Documentos de Trabajo

ISSN 2219-780X

3

MARZO
2024

Plan de Continuidad de Negocios: importancia creciente para las Administraciones Tributarias

Antonio Seco
Wolney Martins
Gilberto Netto

Plan de Continuidad de Negocios: importancia creciente para las Administraciones Tributarias

Antonio Seco
Wolney Martins
Gilberto Netto

Serie: *Documentos de Trabajo*
ISSN 2219-780X

Plan de Continuidad de Negocios: importancia creciente para las Administraciones Tributarias

DT-03-2024

Antonio Seco
Wolney Martins
Gilberto Netto

Diagramación: Coordinación de Comunicación y Publicaciones del CIAT

Contenido

Listado de siglas

BIA	*Business Impact Analysis*
BPP	*Business Priority Processes (IRS)*
CIAT	Centro Interamericano de Administraciones Tributarias
COBIT	*Control Objectives for Information and Related Technology*
CRA	*Canadian Revenue Agency*
ESA	*Essential Support Activities (IRS)*
GCN	Gestión de Continuidad de Negocios
IOTA	*Intra-European Organisation of Tax Administrations*
IRS	*Internal Revenue Service (USA)*
ISO	*International Organization for Standardization*
ITIL	*Information Technology Infrastructure Library*
MEF	*Mission Essential Functions (IRS)*
OECD	*Organization for Economic Cooperation and Development*
PCN	Plan de Continuidad de Negocios
PCO	Plan de Continuidad Operativa
PwC	Price, Waterhouse & Coopers (Consultoría y Auditoría)
RTO	*Recovery Time Objective*
SEFAZ-MA	*Secretaria de Estado de Fazenda do Estado do Maranhão (Brasil)*
SGCN	Sistema de Gestión de Continuidad de Negocios
SUNAT	*Superintendencia Nacional de Administración Tributaria (Perú)*
TADAT	*Tax Administration Diagnostic Assessment Tool*
TI	Tecnologías de Información

Resumen Ejecutivo

La continuidad de negocio ayuda a las organizaciones a mantener la resiliencia y responder rápidamente ante interrupciones, permitiendo que continúen funcionando al menos a un nivel mínimo durante eventos disruptivos.

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. 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.

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. 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.

El PCN describe los procedimientos e instrucciones que la organización debe seguir durante eventos disruptivos para minimizar el tiempo de inactividad, esto incluye procesos organizativos, activos, recursos humanos y partes interesadas externas a la institución.

Para desarrollar un PCN no es necesario reinventar la rueda. Existen experiencias documentadas y un conjunto de normas y buenas prácticas internacionales que pueden guiar el proceso.

Usualmente, se 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. Cada una de estas etapas tiene actividades propias esenciales para el éxito del plan, enmarcadas por la inclusión de la cultura de continuidad de negocios en la organización. Algunos ejemplos de temas tratados en estas etapas son el análisis de riesgos, el análisis de impacto en los negocios y los objetivos de tiempo de recuperación.

Este contexto general debe ser adaptado a cada administración tributaria, ya que estas parten de diferentes condiciones (como el grado de digitalización de los servicios, la disponibilidad de trabajo remoto, los acuerdos de subcontratación y el ámbito de actuación).

La participación de los altos ejecutivos y las auditorías internas también son elementos clave para el éxito de un PCN.

1 Introducción

En el umbral del siglo XXI, el mundo se encuentra en una encrucijada tecnológica y administrativa. Esto es especialmente verdad en el ámbito de las administraciones tributarias, considerando que estas entidades no solo gestionan una gran cantidad de datos críticos y sensibles para gobiernos y contribuyentes, sino que también desempeñan un papel fundamental en la economía y funcionamiento de las sociedades.

El vertiginoso avance de las tecnologías de la información (TI) ha transformado la forma en que estas organizaciones operan. Sus procesos clave son fuertemente dependientes de información y los métodos y técnicas para accederla, tratarla y distribuirla de modo continuo se han vuelto de alta prioridad. Se observan también crecientes amenazas – internas y externas – que afectan la continuidad de los procesos administrativos manuales e informatizados, englobando desde eventos climáticos / fenómenos naturales, ataques cibernéticos, conflictos geopolíticos, cambios regulatorios, hasta crisis sociales.

Parafraseando a Harari[1], en general las organizaciones pueden considerarse como producto de ficciones colectivas creadas por la humanidad. Para escapar de esta clasificación una organización debe estar completamente automatizada, incluyendo las relaciones externas. Dicha ficción puede examinarse desde diferentes perspectivas. La mayoría de los enfoques más importantes pueden realizarse mediante la cooperación entre los componentes de la organización.

La continuidad del negocio de una organización convencional, luego de que ocurra un evento que altere la normalidad de sus operaciones, tiene todo que ver con la cooperación entre los componentes. La propia normalidad de las operaciones depende de la mencionada cooperación. Hay muy pocas actividades que funcionan independientemente de la cooperación entre personas; en estos casos extremos no es necesario hablar de “organización”. No existe ninguna organización que sea funcional sin la cooperación entre las personas.

1 Yuval Noah Harari, profesor de Historia y autor de libros.

La discusión sobre la continuidad es una oportunidad para igualar conocimientos y entendimientos fundamentales para la cooperación. Independientemente de las conclusiones y resultados que surjan de las discusiones, estas actividades permiten que todos compartan y actualicen conocimientos sobre la organización en términos de situación, desafíos, riesgos, estrategias, prioridades, etc. La discusión colectiva puede ayudar en la selección e implementación de medidas preventivas, que preceden a la planificación de acciones de continuidad.

A lo largo de los años, las organizaciones han adquirido instalaciones y recursos para minimizar las interrupciones, ajustando los costos generales y aumentando la porción de los costos fijos. Este enfoque puede clasificarse como técnico o tecnológico, generalmente asociado al uso de soluciones redundantes y tolerantes a fallas, además de la búsqueda de economías de escala. Sin embargo, es necesario considerar también los aspectos sociales: comportamientos y procedimientos. Los desafíos de continuidad requieren una combinación de ambos tipos de soluciones.

