Reporte de Investigación

Propuesta de un plan de continuidad del negocio para el registro del dominio de primer nivel de internet del Paraguay (NIC-PY)

Proposal of a business continuity plan for the registry of the internet first level domain of Paraguay (NIC-PY)

Revista sobre estudios e investigaciones del saber académico

Norma Elizabeth Sapper Danieli[1]
https://orcid.org/0000-0002-9493-7528
[1] Universidad Nacional de Asunción. Asunción, Paraguay. normasapper@gmail.com
Alberto Guzmán Capli Cabello[2]
https://orcid.org/0000-0002-9635-4377
[2] Universidad Nacional de Asunción. Asunción, Paraguay. acapli@cnc.una.py
Horacio Legal Ayala[3]
https://orcid.org/0000-0002-1790-2559
[3] Universidad Nacional de Asunción. Asunción, Paraguay. hlegal@pol.una.py

Resumen

El Plan de Continuidad del Negocio (BCP) es el conjunto de actividades previstas en una organización determinada, para poder responder a incidentes que puedan impactar en la gente, las operaciones y la capacidad de entregar bienes y servicios al mercado. Este Plan se vuelve de particular importancia para una entidad NIC, administradora y patrocinadora del dominio de primer nivel de internet de un país. Este trabajo se aboca en la propuesta de un BCP para el NIC-PY armonizando los criterios sugeridos por ICANN y COBIT 2019. El resultado es una grilla de tareas a incluir en el BCP del NIC-PY para la puesta en operación inmediata.

Palabras Claves: Continuidad del Negocio. Amenazas. Riesgos. Servicios. Procesos.

Abstract

The Business Continuity Plan (BCP) is the set of activities planned in a given an organization, to be able to respond to incidents that may impact people, operations and the ability to deliver goods and services to the market. This Plan becomes particularly important for a NIC entity, administrator and sponsor of a country's top-level Internet domain. This work focuses on the proposal of a BCP for the NIC-PY harmonizing the criteria suggested by ICANN and COBIT 2019. The result is a grid of tasks to include in the BCP of the NIC-PY for immediate start-up.

Keywords: Business Continuity. Threats. Risks. Services. Processes.

Área del conocimiento: Ingeniería y Arquitectura.
Correo de Correspondencia: normasapper@gmail.com
Conflictos de Interés: Los autores declaran no tener conflictos de intereses.

Fecha de recepción: 27/04/2022 Fecha de Aprobación: 12/11/2022
Página Web: http://publicciones.uni.edu.py/index.php/rseisa

Citación recomendada: Sapper Danieli, N. E.; Capli Cabello, A. G.; Legal Ayala, H. (2023). Propuesta de un Plan de Continuidad del Negocio para el Registro del Dominio de Primer Nivel de Internet del Paraguay (NIC-PY). Revista sobre estudios e investigaciones del saber académico (Encarnación), 17(17): e2023016

Introducción

Todas las organizaciones están expuestas a situaciones de riesgo y distintos tipos de amenazas, dependiendo del grado de vulnerabilidad en que se encuentran, la operativa puede ser afectada en menor o mayor grado. En caso de que ocurra un incidente y una amenaza se concrete, es donde un plan de continuidad representa un papel muy importante que permita a la organización, continuar con la operativa.

Los planes de continuidad del negocio (BCP, por sus siglas en inglés), desempeñan una función muy importante en las organizaciones, ya sean públicas o privadas, pequeñas, medianas o grandes. Si la organización no cuenta con un plan de continuidad, es probable que no pueda recuperarse ante una crisis de pérdida de datos o inaccesibilidad a los mismos, causados por factores internos como: recurso humano, tecnología e infraestructura, otros, y factores externos como: hackers, guerras/conflictos, hurto, vandalismos, entre otros.

Se puede decir que una amenaza es un elemento que aprovecha una vulnerabilidad para atacar o dañar a la organización. Las vulnerabilidades son las debilidades que contribuyen a que ocurra un evento desfavorable y dan paso a las amenazas. Las amenazas pueden clasificarse en distintas categorías: desastres naturales, recursos humanos, cibernética, financiero, externa, infraestructura y otros. La materialización de una amenaza genera riesgos que producen contratiempos y pérdidas totales o parciales en una empresa.

