	Se dan al menos los requisitos a), b), c) y d) del apartado anterior.	
C	Se dan los requisitos b) y c) del apartado primero.	

Factor	**3.4.3. Cadena de suministro**	
A	Se cumplen los siguientes requisitos:	
	a)	Se tiene un inventario de proveedores, indicando servicio suministrado y contacto accesibles al Comité de Crisis incluso con caídas del Sistema Informático.
	b)	Existen requisitos exigidos a los proveedores (e.g; personal de seguridad y mantenimiento) orientados a la resiliencia y se prevén penalizaciones en caso de incumplimiento.

	c)	Se exige alguna certificación, cuando procede, a proveedores relacionada con la seguridad y resiliencia y se actualiza cuando cambian el personal que presta el servicio.
	d)	Se realizan sesiones periódicas (al menos anuales) formales o informales con otras instituciones públicas o financieras para intercambiar experiencias sobre incidentes y conocer la calidad de la reacción de los suministradores.
	e)	Se dispone de la oferta económica de los suministradores sobre servicios premium de seguridad (e.g: adicionales frente a los básicos contratados por la instalación) y en su caso valorado e informado a la Dirección sobre los posibles costos y ventajas.
	f)	Se exigen a los proveedores certificaciones relacionadas con la seguridad o la resiliencia.
B	Se da el requisito a) y cualesquiera otros dos requisitos más del apartado anterior.	
C	Se da al menos el requisito a) del apartado primero.	

Indicador	**3.5. Infraestructura TI (Hardware, Software y comunicaciones) - Alta disponibilidad**
Factor	**3.5.1. Política y procedimientos relacionados con la disponibilidad de los sistemas TI**

A	Se cumplen los siguientes requisitos:	
	a)	Existe una política de seguridad donde se definen los criterios de disponibilidad que deben cumplir los sistemas para garantizar el funcionamiento de los procesos críticos de la organización.
	b)	Existe un inventario detallado de recursos TI, y están identificados los sistemas críticos para la organización.
	c)	La AT dispone de procedimientos donde se especifican los detalles y la operativa de la monitorización de los sistemas.
	d)	Se han establecido acuerdos de nivel de servicio con todos los proveedores externos y con los de servicios cloud que gestionan sistemas necesarios para garantizar los procesos críticos de la organización.
B	Se cumplen al menos tres requisitos del apartado anterior.	
C	Se da al menos el requisito a) del apartado primero.	

Factor	**3.5.2. Arquitectura y operación**

A	Se cumplen los siguientes requisitos:	
	a)	Se dispone de algún sistema de redundancia para los componentes críticos.
	b)	Existen al menos dos CPD en ubicaciones físicas diferentes. En caso de indisponibilidad total de uno de los CPD, se puede dar servicio a los procesos críticos de la organización en otra ubicación.
	c)	Se dispone de un sistema automático que permite seguir ofreciendo servicio de forma inmediata en caso de contingencia en uno de los CPD.
	d)	Existen procedimientos de recuperación del servicio en caso de contingencia.
	e)	Se dispone de medidas de mitigación que permiten minimizar el tiempo de inactividad en caso de contingencia.

B	Se cumplen al menos cuatro requisitos del apartado anterior.
C	Se da al menos el requisito a) del apartado primero.

Factor	**3.5.3. Monitorización**
A	Se cumplen los siguientes requisitos:
a)	Existe un sistema de monitorización para detectar fallos en los sistemas críticos y la evolución se notifica a la Dirección de la AT.
b)	Se emplean herramientas de monitorización que generan alertas automatizadas en caso de fallo en los sistemas críticos.
c)	Existe un servicio 24x7 con personal dedicado a la monitorización de las incidencias y a la resolución de las mismas.
B	Se dan los requisitos a) y b) del apartado anterior.
C	Se da al menos el requisito a) del apartado primero.