Aunque pueda parecer obvio, es importante resaltar que la decisión y ejecución de gastos para satisfacer las necesidades operativas y de continuidad de la organización deben dirigirse a recursos directamente relacionados con la agregación de valor y la generación de resultados.

Como se presenta en este texto, el desarrollo de planes de continuidad puede – y debe – utilizar métodos y modelos ampliamente probados y validados. El análisis de riesgos es un paso presente en todas las referencias, habitualmente con evaluación de las probabilidades de ocurrencia y priorización en función de los efectos que cada tipo de interrupción puede provocar.

El análisis de riesgos debe evitar sesgos a corto plazo. Es posible que en los análisis de riesgo realizados en los últimos años se haya sobreestimado el riesgo de pandemias y otros trastornos de la salud. En otras palabras, los riesgos pueden verse fuertemente influenciados por acontecimientos recientes.

Por ejemplo, existen multitud de situaciones en las que el acceso a las instalaciones físicas de la organización puede verse perturbado: incidente de salud, evento de fuerza mayor (inundación, daños materiales, etc.), interrupción del transporte y servicios públicos, etc. Algunas posibles causas pueden mitigarse con acciones preventivas (ejemplo: instalar un generador eléctrico para hacer frente a fallas en el suministro eléctrico). Para el resto de las perturbaciones, se recomienda agruparlas según sus efectos y luego cuidar

la continuidad (ejemplo: tomar medidas para atender la imposibilidad de acceder a las instalaciones de la organización, independientemente de los hechos que provocan la imposibilidad). Cabe señalar que la creciente automatización de los procesos tributarios y las experiencias con la expansión del trabajo remoto, impulsadas también por la reciente epidemia de COVID-19, pueden facilitar decisiones de contingencia en casos de imposibilidad de acceso a los lugares de trabajo.

Según la Encuesta Global de Crisis y Resiliencia 2023 de PwC[2], el 96% de 1.812 líderes empresariales dijeron que sus organizaciones habían experimentado interrupciones en los últimos dos años, y el 76% manifestaron que la interrupción más grave tuvo un impacto mediano a alto en sus operaciones. Debido a las repercusiones negativas, el 89% de los ejecutivos incluyen la resiliencia como una de sus prioridades estratégicas más importantes. Sin embargo, solo el 70% de los encuestados expresaron confianza en la capacidad actual de sus organizaciones para responder a disrupciones.

Las administraciones tributarias no están exentas de estos posibles disturbios y por lo tanto deben aumentar su resiliencia, abordando el enfrentamiento a amenazas a la continuidad de sus actividades como una necesidad estratégica.

Amenazas potenciales a la continuidad operacional de administraciones tributarias – visión general - ejemplos:
1. Ciberataques y Seguridad de Datos: Proteger los sistemas de información tributarios contra ciberataques (*malware*, *ransomware*, *phishing*, ciberactivismo, etc.) y asegurar la integridad y confidencialidad de los datos fiscales.
2. Fallas de Hardware y Software: Preparación para fallos en equipos críticos y en el software de gestión tributaria, incluyendo planes de respaldo y recuperación.
3. Interrupciones en la Red y Conectividad: Garantizar la continuidad de los servicios en caso de fallas de conectividad, ya sean internas o en proveedores de internet.
4. Recuperación de Desastres Naturales/eventos climáticos: Planificar la respuesta y recuperación ante desastres naturales que puedan afectar la infraestructura física de TI.
5. Sobrecarga de Sistemas Durante Periodos Críticos: Manejar la alta demanda en períodos clave, como las fechas límite para presentación de declaraciones de impuestos.
6. Cumplimiento de Normativas y Cambios Legislativos: Adaptarse rápidamente a los cambios en la legislación tributaria y asegurar el cumplimiento normativo en los sistemas de TI.

2 Véase **https://www.pwc.com/gx/en/issues/crisis-solutions/global-crisis-survey.html**

Amenazas potenciales a la continuidad operacional de administraciones tributarias – visión general - ejemplos:
7. Gestión de la Continuidad del Personal: Asegurar la disponibilidad de personal capacitado durante emergencias y desarrollar planes de sucesión y capacitación.
8. Protección contra la Pérdida de Datos: Implementar soluciones robustas de back-up y recuperación de datos para prevenir la pérdida de información crítica.
9. Fallas de Energía: Prepararse para cortes de energía y tener soluciones de respaldo, como generadores o sistemas UPS.
10. Errores Humanos: Minimizar el riesgo de errores humanos que puedan causar interrupciones o pérdidas de datos y ofrecer formación adecuada.
11. Problemas de Escalabilidad y Actualización de Sistemas: Mantener la capacidad de los sistemas para adaptarse a cargas de trabajo crecientes y gestionar actualizaciones sin interrumpir los servicios.
12. Amenazas Internas: Prevenir y detectar acciones maliciosas por parte de empleados que puedan comprometer la seguridad o el funcionamiento de los sistemas.
13. Crisis Sociales: Planear como mitigar interrupciones de servicios derivadas de paros y huelgas internos y externos a la administración tributaria.
14. Mala Gestión de Proveedores y Terceros: Asegurar la continuidad y confiabilidad de servicios proporcionados por terceros– incluyendo servicios administrativos, software, hardware y servicios de nube.

Despunta así la necesidad imperativa de un Plan de Continuidad de Negocios (PCN) específicamente diseñado para las administraciones tributarias y sus complejidades inherentes. Un PCN es un manual estratégico creado para ayudar a una organización a mantener o reanudar rápidamente funcionalidades del negocio ante una interrupción. Este Plan es el principal componente de un Sistema de Gestión de Continuidad de Negocios (SGCN).

El PCN describe los procedimientos e instrucciones que la organización debe seguir durante eventos disruptivos, para minimizar el tiempo de inactividad, y abarca procesos organizacionales, activos, recursos humanos y partes interesadas externas a la institución.