El NIC.PY no está exento de estas amenazas, por este motivo y teniendo en cuenta estos objetivos:

- Identificar los principales riesgos y amenazas que pueden interrumpir la continuidad del negocio.
- Evaluar los procesos y productos con su criticidad y el tiempo máximo de recuperación.
- Presentar un plan de continuidad basado en el marco de referencia COBIT 2019.

Se plantea una propuesta de un plan de continuidad del negocio basado en el marco de referencia de COBIT 2019 ajustada para el Registro del Dominio de Primer Nivel de Internet del Paraguay (NIC-PY).

Materiales y Métodos

El proyecto de Investigación se llevó a cabo en el departamento del NIC.py del Centro Nacional de Computación (CNC), que funciona en el campus de la Universidad Nacional de Asunción (UNA), ubicada sobre la Av. Mcal. López 3492 c/26 de febrero, San Lorenzo, Dpto. Central, Paraguay.

Fue utilizado el marco de referencia COBIT® desarrollado por ISACA. COBIT constituye una herramienta de implementación de componentes de gobierno y gestión para las empresas. Según información publicada por ISACA, las empresas que adoptaron el marco de referencia COBIT presentaron mejoras en su funcionamiento y en la elaboración BCP.

ISACA menciona que la correcta implementación de un gobierno empresarial de la información y la tecnología (GEIT) es casi imposible sin el uso de un marco de referencia de gobierno competente.

Fundamentalmente, el GEIT se ocupa de la creación de valor a partir de la transformación digital y la mitigación del riesgo de negocio derivado de dicha transformación. Específicamente, tras la adopción satisfactoria del GEIT se generan tres resultados principales [ISACA 2018]:

- **Obtención de beneficios.** La base fundamental del valor de la información y la tecnología (I&T, por sus siglas en inglés) consiste en ofrecer servicios y soluciones acertadas, a tiempo y dentro del presupuesto, que generen los beneficios financieros y no financieros esperados.
- **Optimización de riesgos.** Esto implica tener en cuenta el riesgo empresarial asociado al uso, propiedad, operación, involucramiento, influencia y adopción de I&T dentro de una empresa. El riesgo empresarial asociado a la información y la tecnología consiste en eventos relacionados con I&T que podrían llegar a tener un impacto en el negocio.
- **Optimización de recursos.** Asegura la dotación de una integrada, económica infraestructura de la Tecnología de la Información (TI), la introducción de nueva tecnología conforme lo requiera el negocio y la actualización o sustitución de sistemas obsoletos. Porque reconoce la importancia de las personas, además del hardware y software, se centra en proporcionar formación, fomentar la retención y garantizar la competencia del personal clave de TI.

COBIT 2019 está conformado por 5 dominios, estos dominios se dividen en 40 procesos, de los cuales 5 son de gobierno y el resto (35) son de gestión.

Fue utilizada la metodología de diseño descriptivo para seleccionar de estos 40 procesos 3 de ellos, cuyos componentes hacen referencia a prácticas relevantes para un BCP:

1. **EDM03 Asegurar la Optimización del Riesgo**: Asegurar que el apetito y la tolerancia al riesgo de la empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado [ISACA 2018].
2. **APO12 Gestionar el Riesgo**: Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa [ISACA 2018].
3. **DSS04 Gestionar la Continuidad:** 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 [ISACA 2018].

La motivación principal que impulsa este trabajo es tomar como base el Plan de Continuidad Comercial publicado por ICANN y adecuar a la guía de buenas prácticas, recomendadas por ISACA en el marco de referencia COBIT2019, para proponer un plan adecuado para el NIC.PY.

ICANN tiene participantes de todo el mundo dedicados a mantener una Internet segura, estable e interoperable. Forma parte de ICANN un Comité Permanente de Operaciones de Dominio de Nivel Superior (TLD-OPS) que llevó a cabo una serie de talleres de recuperación ante desastres y continuidad del negocio y elaboró una Guía para la implementación de continuidad comercial para operadores de DNS. Esta guía se encuentra disponible en la página https://ccnso.icann.org/en/announcements/announcement-17dec19-en.htm y se usará como modelo además de las buenas prácticas mencionadas en COBIT 2019, para la elaboración de esta propuesta.

