Auditoría Interna

24 de noviembre de 2021
AI-Ad-020-2021

Señor
Alberto López Chaves
Gerente

Asunto: *Plan de continuidad del negocio del ICT*

Estimado señor:

La Auditoría en cumplimiento del Plan Anual de Trabajo y en seguimiento al AI-Ad-09-2020 "*Plan de Continuidad de Negocio del ICT ante la emergencia del COVID 19*", revisa el "*Plan de Continuidad del Negocio del ICT*", (PCN) con la finalidad de comprobar si el mismo cumple con los requerimientos mínimos establecidos por COBIT 2019 y las buenas prácticas, determinándose lo siguiente:

a) Estándar aplicado:

Se utiliza COBIT 2019 y el estándar ISO/ IEC 27031: 2012[1] para su desarrollo; sin embargo, este último estándar describe los conceptos y principios de la preparación de las tecnologías de la información y las comunicaciones (TIC) para la continuidad del negocio y tiene como objetivo proporcionar la continuidad de los servicios prestados por el Departamento de TI y no se incluye las otras unidades, es decir, no se está considerando lo siguiente:

- Definición de la política de continuidad del negocio, sus objetivos y alcance.
- La resiliencia del negocio.
- Desarrollar la respuesta de continuidad del negocio.
- Realizar ejercicios, probar y revisar el plan de continuidad del negocio (BCP) y el plan de respuesta ante desastres (DRP).
- Revisar, mantener y mejorar los planes de continuidad.

[1] Directrices para la adecuación de las tecnologías de la información y las comunicaciones para la continuidad del negocio (Correspondiente a la norma ISO/IEC 27031:2011).

(506)2299.5800, San José Costa Rica
www.ict.go.cr / www.visitcostarica.com

- Realizar formación sobre el plan de continuidad.
- Administrar los acuerdos de respaldo.
- Realizar revisiones post-reanudación.

b) Política de Continuidad

El PCN no incluye la revisión y actualización de la política de continuidad del negocio, por lo que no se logra determinar si ésta cumple con los aspectos establecidos por COBIT 2019 e ISO 27301 siguientes:

- Si es apropiado para el propósito de la Institución.
- Alcance de la continuidad del negocio.
- Alineación con los objetivos del ICT y de las partes interesadas.
- El marco para establecer los objetivos de la continuidad del negocio
- Compromiso de cumplir los requisitos aplicables.
- Los procesos de negocio de soporte esenciales y servicios de I&T relacionados.
- Los roles y responsabilidades para la continuidad del negocio asignados y comunicados en la institución.

c) Análisis de Impacto de Negocio (BIA)

El BIA del PCN no contempla:

  - Los criterios utilizados para establecer funciones críticas del negocio.
  - Identificación de componentes críticos.
  - Identificación de personal clave y partes interesadas.
- Se basa en actividades y no en procesos críticos de la Institución.
- No se analiza otros tipos de impactos que se pueden producir como consecuencia de la interrupción de los procesos, como el operacional, reputación, legal y contractual.
- No se indica la escala para el análisis de impacto financiero bajo la cual se va a evaluar cada proceso crítico.
- La información de la tabla en la descripción indica que es un comparativo del año 2015 y 2021, sin embargo, se incluye información de los tiempos de recuperación (RTO) y la columna TIR (no se indica la definición de TIR) que no son comparativos entre sí.

- No se realiza un análisis cuantitativo de cada una de los procedimientos críticos identificados.
- La “Tabla 6. Impactos de actividades prioritarias”, no coinciden con el total de procedimientos identificados.
- No se detalla el período máximo tolerable de interrupción, el tiempo y Objetivo de tiempo de recuperación (RTO).

El BIA es un documento en el cual convergen los criterios del área de TI y del negocio para definir cuáles procesos[2], actividades, sistemas, recursos e información son **críticos** para la prestación de servicios y define una serie de indicadores que afectan la planificación de la continuidad del negocio y de TIC[3] (**El subrayado no consta en el original).**

El proceso para realizar un BIA debe incluir al menos:

- Definir los tipos de impacto y los criterios relevantes para el contexto de la organización.
- Identificar y priorizar las actividades clave y los productos y servicios necesarios para lograrlas.
- Evaluar los impactos desde la interrupción hasta las actividades.
- Identificar el momento en el que la no reanudación de estas actividades tendría un impacto perjudicial en la organización (MTPD).
- Identificar el momento en que la reanudación de estas actividades se reanudará a un nivel aceptable (RTO).
- Identificar los recursos para apoyar las actividades priorizadas.
- Determinar las dependencias internas y externas necesarias para respaldar las actividades prioritarias.

d) Análisis de riesgos

El análisis de riesgos realizado por la Administración:

- No identifica, no evalúa, no administra y no revisa las amenazas que podrían afectar la continuidad.