Para el desarrollo de un PCN no se necesita reinventar la rueda. Existen experiencias documentadas y un conjunto de normas y buenas prácticas internacionales que pueden guiar el proceso, tales como:

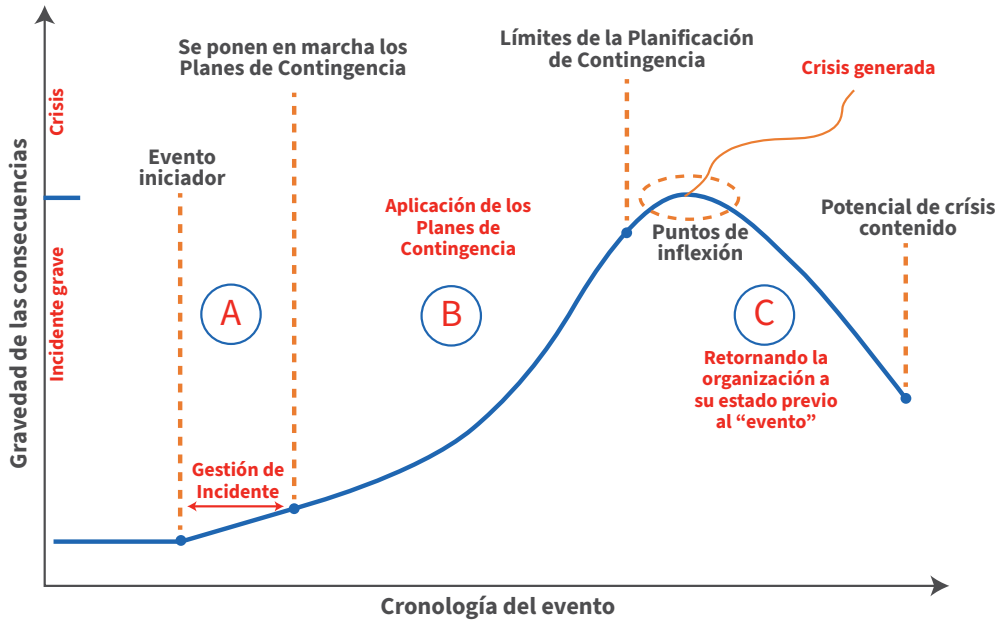
- Norma ISO 22301 – 2019 – Seguridad y resiliencia - Sistema de gestión de la continuidad del negocio – Requisitos;
- Norma ISO 22313 – 2020 – Seguridad y resiliencia - Sistema de gestión de la continuidad del negocio – Directrices para el uso de la ISO 22301;
- Especificación Técnica ISO/TS 22317 –2021 – Seguridad de la sociedad - Sistema de gestión de la continuidad del negocio – Directrices para el Análisis de Impacto en el Negocio (BIA por su sigla en inglés).
- Marcos de gestión de servicios de TI, como ITIL y COBIT (segmentos de riesgo y continuidad)

2 Génesis de una crisis

La Figura 1 a continuación describe la cronología de transformación de una situación normal hacia un incidente, que al no contenerse puede llegar a un nivel grave y requiere la aplicación de planes de contingencia para evitar una crisis.

Incidente es un episodio inesperado o circunstancia accidental que cambia el orden normal de las cosas. Es algo corriente en la vida de instituciones y existen procesos propios para corregirlo ("A"). Sin embargo, si tales procesos resultan insuficientes, sería necesario poner en marcha planes de contingencia ("B"). Normalmente los planes de contingencia son suficientes para estancar incidentes graves, retornando la organización a su estado previo al evento inicial ("C").

Figura 1: **Cronología y gravedad de las consecuencias de un incidente.**



Fuente: Adaptado de Smith y Elliot (2006).

Las grandes perturbaciones surgen cuando el evento se amplifica, generando circunstancias que no fueron consideradas por los responsables de evaluar los riesgos. Se produce así una situación de crisis; en este punto, probablemente se requerirán recursos externos para recuperarse del daño causado y evitar una mayor escalada. Dado que los planes de contingencia cubren situaciones de riesgo previamente evaluadas, vemos la importancia de un estudio de riesgo más completo y detallado.

3 Sistema de Gestión de Continuidad de Negocios

Un Sistema de Gestión de Continuidad de Negocio (SGCN) identifica los efectos que puede tener una interrupción de la actividad y establece medidas de respuesta. Resáltese que la evaluación anticipada del potencial de interrupción puede conllevar a la adopción de medidas preventivas. Debe tener en cuenta todos los diferentes factores y agentes a los cuales corresponde actuar ante una situación de riesgo. Si es rígido, seguramente dejará de lado algunas de las amenazas que pueden afectar negativamente a su funcionamiento (Estruga, 2023).

La gestión de la continuidad de negocio (GCN) es un proceso recurrente, con su propio ciclo de vida.

La Figura 2 a continuación resume el ciclo de vida de la GCN.

Figura 2: **Ciclo de vida de la GCN**

Fuente: Adaptado de las Normas BSI 25999 e ISO 15999–1.

El principal objetivo de un SGCN es permitir la administración, planificación, seguimiento, control y mejoramiento permanente de la estrategia de continuidad del negocio de la organización para garantizar su operación crítica en caso de una contingencia.

4 Las 4 etapas del SGCN

El ciclo comienza con el **entendimiento de la organización (I)**, sus procesos de negocio, recursos y prioridades. El SGCN debe estar alineado con las estrategias de la organización. Además, una de las mejores prácticas para los equipos de liderazgo es entender el panorama de amenazas, especialmente las más probables en los contextos social y natural en que actúa la administración tributaria, e identificar problemas potenciales. En la medida en que las estrategias son dinámicas, la ejecución del SGCN también debe reflejar cambios. Por lo tanto, el SGCN no puede ser inalterable o independiente de la dirección de la organización. Análisis de los tipos SWOT[3], análisis de riesgos y planeación estratégica también pueden ser útiles para subsidiar el conocimiento.

La ISO 22301 requiere que la organización determine qué será cubierto por la continuidad del negocio, así como qué será excluido. Por otro lado, a la organización se le exige que comunique a las partes, tanto internas como externas, el alcance del SGCN.