Participantes

Participaron del relevamiento de la información requerida, la Dirección y un Analista Desarrollador del NIC.py, por el CNC, el Director de Proyectos TIC.

Resultados y Discusión

Se adecuó el Plan de Continuidad del ICANN al marco de referencia COBIT 2019, para ello, se deben realizar las siguientes prácticas:

- **Listado del personal y sus habilidades.**

Teniendo en cuenta las recomendaciones de COBIT, se debe conocer la lista de los cargos disponibles en la organización y cuáles son las habilidades de la persona que ejerce el cargo, teniendo esta información, a medida que se avanza con el plan, se podrá definir cuál sería el rol que desempeñaría dicha persona en caso que se tenga la necesidad de activar el BCP.

- **Inventario de todas las partes interesadas y sus expectativas.**

Los integrantes de una empresa tienen sus expectativas y sus exigencias establecidas, por esto se recomienda efectuar un inventario de todas las partes interesadas con sus expectativas y darle una prioridad a cada ítem, esta información servirá para construir una estrategia de continuidad del negocio eficaz, según las recomendaciones de ICANN.

- **Listado de proveedores.**

En toda organización existen dependencias externas para el suministro de servicios que muchas veces son indispensables y necesarias como por ejemplo la energía eléctrica.
Según menciona ICANN y COBIT, se recomienda contar con un listado de los proveedores, los servicios que ofrecen, la importancia de estos servicios y el impacto que podría tener en la operativa de la organización.

- **Listado de Productos o Servicios.**

COBIT recomienda listar todos los productos o servicios que brinda la organización, clasificar por criticidad, definir el/los responsables y el tiempo objetivo de recuperación (RTO, por sus siglas en inglés). El RTO se refiere al tiempo máximo que una organización define o puede esperar para recuperar o restaurar los procesos o servicios y que estén accesibles nuevamente ya sea para el cliente interno o externo.

- **Listado de los Procesos.**

COBIT recomienda listar todos los procesos existentes en la organización, clasificar por criticidad y definir el RTO.

- **Registro de amenazas y su probabilidad.**

Las amenazas son posibles eventos no deseados que si se materializan pueden ocasionar un impacto negativo en la organización, según lo recomendado por COBIT al evaluar las amenazas es importante estimar la probabilidad de ocurrencia del evento en función a datos estadísticos disponibles en la región o país.

En esta sección se debería proponer una lista exhaustiva de las amenazas que de alguna manera pueden afectar a la organización a corto, mediano o largo plazo, para esto se puede definir una escala de probabilidades en el que se define el periodo promedio la ocurrencia de acuerdo a datos históricos estadísticos.

- **Evaluación de amenazas potenciales.**

Las amenazas potenciales pueden producir un daño a la organización bajo una condición de vulnerabilidad, COBIT recomienda identificar las vulnerabilidades para determinar cuáles son las amenazas potenciales.

- **Identificar los riesgos**

El riesgo es la probabilidad de que se presente una consecuencia negativa debido a la materialización de una amenaza. Los riesgos pueden ser inaceptables o elevados por ello se recomienda identificarlos y clasificarlos, definir niveles de riesgo teniendo en cuenta el impacto económico, político, reputacional, legal, humano y legal. Se debe definir un registro de amenazas aplicando la evaluación del impacto en las operaciones de la organización según lo recomendado por ICANN y COBIT.

- **Definir los niveles de tolerancia al riesgo y el impacto de los riesgos sobre las operaciones.**

Se propone utilizar 5 niveles de tolerancia de riesgo que menciona la Corporación Internacional para la Asignación de Nombres y Números en Internet [ICANN] en su manual actual de recuperación de desastres: aceptar el riesgo, evitar el riesgo, reducir el riesgo, contener el riesgo y transferir el riesgo.

ICANN y COBIT recomiendan sugerir acciones para cada amenaza teniendo en cuenta los niveles de tolerancia y mencionar el impacto del riesgo sobre las operaciones de la organización.