[2] Conjunto de actividades mutuamente relacionadas o que interactúan, que utilizan las entradas para proporcionar un resultado previsto. (ISO 9000 3.4.1)
[3] Tomado del Informe N.° DFOE-LOC-IF-00006-2021 del 5 de agosto, 2021

- Solo se identifican recursos relacionados con las TI y no se consideran otro tipo de recursos que pueden afectar la continuidad del negocio.

La norma ISO 27301 señala que el proceso de evaluación de riesgos debe:

- Identificar los riesgos para las actividades priorizadas de la organización y sus recursos requeridos.
- Analizar y evaluar el riesgo identificado.
- Determinar los riesgos que requieren tratamiento.

El marco COBIT 2019 en la práctica de gestión “DSS04.02 Mantener la resiliencia del negocio”, actividad 5, indica que se debe:

- Evaluar la probabilidad de amenazas que pudieran causar la pérdida de la continuidad del negocio.
- Identificar medidas que reducirán la probabilidad y el impacto a través de una mejor prevención y una mayor resiliencia.

e) Selección de estrategias y soluciones

Las estrategias definidas en el apartado “Formulación de estrategias de continuidad” del PCN no incluyen al menos los elementos siguientes: relación con los procedimientos críticos y departamentos, costos, recursos y responsables.

La norma ISO 27301 señala que la selección de la estrategia y las soluciones de continuidad del negocio de una organización se basará en:

- La capacidad de cumplir con los requisitos para continuar y recuperar actividades priorizadas en una capacidad predeterminada y en un plazo acordado.
- Reducir la probabilidad y el período de interrupción.
- Los recursos necesarios.
- La tolerancia del riesgo de la organización.
- Costes y beneficios.

El marco COBIT 2019 en la práctica de gestión “DSS04.02 Mantener la resiliencia del negocio”, actividad 6, 7 y 8, indica que se debe:

- Analizar requisitos de continuidad para identificar posibles opciones estratégicas empresariales y técnicas.

- Identificar los requisitos y costes de recursos para cada opción técnica estratégica y realizar recomendaciones estratégicas.
- Obtener la aprobación de ejecutivos del negocio para las opciones estratégicas seleccionada.

f) Implementación del plan de continuidad

El apartado denominado “Implementación del plan de continuidad” no detalla los siguientes aspectos:

- Identificación de pasos tomados durante una interrupción.
- Los roles, responsabilidades, personas y los contactos que deberían participar en el mismo.
- Fases y actividades a realizar en los escenarios y posibles desastres.
- Acciones de respuesta frente a cada posible escenario.
- Acciones para recuperar la normalidad.
- Recursos necesarios.
- Dependencias internas y externas.
- No se incluye las oficinas regionales.
- El plan se debe de validar con el plan de emergencias de la Institución.

La norma ISO 27301 señala que el plan y procedimientos de continuidad de negocio deben estar basado en los resultados de las estrategias y soluciones de continuidad de negocio seleccionadas, por lo se requiere que la organización establezca una estructura de respuesta e implemente planes y procedimientos para administrar la organización durante un incidente disruptivo que requiera la activación de soluciones de continuidad del negocio.

Los procedimientos deberán:

- Identificar los pasos tomados durante una interrupción.
- Adaptarse a los cambios en las condiciones internas y externas como resultado de la interrupción.
- Centrarse en el impacto de incidentes que causen interrupción.
- Minimizar el impacto de la interrupción.
- Asignar roles y responsabilidades para las tareas.