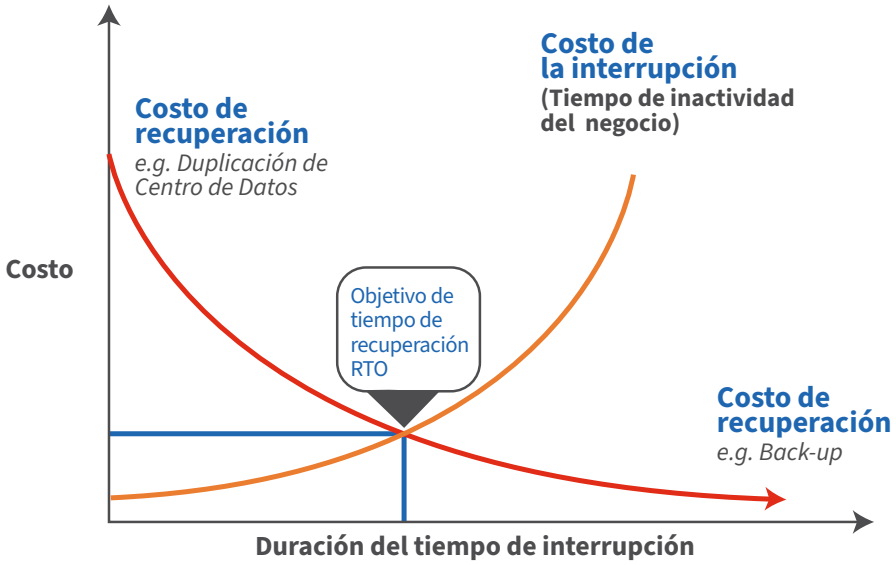
A partir de este entendimiento, podemos trabajar en la determinación de la estrategia de **GCN (II)**. Para ello, es fundamental evaluar cómo las disrupciones y desviaciones pueden afectar al negocio, dada la dirección estratégica de la organización. Esto se hace a través del Análisis de Impacto de Negocios (*Business Impact Analysis / BIA*). Este análisis debe examinar el impacto que produce la disrupción en términos de criticidad e importancia, las consecuencias sobre otras áreas de negocios y los datos que se perderán. Dicho de otra manera, el primer paso para construir un PCN es evaluar los procesos de negocio para determinar cuáles son los más críticos; cuáles son los más vulnerables y ante qué tipo de eventos; y cuáles son las pérdidas potenciales correspondientes a periodos de inactividad de horas, días o semanas.

Si bien lo ideal es tener una interrupción muy baja y no perder ninguna operación ni dato, este tipo de capacidad requiere muchos recursos y **es necesario evaluar adecuadamente los costos**. La Figura 3

3 Sigla para Fuerzas (Strengths), Debilidades (Weaknesses), Oportunidades (Opportunities) y Amenazas (Threats).

a continuación muestra la variación de costos de una estrategia, desde una que presupone interrupción próxima a cero, pero de alto costo, hasta otra que admite una interrupción prolongada, pero de bajo costo.

Figura 3: **Costo de recuperación versus tiempo de interrupción**



Fuente: Adaptado de Smith y Elliot (2006).

El Objetivo de Tiempo de Recuperación (RTO - Recovery Time Objective) es el tiempo máximo aceptable que una aplicación, computadora, red o sistema puede estar inactivo después de que se produzca un desastre inesperado, una falla o un evento comparable.

La disponibilidad de recursos financieros y/o humanos es un factor crítico para la determinación de una estrategia ideal para la gestión de continuidad del negocio, indicada por la evaluación de riesgos. Asimismo, no tomar decisiones por falta de recursos para una solución óptima no debe ser considerado una opción. Se pueden crear escenarios con estrategias sencillas y de bajo costo (contemplando las situaciones más probables detectadas y ampliándose los RTO), que avanzan para niveles más completos conforme recursos son puestos a disposición. Por ejemplo, iniciar con back-ups completos ubicados fuera del centro de datos principal, hasta llegar – posiblemente – a una duplicación del centro de datos. En la misma línea se ubica la contratación de servicios en nube, que puede ser otra estrategia factible.

La continuidad de los sistemas de información es de extrema importancia en la continuidad de negocios de una administración tributaria. La criticidad de cada sistema depende de la importancia estratégica del área a la que sirve y los criterios de evaluación suelen variar con el tiempo: puede haber estacionalidad en los impuestos (como la determinación y recaudación del Impuesto Vehicular, por ejemplo) o la concentración de una actividad en determinados días del mes (fechas límites de recaudación de determinados impuestos, por ejemplo).

Los criterios también pueden variar dependiendo de otros factores, como hacer que la funcionalidad de registro de contribuyentes esté disponible durante un período de estímulo para la regularización del estatus fiscal de las empresas.

La ampliación del uso de facturas electrónicas incluye nuevos riesgos. Casos importantes están relacionados con los sistemas de emisión/validación de facturas electrónicas: algunas veces la propia administración tributaria emite las facturas para pequeños/medianos contribuyentes, y la paralización de este sistema causaría muchos daños a la economía; otras veces estas operaciones están tercerizadas y las empresas involucradas deben ser analizadas por el Plan de Contingencia.

Como se puede ver, debe haber sentido común y cooperación en estas evaluaciones de criticidad e importancia para las partes interesadas, de modo que el estudio se base en intereses y objetivos amplios, y no sólo en percepciones localizadas.

La interdependencia entre sistemas es un tema importante por considerar. Puede suceder que se haga uso directo de un sistema y este dependa de otro sistema que no se considera crítico o importante. Las cadenas de dependencia deben ser claramente conocidas y respetadas, esto hecho con el apoyo de la unidad de TI.

El **desarrollo e implementación de la estrategia de Gestión de Continuidad de Negocios (III)** permite elegir e implementar una respuesta adecuada para cada escenario, sistema o servicio, considerando parámetros definidos como aceptables, como nivel de operación y tiempos. Las opciones tendrán en cuenta la resiliencia y las opciones de contramedidas existentes, con especial atención a los costos de implementación y mantenimiento.

También en este renglón se crea una estructura de gestión que abarca la gestión de incidentes, la continuidad del negocio y los planes de recuperación, entre otros. Estos planes detallan las acciones a tomar durante y después de un incidente, con el objetivo de mantener y restaurar las operaciones según los parámetros establecidos.

Probar, mantener y revisar (IV) el plan de gestión de continuidad de negocios permite a la organización poder demostrar en qué medida sus estrategias y planes son completos, actualizados y precisos. Es una ocasión para identificar oportunidades de mejora.