Factor	**3.5.4. Evaluación y mejora continua**
A	Se cumplen los siguientes requisitos:
a)	Existe un registro donde se recopila la información de los incidentes que afectan a la disponibilidad del sistema.
b)	Se implementan mejoras basadas en el análisis de los incidentes que afectan a la disponibilidad del sistema.
c)	Se revisan periódicamente las políticas y procedimientos relacionados con la disponibilidad de los sistemas y al menos una vez durante los dos últimos años
d)	El personal recibe formación sobre buenas prácticas en disponibilidad de los sistemas.
e)	Se realizan simulacros de fallo para valorar la efectividad de los procedimientos de alta disponibilidad de los sistemas TI.
B	Se cumplen los requisitos a), b) y c) del apartado anterior.
C	Se da al menos un requisito del apartado primero.

Indicador	**3.6. Gestión de la seguridad y respuesta ante ciberincidentes**
Factor	**3.6.1. Política y procedimientos relacionados con la ciberseguridad**
A	Se cumplen los siguientes requisitos:
a)	La AT dispone de procedimientos definidos para la gestión de incidentes de seguridad.
b)	Se dispone de procedimientos para la gestión de las vulnerabilidades y brechas detectadas en los sistemas y las aplicaciones.
c)	Se dispone de procedimientos para la detección y monitorización de incidentes de seguridad.
B	Se da el requisito a) y cualquier otro requisito más del apartado anterior.
C	Se da al menos el requisito a) del apartado primero.

Factor	3.6.2. Gestión y monitorización
A	Se cumplen los siguientes requisitos:
	a) La AT dispone de herramientas orientadas a la detección y prevención de intrusiones (IPS, IDS, SIEM, etc.).
	b) Se dispone de un sistema de centralización de registro y logs de los sistemas, y se explota para detectar incidentes de seguridad.
	c) Se emplean herramientas automatizadas para la identificación de vulnerabilidades de los sistemas críticos.
B	Se cumplen los requisitos a) y b) del apartado anterior.
C	Se da al menos el requisito a) del apartado primero.

Factor	3.6.3. Respuesta ante ciberincidentes
A	Se cumplen los siguientes requisitos:
	a) La AT dispone de un protocolo de respuesta frente a ciberincidentes.
	b) Los protocolos de respuesta frente a ciberincidentes detallan claramente los procedimientos para la comunicación interna de incidentes, comunicación con terceros y el escalado interno a la dirección de la administración.
	c) Existe un centro de operaciones de seguridad (SOC) o similar para la detección y respuesta frente a ciberincidentes.
	d) Se ejecutan automáticamente acciones de respuesta frente a alertas generadas por los sistemas de detección de intrusiones.
	e) Se dispone de procedimientos para evaluar y restaurar la integridad de los sistemas tras un ciberincidente.
B	Se cumplen los requisitos a) y b) y cualquier otro más del apartado anterior.
C	Se da al menos el requisito a) del apartado primero.

Factor	3.6.4. Evaluación y mejora continua
A	Se cumplen los siguientes requisitos:
	a) La AT realiza periódicamente análisis de vulnerabilidades y pruebas de penetración sobre los servicios críticos de la organización.
	b) Se realizan periódicamente auditorías de seguridad sobre los servicios críticos por parte de terceros.
	c) Se realizan simulacros y ejercicios de ciberincidentes para evaluar la efectividad de los planes de respuesta ante incidentes.
	d) Existe un plan de formación en materia de ciberseguridad para el personal encargado de la gestión de los incidentes de seguridad.
	e) Existe un plan de formación y concienciación en materia de seguridad, orientado de forma general al personal de la AT.

	f)	Se lleva un registro con todos los detalles de los ciberincidentes que han ocurrido en la organización y que afectan a servicios críticos.
	g)	Se implementan mejoras basadas en el análisis de los incidentes de seguridad.
	h)	Se revisan y actualizan periódicamente los procedimientos y documentación relacionados con la gestión de incidentes de seguridad.
B	Se cumplen los requisitos a), e), f) y h) del apartado anterior.	
C	Se da al menos un requisito del apartado primero.	