Auditoría Interna

El marco COBIT 2019 en la práctica de gestión "DSS04.03 Desarrollar e implementar una respuesta de continuidad del negocio, indica que se debe:

- Definir acciones y comunicaciones de respuesta a incidentes que se deban tomar en caso de interrupción. Definir roles y responsabilidades relacionados, incluida la rendición de cuentas para la política y la implementación.
- Garantizar que los proveedores clave y socios externalizados cuenten con planes de continuidad efectivos. Obtener evidencia auditada según se requiera.
- Definir las condiciones y los procedimientos de recuperación que permitirán la reanudación del procesamiento de negocio. Incluir la actualización y sincronización de bases de datos para preservar la integridad de la información.
- Desarrollar y mantener BCPs[4] y DRPs[5] operativos que contengan los procedimientos a seguir para permitir el funcionamiento continuo de procesos de negocio críticos y/o acuerdos de procesamiento temporales. Incluir vínculos a los planes de proveedores de servicios externalizados.
- Definir y documentar los recursos requeridos para respaldar los procedimientos de continuidad y recuperación, teniendo en cuenta las personas, las instalaciones y la infraestructura de TI.
- Definir y documentar los requisitos de copias de seguridad de la información necesarios para respaldar los planes. Incluir planes y documentos en papel, así como archivos de datos. Considerar la necesidad de seguridad y almacenamiento fuera de las instalaciones.
- Determinar las habilidades requeridas para los individuos involucrados en la ejecución del plan y los procedimientos.
- Distribuir los planes y la documentación soporte de forma segura a las partes interesadas debidamente autorizadas. Asegurar que los planes y la documentación son accesibles en todos los escenarios de desastre.

[4] Plan de continuidad del negocio (BCP)
[5] Plan de recuperación de desastres (DRP)

g) Planes de recuperación y pruebas

El PCN no incluye los planes de recuperación de la Junta Directiva, la Asesoría Legal, la Auditoría, la CIMAT y el PTGP. Además, no incluye el plan de pruebas.

Las buenas practicas indican que se debe establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.

h) Análisis del impacto en el negocio

El análisis del impacto en el negocio se enfoca solo a la parte cuantitativa de la Institución, omitiendo el análisis de otros factores que pueden afectar la continuidad del negocio, asimismo, la omisión de otro tipo de análisis afecta los demás productos de la gestión de la continuidad.

Las observaciones anotadas se deben a que el estándar utilizado es para determinar solo la continuidad de Tecnologías de Información, por lo que el PCN carece de una vinculación con los procesos críticos de la Institución.

Las situaciones determinadas pueden provocar que:

- En caso de desastre[6] el ICT no esté preparado de forma integral para minimizar los efectos de una interrupción de actividades, servicios críticos, ni se protejan bienes y equipos prioritarios de la institución.
- Haya pérdida de información financiera y operativa y documentación valiosa para el ICT.
- Haya pérdidas de recursos humanos y económicos.

La Ley Orgánica, artículo 32, establece que el Gerente es el responsable del eficiente y correcto funcionamiento administrativo de la Institución y debe ejercer las funciones inherentes a su condición de administrador general y jefe superior del

[6] Desastre: Incidente que puede ser anticipado (ejemplo huracanes) o no anticipado (ejemplo falla del fluido eléctrico, terremoto, ataque a la infraestructura de TI) que interrumpe el curso normal de las operaciones de la organización.

Auditoría Interna

Instituto, vigilando la organización, funcionamiento y coordinación de todas sus dependencias y la observación de las leyes, reglamentos y resoluciones de la Junta Directiva, razón por la cual, se comunica lo determinado en el Plan de Continuidad del Negocio, con el propósito de que se tomen las acciones, se cuente con un instrumento actualizado, acorde con la normativa, y que el ICT esté preparado para minimizar los efectos ante una posible interrupción de actividades en los servicios críticos y se proteja la integridad de las personas, los bienes y equipos prioritarios de la institución.

Se solicita a ese Despacho, informar a esta Auditoría Interna dentro de los próximos diez días hábiles, sobre las acciones tomadas en relación con este servicio preventivo, a efecto de determinar lo procedente.

El presente servicio se realiza con fundamento en las competencias conferidas a la Auditoría Interna en la Ley Orgánica del ICT, artículos 33 y 35, la Ley General de Control Interno, artículo 22, inciso d), las “Normas para el Ejercicio de la Auditoría Interna en el Sector Público”, norma 1.1.4 y en atención del Plan Anual de Trabajo.

Atentamente,

FERNANDO JOSE RIVERA SOLANO (FIRMA)

Firmado digitalmente por FERNANDO JOSE RIVERA SOLANO (FIRMA)
Fecha: 2021.11.24 15:46:15 -06'00'

Fernando Rivera Solano
Auditor Interno

C. Consecutivo

FRS / kbm