Se debe planear las pruebas periódicas utilizando los tipos y métodos propuestos en la norma ISO 22301 (sencillo, mediano, complejo). Cada tipo de plan debe tener un programa de mantenimiento/revisión definido (por ejemplo, semestral, anual). Probar un PCN es la única forma de comprobar su efectividad antes que ocurra un evento imprevisto.

El plan debe ser un documento vivo que sea revisado periódicamente para mantenerse actualizado también con las mejoras de los sistemas y los cambios organizacionales.

5 Cultura organizacional

Otro aspecto crítico es la inclusión de la gestión de continuidad de negocios en la cultura organizacional, permitiendo que se configure como parte de los valores de la organización, brindando confianza a las partes interesadas sobre la capacidad de esta para sobrevivir a eventos disruptivos. Las acciones de sensibilización y formación cubren este aspecto. El factor humano es una parte importante en este contexto, el cual debe ser considerado tanto en la estructuración y ejecución del proyecto como en su operacionalización, incluyendo la creación de un consenso institucional sobre su importancia estratégica para la organización.

6 PCN, COVID-19 y otras crisis de amplio alcance

La crisis provocada por el COVID-19 no solo afectó la vida de las personas alrededor del mundo, como también trajo desafíos para las administraciones tributarias sobre cómo asegurar la continuidad de sus actividades críticas y la seguridad de los funcionarios y de los contribuyentes durante la pandemia.

En esta línea, organismos internacionales propusieron orientaciones a las administraciones tributarias para afrontar esos desafíos mencionados, como CIAT/IOTA/OECD, 2020 y Brondolo, Aslett y Komso, 2020. Se observa que estas orientaciones siguen, estructuralmente, el modelo propuesto por las normas ISO de seguridad y resiliencia, mencionadas al inicio de este documento.

Aunque escritas en el contexto del COVID-19, estas orientaciones pueden servir de base para evaluación de medidas destinadas a afrontar otros tipos de crisis de amplio alcance, especialmente las causadas por eventos naturales (por ejemplo, otras pandemias, terremotos, inundaciones, erupciones volcánicas).

Existe consenso entre los organismos internacionales en que no existe una única solución a este problema, ya que las administraciones tributarias parten de diferentes posiciones (tales como grado de digitalización de los servicios, despliegue de posibilidades de trabajo remoto, acuerdos de subcontratación, ámbito de actuación de estas).

Se observa que el apoyo de las tecnologías de la información es de suma importancia para un Plan de Contingencia diseñado para mitigar una epidemia. Como mínimo, el plan debe garantizar la disponibilidad ininterrumpida de: (1) sistemas centrales de procesamiento; (2) servicios electrónicos al contribuyente; y (3) elementos de TI de funciones de soporte esenciales y de misión crítica. Esto incluye permitir que directivos y funcionarios trabajen de forma remota proporcionándoles el equipo necesario, la capacitación y el acceso electrónico seguro a los sistemas.

Se considera así que las administraciones tributarias que lograron desarrollar los dos atributos a continuación pueden enfrentar más prontamente estos desastres:

- Maximización de la automatización (informatización) de los procesos tributarios internos – utilizados por los funcionarios, y externos – utilizados por los contribuyentes.
- Disponibilidad de capacidades administrativas y tecnológicas para implementación de trabajo remoto en larga escala.

En Brondolo, Aslett y Komso, 2020 se propone un conjunto de Planes de Acción, similares a las indicaciones de las normas ISO, pero orientados a la pandemia en discusión:

a) Plan de acción para sistemas de misión crítica
Garantiza que la administración tributaria pueda seguir actuando en sus operaciones más importantes durante la crisis.

b) Plan de acción para soporte a salud y seguridad
Acciones destinadas a proteger empleados y visitantes de enfermedades infecciosas.

c) Plan de soporte al despliegue de fuerza laboral
Garantizar que la administración tributaria tenga fuerza laboral adecuada para realizar sus funciones críticas.

d) Plan de soporte a las TI
Las TI son muy importantes para acciones de mitigación de la pandemia. Varias orientaciones son propuestas en este documento.

e) Plan de apoyo a las instalaciones
Destinado a asegurar la seguridad y la integridad de los espacios físicos de la administración tributaria durante la epidemia.

f) Plan de soporte a las comunicaciones
La comunicación efectiva es parte importante de la respuesta a una crisis, tanto las comunicaciones internas (con gestores y empleados de la administración tributaria) como externas (con todas las partes interesadas dentro y fuera del gobierno, incluyendo contribuyentes).

7 La práctica de PCN en Administraciones Tributarias

A continuación, serán resumidas prácticas de continuidad de negocio/continuidad operativa disponibles en administraciones tributarias seleccionadas.

7.1 SUNAT (Superintendencia Nacional de Aduanas y de Administración Tributaria – Perú)

La SUNAT es un organismo técnico especializado adscrito al Ministerio de Economía y Finanzas, tiene como finalidad primordial administrar los tributos del gobierno nacional.

Aunque SUNAT disponga de sedes en todo el territorio del país, pero las principales actividades se desarrollan en Lima Metropolitana, siendo estas las más vulnerables geográficamente.

El desarrollo del Plan de Continuidad Operativa (PCO) atiende a lo determinado por resolución ministerial que orienta la formulación de planes de continuidad operativa de entidades públicas. La activación del PCO está prevista ante la ocurrencia de un evento adverso cuya magnitud afecte específicamente la operatividad de la SUNAT, ocasionado por un sismo de gran magnitud, tsunami en Lima y Callao, incendio, ataque terrorista, convulsión social, ataque informático o pandemia, sin que por ello deje de considerarse otros peligros que puedan suscitarse.

El Plan identifica y describe en detalles los riesgos presentes y los recursos disponibles, con estimación de los niveles de impacto asociados y respectivas acciones.

Entre los recursos principales de SUNAT están sus sistemas informáticos, catalogados como Activo Crítico Nacional. La SUNAT mantiene una estrategia general de alta disponibilidad entre sus centros de datos de Surco y San Isidro, lo que le permite recuperar cualquier servicio de forma eficiente y efectiva ante un fallo de red, servidor de aplicaciones o servidor de base de datos. El Centro de Datos de Surco, especialmente, es un

servicio de housing con certificación TIER III por el Uptime Institute[4]. Esta estrategia está considerada en las determinaciones de acciones del PCO.