Indicador	**3.7. Recursos humanos**	
Factor	**3.7.1. Análisis de necesidades: roles y habilidades**	
A	Se cumplen los siguientes requisitos:	
	a)	Existe un estudio conocido por la Dirección sobre las necesidades de roles y habilidades necesarios para mantener la Continuidad de Negocio para los próximos tres años.
	b)	Existe un estudio y se han presupuestado la cobertura de los puestos de trabajo necesarios para cubrir las necesidades detectadas en el punto anterior.
	c)	Se han adjudicado los puestos de trabajo definidos en el punto anterior, en al menos un 75%.
	d)	Existen los recursos necesarios para implantar los nuevos cambios legislativos y de procedimientos sin necesidad de detraer recursos que sean necesarios para el adecuado mantenimiento de los servicios considerados básicos .
	e)	Se ha elaborado un plan de contratación de personal alternativo para cubrir las necesidades detectadas en el punto a) y ha sido remitido a Dirección.
	f)	En el diseño del Plan de Formación se han tenido en cuenta criterios como la necesidad de contar con personal polivalente para la oferta de cursos.
B	Se dan al menos tres requisitos del apartado anterior.	
C	Si no se da el requisito a) del apartado primero.	

Factor	**3.7.2. Equipos de respuesta**	
A	Se cumplen los siguientes requisitos:	
	a)	Se ha definido la composición y funciones de los Equipos de Respuesta y es conocida por la dirección. Están identificados los responsables.
	b)	Se han definido los procedimientos de funcionamiento internos de los Equipos de Respuesta.
	c)	Existen actas, informes o documentación asociada al funcionamiento de los Equipos de Respuesta.
B	Se da el requisito c) y cualquier otro requisito más del apartado anterior.	
C	Si no se da el requisito c) del apartado primero.	

Factor		3.7.3. Formación y entrenamiento
A		Se cumplen los siguientes requisitos:
	a)	Planes de Formación y actualización específicos para los Equipos de Respuesta.
	b)	Planificación de simulacros e informe de resultado.
	c)	Existe una cultura adecuada de aceptación del error humano orientada a la mejora progresiva en vez de a la exigencia de responsabilidad.
	d)	Certificación o superación de itinerario formativo del personal que forma parte de los Equipos de Respuesta.
	e)	Existe un Plan de Comunicación.
B		Se cumplen al menos dos requisitos del apartado anterior.
C		Se da al menos un requisito del apartado primero.

Indicador		3.8. Precariedad
Factor		3.8.1. Por escasez
A		Se cumplen los siguientes requisitos:
	a)	Se dispone de capacidad instalada para asegurar el nivel de servicios durante el próximo periodo de alta carga planificada.
	b)	El número de desarrolladores es tal que el backlog de aplicaciones en espera de desarrollo no ha aumentado durante el último año.
	c)	No se utiliza Sw sin licencia u obsoleto por razones presupuestarias.
	d)	Se conoce el ratio de personal técnico con relación al número de contribuyentes y no es inferior en más de un 20% a la de los países de la región.
	e)	No existe ningún proyecto en materia de seguridad que pueda comprometer la continuidad del negocio (como centro de backup) paralizado durante al menos dos años por falta de presupuesto.
B		Se cumplen al menos cuatro requisitos del apartado anterior.
C		Se da al menos el requisito a) del apartado primero.

Factor		3.8.2. Por rigidez
A		Se cumplen los siguientes requisitos:
	a)	Existe la flexibilidad de recursos para atender a los cambios normativos sin comprometer la planificación anual de proyectos de transformación.
	b)	Exista la flexibilidad (e.g; máquinas virtuales suficientes para poder realizar al menos una vez al año pruebas de seguridad y/o restauración.
	c)	Existe la flexibilidad presupuestaria y normativa para provisionar un servicio crítico de seguridad (e.g: licencias, dispositivos, consultoría en menos de 9 meses para importes superiores a 100.000 USD).

	d)	Existe la flexibilidad de la plantilla y los proveedores para poder realizar cambios críticos durante fines de semana y periodos de menos servicio al contribuyente.
	e)	Existe un presupuesto asociado al PCN que muestra los recursos que serían necesarios y los que van siendo asignados en cada ejercicio.
B	Se cumplen los requisitos a) y b) del apartado anterior.	
C	Se da al menos el requisito a) del apartado primero.	