Están determinadas 8 actividades críticas que deben ser mantenidas:

1. Control de ingreso de mercancías
2. Control de salida de mercancías
3. Administración de la recaudación tributaria
4. Asistencia al contribuyente y al ciudadano
5. Procedimiento de intercambio de información entre países
6. Gestión de Recursos Humanos
7. Gestión administrativa
8. Administración financiera

El PCO identifica roles y responsabilidades para el desarrollo de las actividades críticas, sedes alternas para distintas actividades, considerando sus capacidades y características de construcción (por ejemplo, elementos de disipación de energía en eventos sísmicos), responsabilidades por evaluación de daños y procesos de divulgación y de convocatoria de funcionarios.

Consta también del Plan cronogramas de ejercicios (simulacros y simulaciones).

Para más detalles, véase SUNAT, 2022a y SUNAT, 2022b.

7.2 IRS (Servicio de Rentas Internas de los Estados Unidos de América)

Lo que sigue es una descripción general del Plan de Continuidad del IRS, sus directrices y componentes.
La planificación de la continuidad establece actividades y esfuerzos para documentar y garantizar que el IRS sea capaz de continuar con las Funciones Esenciales de su Misión (MEF por su sigla en inglés) y las Actividades de Apoyo Esenciales (ESA por su sigla en inglés) durante una amplia gama de emergencias potenciales.

4 Uno de los requisitos de la certificación TIER III es disponibilidad de 99,98%.

La planificación de la continuidad del IRS se basa en el supuesto de que no habrá advertencias de posibles emergencias o incidentes, utilizando el peor de los casos (la inaccesibilidad o indisponibilidad de una instalación del IRS y todo su contenido). El objetivo principal del Plan de Continuidad es asegurar la recuperación de los MEF y las ESA.

Los MEF están directamente relacionados con el cumplimiento de la misión de la organización: proporcionar los bienes y servicios a la Nación para cuya producción se creó la agencia en primer lugar. Son ellos: (i) procesamiento de la recepción de impuestos, (ii) procesamiento de declaraciones de impuestos y (iii) procesamiento de reembolsos de impuestos. Estos servicios deben estar operativos en un plazo de 12 horas.

Las ESA son las funciones esenciales que deben realizarse para apoyar el desempeño de la agencia en sus MEF. Por lo general, las ESA son comunes a la mayoría de las agencias (pagar al personal, proporcionar un lugar de trabajo seguro, garantizar que los sistemas informáticos estén funcionando, etc.), pero no cumplen la misión de la agencia. Estas deben estar operativas rápidamente para apoyar la recuperación del MEF. El tiempo específico será determinado para cada proceso. Las ESAs son las siguientes: Seguridad Física; Gestión de instalaciones; Tecnología de la información; Servicios Legales Generales/Asesor Principal; Gestión financiera; Adquisiciones; Comunicaciones; Nómina; Recursos Humanos/Beneficios.

Existen además los Procesos de Negocio Prioritarios (BPP, por su sigla en inglés), importantes y urgentes para cumplir la misión de las unidades de negocio en apoyo al MEF, pero el cumplimiento de los BPP no completa la misión ni entrega los servicios para los cuales la agencia fue creada. Estas funciones suelen recuperarse mediante reubicación.

El IRS tiene seis BPP: Asistencia a los contribuyentes; Defender el trato justo al contribuyente; Realizar actividades de cumplimiento tributario; Efectuar litigios; Proporcionar procesos de apelación y Servicios en línea.

Los objetivos del Plan de Contingencia están establecidos por Directiva Federal e incluyen: Garantizar la seguridad del personal y los visitantes del IRS; Garantizar que el IRS pueda continuar realizando sus MEF y ESA, incluida la realización de actividades desde una ubicación alternativa, si necesario; Reducir la pérdida de vidas y minimizar los daños y pérdidas a la propiedad; Ejecutar según sea necesario una sucesión exitosa en el cargo con la correspondiente delegación de autoridades en caso de que una interrupción haga que

el liderazgo del IRS sea incapaz, no esté disponible o sea incapaz de asumir y desempeñar sus deberes y responsabilidades; Reducir o mitigar las interrupciones en las operaciones del IRS; Garantizar que el IRS tenga instalaciones disponibles donde pueda continuar realizando sus MEF durante un evento de continuidad o emergencia; Proteger las instalaciones esenciales, los registros esenciales, los equipos y otros activos en caso de una interrupción; Lograr una recuperación y reconstitución oportuna y ordenada de un evento de continuidad o emergencia; Garantizar y validar la preparación para la continuidad del IRS a través de un programa integrado de pruebas, capacitación y ejercicios de continuidad para respaldar la implementación de los planes de continuidad del IRS.

Los siguientes requisitos de continuidad son, entre otros, parte del plan:

- El IRS debe ser capaz de continuar el desempeño de sus MEF y ESA durante cualquier emergencia por un período de hasta 30 días o hasta que se puedan reanudar las operaciones normales.

- El IRS debe tener la capacidad de estar en pleno funcionamiento en sus instalaciones de continuidad lo antes posible después de que ocurra una emergencia, pero a más tardar 12 horas después de la activación de las operaciones de continuidad.

También conforman el Plan de Contingencia las autoridades y sus responsabilidades, órdenes de sucesión (cambio de liderazgos), delegaciones de autoridad de emergencia, responsabilidades por supervisión y otros. Para más detalles, véase IRS, 2022.

7.3 SEFAZ-MA (Secretaría de Hacienda del Estado de Maranhão – Brasil)

Maranhão es un Estado del noreste de Brasil y su Secretaria de Hacienda (SEFAZ) tiene como misión promover y controlar el cumplimiento de las obligaciones tributarias con equidad y eficiencia para contribuir al desarrollo del Estado[5].

5 En Brasil los Estados son unidades federativas con autonomía administrativa / tributaria / financiera, con competencia para legislar y administrar determinados tributos.

El uso intensivo de las tecnologías de información ha contribuido fuertemente para el cumplimiento de la misión de la SEFAZ.