Factor	**3.8.3. Por contexto**	
A	Se cumplen los siguientes requisitos:	
	a)	No existen antecedentes durante el último año de movimientos sociales críticos de las instituciones con violencia callejera.
	b)	No ha existido en los últimos diez años un incidente físico (Fuego, lluvias, etc.) que haya alterado el servicio de las instalaciones centrales de IT.
	c)	No se ha dado el caso que durante los dos últimos años no se hayan podido atender el pago de licencias u otros proveedores.
	d)	Las tarifas establecidas hacen inviable la contratación de profesionales con conocimientos especializados críticos.
	e)	No es el caso en que una norma legal imposibilite la renovación de contratos de licencias críticas existentes y obligue a una migración no deseada a productos *open source* sobre los que no existe formación o confianza.
	f)	No es el caso que durante los dos últimos años exista un litigio con algún proveedor o desarrollador crítico que pueda conducir a una anulación litigiosa de un contrato previo.
B	Se cumplen los requisitos a), b) y c) del apartado anterior.	
C	Se da al menos un requisito del apartado primero.	

7.5. Madurez

Área	**4. MADUREZ**	
Indicador	**4.1. Cobertura**	
Factor	**4.1.1. ¿Existe modelo BCM@M?**	
A	Se cumplen los siguientes requisitos:	
	a)	Existe alguna norma que utiliza el concepto de madurez en lo relativo a la continuidad de negocio, lo define y establece, un responsable y personal asignado
	b)	Existe un *roadmap* y un objetivo para alcanzar un grado definido de madurez y un calendario de revisiones planificadas.
	c)	Existe un presupuesto específico asignado.

	d) La Dirección recibe informes y propicia acciones.
	e) Existen cada año objetivos para mejorar el nivel de la resiliencia.
	f) Existe un diagnóstico de la instalación (AS IS) y un objetivo a alcanzar explicito (TO BE).
	g) Existe algún estudio o informe de consultoría sobre la situación de la AT en relación con las mejores prácticas internacionales en la que se valore el grado de madurez frente a otras instalaciones similares.
B	Se cumplen al menos tres requisitos del apartado anterior.
C	Se dan dos o menos requisitos del apartado primero.

Indicador	**4.2. Pruebas**
Factor	**4.2.1. De actuación**
A	Se han realizado pruebas de:
	a) Desalojo de los centros de procesos de datos y edificios.
	b) De continuidad de servicios desde un Centro de Respaldo si la configuración es Activo - Activo.
	c) De continuidad tras un incidente con respaldo ACTIVO PASIVO.
	d) Simulación de acciones frente a un ataque con *ransonware*.
	e) Cambio entre proveedores (Redes de cloud, suministro eléctrico, telefonía en su caso).
B	Se cumplen al menos cuatro requisitos del apartado anterior.
C	Se da al menos el requisito a) del apartado primero.

Indicador	**4.3. Gestión cuantitativa**
Factor	**4.3.1. Herramientas cuantitativas**
A	Se cumplen los siguientes requisitos:
	a) Existe un documento de análisis de riesgo donde se muestren vulnerabilidades y calificación de probabilidad e impacto.
	b) Existe un documento con el detalle de los impactos aceptables.
	c) Se han realizado análisis coste beneficio de las alternativas.
	d) Existe una estadística de los incidentes ordenados por tipo y gravedad de los tres últimos años.
	e) Se dispone de datos para realizar un benchmarking entre ellos los tiempos de respuesta hasta la resolución del incidente por causa y gravedad.
B	Se cumplen al menos dos requisitos del apartado anterior.
C	No se da el requisito del apartado anterior.

7.6. Instrucciones de cumplimentación del cuestionario

Figura 8. Ejemplo de cumplimentación del cuestionario

				Total	Normalizado			
Área	**Indicadores**				**Resultados**	**Objetivos**	**Resultado**	**Max**
1. ACTITUD	1.1 Liderazgo y Normas	1.1.1. Organizativos	A	12	0,67	1,00	4	4
		1.1.2. Procedimientos	A				4	4
	1.2 Planes	1.2.1. Actuaciones	B				3	4
	1.3 Actividades	1.3.1. Impulso	C				1	4

Como se muestra en el ejemplo de la *Figura 8* quien lo cumplimente deberá:

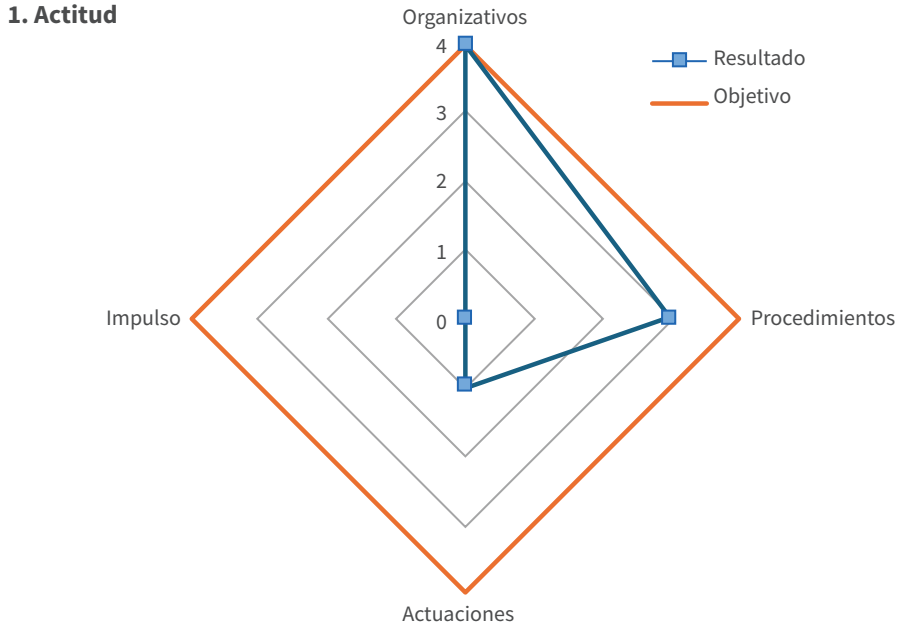
1. Marcar las calificaciones asignadas (A, B o C). En caso de que para un factor no se alcance la calificación más baja, es decir no se den los requisitos para responder con la calificación C, dejar la respuesta en blanco.

2. Para cada área, se suman los puntos obtenidos en cada área por separado. Para ello las A se valoran en 4 puntos, las B en 3, las C en 1 y las respuestas en blanco se valoran con cero puntos. Se suman las puntuaciones así obtenidas por área en la columna total con lo que se dispone de cuatro parciales.

3. Cada uno de ellos se normaliza con la expresión situada a su derecha para obtener una calificación por área entre 0 y 1.

Si se desea se representa el resultado gráficamente, puede obtenerse por cada área como en la *Figura 9*.

Figura 9. **Diagrama de araña del área Actitud**



O como el de la *Figura 10*, para el área de Recursos.

Figura 10. **Aplicación del cuestionario a Recursos**

Se hace notar que en cada diagrama la diferencia entre el perímetro exterior y el interior es el GAP que deberá ser corregido en los sucesivos planes.

8. Glosario

Glosario de términos técnicos utilizados:

Actividades de soporte básicas. Actividades que deben ser prestadas para garantizar el cumplimiento de las misiones esenciales de una organización de acuerdo con los niveles de servicio establecidos.

Acuerdo de nivel de servicio (SLA). Acuerdo formal por el que una empresa, institución u órgano se compromete a proporcionar a otra un servicio con niveles de calidad previamente establecidos mediando o no un precio.

Comité de crisis. Es el grupo de personas dentro de una organización designados previamente que coordinan y gestionan las respuestas ante situaciones de emergencia críticas, desastres y otras que comprometan la operación, la existencia o la reputación de la organización.

Comité de dirección. El formado por el/la presidente/a de la Institución y que dirige su funcionamiento ordinario con competencias asignadas por una norma vigente.