En 2019, se realizó un análisis mediante la Herramienta de Evaluación de Diagnóstico de la Administración Tributaria (TADAT). En aquella ocasión, una de las debilidades destacadas fue la inexistencia de un Plan de Continuidad de Negocios especialmente relacionados con la TI. El Plan Estratégico 2020-2023 atendió esta necesidad, determinando el desarrollo de un Plan de Continuidad de Negocios para las tecnologías de información, alineado con las demás actividades de la SEFAZ[6].

Cabe resaltar que ya se utilizaba como parámetro de adquisiciones de TI la resiliencia del ambiente central (Centro de Datos), con equipos redundantes de alta disponibilidad, sala cofre, refrigeración independiente, generadores eléctricos suplementares y sistema de seguridad física avanzado.

El Plan de Continuidad desarrollado utilizó como base metodológica las normas ISO y ABNT[7], generando un conjunto de planes operativos para los escenarios de fallas identificadas y además estrategias para mejoría de la continuidad:

i) Estrategia de corto plazo, basada en el fortalecimiento del ambiente central de TI e identificación de local para futura implementación de un site secundario. Será utilizado para este fin el Centro de Dados de la Secretaría Adjunta de Tecnología de Información, que necesita ser ampliado y adecuado. En esta fase inicial, este local abrigará medias de back-up de datos.

ii) Estrategia de mediano/largo plazo, que evaluará la factibilidad de implementación de un sitio secundario operando en frío (recibiendo actualizaciones en una base de datos de respaldo y con el equipo informático necesario para operar sistemas prioritarios en modo de contingencia. En caso de una falla crítica en el sitio principal, el sitio secundario asumiría la operación planificada mediante acciones / procedimientos previamente definidos; el alcance de los sistemas prioritarios a operar depende del

6 Véase SEFAZ-MA, 2020.

7 Asociación Brasileña de Normas Técnicas.

tamaño del equipo involucrado) u operando en caliente (simultáneamente con el sitio principal, con la carga distribuida de aplicaciones y bases de datos idénticas y sincronizadas; en caso de falla en uno de los sitios, el otro se haría cargo automáticamente de todas las operaciones; dependiendo del tamaño del equipo, la degradación del servicio podría ser mínima o aceptable).

El uso de la nube será evaluado como una alternativa.

El Plan Estratégico 2024-2027 contempla la complementación de la estrategia de continuidad de mediano/largo plazo, con la asignación de los recursos necesarios.

8 Auditorías y automatización

Realizar una auditoría de continuidad de negocio es una de las formas de asegurar que los eventos disruptivos afectarán al mínimo la actividad.

Para que esta sea efectiva, los auditores (tanto internos como externos) deben seguir una serie de pautas y recomendaciones. Algunos temas que deben ser tratados: confirmar el alcance del SGCN; liderazgo e implicación de la alta dirección (los ejecutivos deben acordar los principios y el equilibrio entre costos, complejidad y alcances); documentación de los objetivos de la continuidad de negocios; concientización de todas las partes implicadas; revisar si existen todos los componentes necesarios (BIA, estrategias, planes de continuidad, etc.); proponer mejoras y correcciones (Estruga, 2023).

La Administración Tributaria de Canadá (CRA, por su sigla en inglés) promociona auditorías internas periódicas a sus sistemas de información, como parte de un Programa de Gestión de Continuidad de Negocios. En vísperas de que el COVID-19 fuera declarado pandemia, estaba realizando una de estas auditorías, cuyos resultados fueron utilizados también para mejorar la respuesta a la calamidad (CRA, 2021).

Los resultados clave esperados de las auditorías impulsadas por CRA son ajustes a los siguientes documentos: **Planes de continuidad del negocio:** mejorías de los planes que describen los requisitos mínimos aceptables de configuración de recuperación, las estrategias y toda la información de contacto necesaria para mantener y recuperar los servicios críticos; **Inventario de servicios críticos:** revisión de la lista de servicios cuyo compromiso, en términos de disponibilidad o integridad, daría lugar a un grado alto o muy alto de daño a la salud, la seguridad o el bienestar económico de los canadienses o al funcionamiento eficaz del Gobierno de Canadá; **Aplicaciones y servicios comerciales críticos:** actualización de la lista de aplicaciones que habilitan los servicios críticos; **Informes posteriores a la acción:** exploración de los documentos que capturan experiencias, brechas y lecciones aprendidas después de interrupciones no planificadas o ejercicios de prueba.

En el mercado existen paquetes de software que automatizan la mecánica operativa de un SGCN. En realidad, eses sistemas mantienen un repositorio de los documentos del SGCN y establecen las relaciones entre ellos, permitiendo la visualización integrada y agilidad en el accionamiento de estos. No resulta eficaz ni operativo depender de búsquedas en manuales en papel. Además, en desastres naturales es común que el personal responsable no llegue a tiempo a los centros de trabajos asignados, por quedar atrapadas en atascos, indisponibilidad de transporte, etc. Estos paquetes de software pueden posibilitar la interacción a distancia entre los responsables, con base en una infraestructura adecuada. Los mismos paquetes son continuamente mejorados y las más recientes alternativas pueden ser buscadas en la Web, como el documento de la empresa Veritis[8].

Es muy importante resaltar que un software de automatización no hace la gestión de continuidad: sencillamente, él automatiza muchas tareas administrativas y de coordinación previamente establecidas en el Plan.

8 Véase https://www.veritis.com/blog/8-best-business-continuity-management-software-solutions/

9 PCN en la nube

Otra consideración importante es evaluar el uso de la nube como estrategia de contingencia. Aunque se considere la problemática de uso de datos confidenciales confiados a la administración tributaria en ambientes externos, se puede evaluar por lo menos la contingencia de subsistemas y datos no críticos en nube.

Hay aspectos importantes que deben ser considerados en una estrategia de continuidad de negocios en la nube, conforme propuesto en Posey (2022):

- **Costo:** Los ahorros propagados de las nubes públicas pueden ser difíciles de lograr. Lo mismo para nubes privadas o estatales. Es importante evaluar el costo específico para un plan de contingencia.

- **Compatibilidad de hardware y software:** Algunas aplicaciones no funcionarán en la nube, mientras que otras funcionarán, pero pueden ser demasiado costosas para ejecutarlas en ese entorno.