Centro de Procesamiento de Datos. Un centro de procesamiento de datos (o CPD) es la instalación que centraliza las operaciones y la infraestructura de TI de una organización, en la que se almacenan, procesan, tratan y difunden datos y aplicaciones. Un centro de datos suele reunir muchos servidores, tanto de procesamiento como de almacenamiento y redes, y suele tener algunos de los activos más críticos e importantes de una organización. Estas grandes instalaciones consumen mucha energía y, al reunir tantos equipos en tan poco espacio, necesitan de unos buenos sistemas de ventilación y refrigeración para mantener unas óptimas condiciones de trabajo.

Crisis. Se debe entender por crisis" [ ] *un evento crítico que puede afectar la rentabilidad, la reputación o la capacidad de operación de una organización*". (Fuente: *Business Continuity Management Institute* – BCM Institute). Lo que se aborda en este documento es la posibilidad de que esta crisis afecte a intereses vitales de una nación.

Grupos electrógenos. Un grupo electrógeno es una máquina que genera energía eléctrica. Suele usarse en lugares que no tienen acceso a la red, sobre todo para proyectos que requieren más energía de la que la red puede proporcionar o para situaciones en las que la se necesita un respaldo en caso de falla eléctrica.

Misiones esenciales. Actividades que debe prestar la organización en todo caso.

Modelo BCM@M. Los modelos de madurez de continuidad del negocio son herramientas para conocer (medir) del estado en que se encuentra una organización en términos de nivel de preparación para afrontar y recuperar sus operaciones críticas. Una gestión de continuidad bajo la perspectiva del "nivel de madurez" permite medir la organización tomando como referencia las prácticas metodológicas reconocidas mundialmente como "claves" para asegurar la resiliencia, para luego encaminar y monitorear las acciones requeridas para alcanzar la excelencia.

Plan estratégico. El que despliega a medio y largo plazo las acciones y objetivos que permiten alcanzar la misión.

Plan anual. Concreción para un año concreto del plan estratégico.

Pruebas piloto. Una prueba de concepto supone el análisis de la viabilidad de una idea con datos y recursos parciales. Si es exitosa puede pasarse al desarrollo de un prototipo, solución ya robusta que permite evaluar para un caso particular o a un número limitado de usuarios en servicio. En el proceso de escalado de la solución hasta alcanzar el completo despliegue se suelen realizar pruebas de componentes parciales de un sistema que reciben el nombre de pruebas piloto que prestan parte de la funcionalidad final a parte de los usuarios finales.

Resiliencia. Originalmente la capacidad (planificada) para soportar las adversidades y volver proactivamente al estado inicial. No debe confundirse por tanto con la mera resistencia o impasibilidad.

Requisitos de nivel de servicio. Los Requisitos de Nivel de Servicio (*Service Level Requirements, SLR*) deben recoger información detallada sobre las necesidades del cliente y sus expectativas de rendimiento y nivel de servicios. El documento de SLR constituye el elemento base para desarrollar los Acuerdos de Nivel de Servicio SLA y posibles Acuerdos de Nivel Operativo OLAs correspondientes.

Respaldo Activo-Activo y Activo-Pasivo. Los conceptos de respaldo activo-activo y activo-pasivo se refieren a configuraciones de sistemas de alta disponibilidad y recuperación ante desastres.

En una configuración activo-activo, múltiples sistemas o servidores están activos simultáneamente, compartiendo la carga de trabajo. Esta configuración se usa para asegurar la disponibilidad continua y la eficiencia operativa. Si uno de los nodos falla, la carga se redistribuye automáticamente entre los nodos restantes. Es importante destacar que los datos y las aplicaciones deben estar sincronizados en todos los nodos activos para asegurar consistencia y evitar conflictos.

En una configuración activo-pasivo, solo un sistema o servidor está activo en cualquier momento, mientras que el otro está en espera (pasivo) y solo se activa cuando el sistema activo falla. Cuando el sistema activo falla, el sistema pasivo se activa y asume el control. Puede haber un breve período de inactividad durante la conmutación. La configuración y la sincronización pueden ser más sencillas.

Roles. Misiones a realizar por un componente de la organización.

ciat@ciat.org