- **Reputación del proveedor de la nube y garantías sobre la continuidad:** No se deben confiar sistemas de misión crítica a un proveedor con reputación de sufrir interrupciones periódicas o uno que podría cerrar la próxima semana. Un acuerdo de nivel de servicio debe garantizar un nivel mínimo de servicio.

- **Propiedad de los datos:** El proveedor debe ser transparente sobre dónde se almacenarán los datos y los términos de servicio deben garantizar la seguridad de acceso a estos datos.

- **El costo de sacar datos de la nube:** La mayoría de los proveedores de nube cobran una tarifa de retirada de datos. Esto incluye datos que migran al propio centro de datos de una organización o a otra nube. Estas tarifas pueden ser bastante elevadas, por lo que es importante saber cuánto costaría un traslado. Incluso existen ciertas operaciones de respaldo y recuperación que pueden generar tarifas de salida de datos. Se debe tener en claro cuándo se podría incurrir en dichos cargos.

- **¿Quién es responsable de realizar copias de seguridad de los datos y qué métodos se utilizarán?** La mayoría de los proveedores de nube han adoptado un modelo de responsabilidad compartida en el que el proveedor es responsable de mantener la infraestructura subyacente y los suscriptores son responsables de realizar copias de seguridad y proteger sus propios datos.

- **Costo y disponibilidad de soporte dentro de la nube:** Es importante verificar que habrá ayuda disponible en tiempos de crisis y cuánto podría costar ese apoyo adicional.

- **Seguridad:** Se debe verificar si el plan de continuidad de negocios basado en la nube socavará la seguridad. Esto es especialmente cierto en instituciones reguladas, como las administraciones tributarias, donde se pueden incurrir en sanciones por violaciones de las mejores prácticas de seguridad.

Como se observa, muchos de estos aspectos deben ser considerados en cualquier estrategia de uso de la nube para hospedar sistemas de información. Administraciones tributarias de México, Perú, Guatemala y Colombia poseen estrategias propias de uso de la nube.

10 Comentarios finales

A pesar de la importancia asumida por los gestores tributarios y ahora reforzada por la pandemia de COVID-19, de 92 evaluaciones en TADAT (Herramienta Diagnóstica de Evaluación de la Administración Tributaria) realizadas a la fecha, la mayoría de los países de ingreso mediano y bajo no contaban con PCN robustos (FMI-FA, 2020).

El desarrollo de un SGCN abarca aspectos tecnológicos y de gestión, pero posiblemente es el diseño e implementación del componente estratégico el principal factor para lograr éxito.

Los ejecutivos principales de la administración tributaria deben estar involucrados desde el inicio, conociendo y participando en los aspectos principales del Plan y en la definición de sus límites.

La definición de los límites y condiciones de interrupción implican en nuevos recursos financieros y humanos: menos interrupción de servicios significa más costos (ver Figura 3). Así, el análisis conjunto de las opciones estratégicas de recuperación versus los respectivos costos y límites de actuación evitarán futuras sorpresas.

Referencias

Brondolo, J., Aslett, J., Komso, A. (2020). Tax Administration: Designing a Business Continuity Plan for an Epidemic. IMF Technical Notes and Manuals. TNM 2020/001. IMF Fiscal Affairs Department. Washington, DC.

CIAT/IOTA/OECD (2020). Tax Administration Responses to COVID-19: Business Continuity Considerations. OECD. Paris. Disponible en: https://biblioteca.ciat.org/opac/book/5721

CRA (2021). Internal Audit – Information Technology Continuity Management. Disponible en: https://bit.ly/4b250gh

Estruga, N. (2023). ISO 22301: Cómo establecer un Sistema de Gestión de Continuidad del Negocio. Ealde Business School. Disponible en: https://www.ealde.es/iso-22301-continuidad-negocio/

FMI-FA (2020). Continuidad de las Operaciones de las Administraciones de Ingresos Públicos. Fondo Monetario Internacional – Fiscal Affairs. Disponible en: http://bit.ly/48F9at1

IRS (2022). Security, Privacy and Assurance: Overview of Continuity Planning (Manual). IRS. Disponible en: https://www.irs.gov/irm/part10/irm_10-006-001

Posey, B. (2022). Business continuity in the cloud: Benefits and planning tips. TechTarget Blog. Disponible en: https://www.techtarget.com/searchdisasterrecovery/tip/Business-continuity-in-the-cloud-Benefits-and-planning-tips

SEFAZ-MA. (2020). Plano Estratégico 2020-2023. Secretaria de Estado de Fazenda – SEFAZ. São Luís. Disponible en: https://sistemas1.sefaz.ma.gov.br/portalsefaz/files?codigo=20180

Smith, D. y D. Elliot (Editores) (2006). Key Readings in Crisis Management. Routledge, London y New York.

SUNAT (2022) a. Plan de Continuidad Operativa. Oficina de Seguridad y Defensa Nacional. Julio. Disponible en: https://www.sunat.gob.pe/legislacion/superin/2022/anexo-135-2022.pdf

SUNAT (2022) b. Plan de Prevención y Reducción de Riesgos de Desastres de la SUNAT. Oficina de Seguridad y Defensa Nacional. Disponible en: https://www.sunat.gob.pe/legislacion/superin/2023/anexo-000241-2023.pdf

ANEXO:
Documentos que componen un Plan de Continuidad de Negocios (lista no exhaustiva)

- Arquitectura Sistémica
- Política de Continuidad de Negocios
- Reporte de BIA – Business Impact Analysis (Análisis de Impacto de Negocios)
- Reporte de Análisis de Riesgos – RAR y Reporte Operacional de Riesgos - ROR
- Reporte de Estrategia de Continuidad de Negocios
- Plan de Administración de Crisis
- Plan de Gestión de Incidentes
- Plan de Continuidad Operacional
- Plan de Recuperación de Desastres
- Plan de Teste y Validación
- Plan de Continuidad de Negocios

Serie
Documentos de Trabajo

Secretaría Ejecutiva del CIAT
Apartado: 0834-02129, Panamá, República de Panamá
Teléfono: (507) 3072428
Fax: (507) 2644926
Correo electrónico: ciat@ciat.org
Sitio web: www.ciat.org