- **Determinar los canales de comunicación y los responsables.**

Según recomendaciones de COBIT, es preciso establecer los canales de comunicación que serán los medios por el cual el responsable informará lo sucedido en caso que ocurra un incidente. Las comunicaciones pueden ser internas como externas en caso que afecte algún servicio que utilizan los clientes.

- **Definir el Plan de Continuidad del Negocio**

Una vez realizado el relevamiento de la información para cada una de las prácticas citadas arriba, se realiza la propuesta del plan de continuidad del negocio teniendo en cuenta las recomendaciones de COBIT, fue adaptada y mejorada la plantilla propuesta por [ICANN].

Se expone una breve explicación de cada uno de los ítems:

- **Escenario**: describe las condiciones que activaron el plan.
- **Proceso**: ¿afecta algún proceso?
- **Producto/Servicio**: ¿afecta algún producto o servicio?
- **Activación**: definir el momento en que se debería activar el plan.
- **Impacto**: que tan grave es el evento ocurrido.
- **RTO**: objetivo de tiempo de recuperación.
- **RPO**: objetivo de punto de recuperación.
- **Equipo de crisis**: ¿quién/es realmente se encargara/n del incidente?
- **Prioridad**: ¿Cuál es la prioridad?
- **Evaluación**: evaluar el grado del incidente, factores que deberían tenerse en cuenta.
- **Contención**: describir el curso de acción para prevenir un empeoramiento de la situación.
- **Recuperación/Acción**: describir el curso de acción para restaurar la preparación operativa.
- **Retiro**: una vez reestablecidas las operaciones, el equipo de crisis se retira y deja instrucciones.
- **Comunicación**: describir el comunicado y el medio de comunicación interna y externa.
- **Materiales vitales**: lista de recursos necesarios para gestionar el incidente.
- **Registros**: registrar el histórico de incidentes ocurridos.

Teniendo en cuenta cada ítem, a continuación un ejemplo de un Plan de continuidad para una de las amenazas identificadas:

Tabla 1.

Plan de continuidad del negocio (adaptado de [ICANN]).

Plan de Continuidad de Negocio			
Referencia:	BCP - 9.1.1	CIBERNÉTICA: DDOS	Servidores y usuario final
Escenario:	La respuesta de accesos a los servicios de dominio y/o portal WEB se encuentran mucho más lentos de lo normal y muchas peticiones son denegadas.		
Proceso:	Creación de nuevos dominios. Actualización de dominios.		
Producto/Servicio afectado:	Sistema de Administración de Dominios. Portal WEB.		
Activación:	Inmediatamente al momento de la detección.		
Impacto	Leve		
RTO:	Dentro de 24 hs.		
RPO:	Perdida de datos de un día hábil.		
Encargado del seguimiento de ejecución:	Dirección General. Dirección del NIC.		
Equipo de crisis:	Departamento de Soporte y Operaciones. Departamento de Mantenimiento Tecnológico. Área de Ciberseguridad externa al NIC.		
Prioridades:	Proteger la integridad y disponibilidad de los servicios. Recolectar evidencias. Determinar el alcance. Aislar los servidores afectados.		
Evaluación:	Identificar los componentes de la infraestructura afectada. Evaluar los archivos logs de servidores, ruteadores, firewalls, aplicaciones y cualquier otro recurso afectado. Evaluar la necesidad de contactar para solicitar ayuda al Equipo de Respuesta a Emergencias Cibernéticas. Identificar qué aspectos del tráfico del ataque DDoS se diferencia del tráfico normal.		
Contención:	Desconectar de la red externa los servidores afectados y aplicar configuraciones de firewalls si es necesario. Intentar bloquear el tráfico DDoS de la red. Actualizar antivirus de todos los equipos. Elevar niveles de seguridad en el firewalls. Si es necesario, ponerse en contacto con el proveedor de ISP para aplicar las medidas correctivas.		
Recuperación/Acción:	Asegurarse de que los servicios sean accesibles de nuevo. Asegurarse de que la accesibilidad a los servidores responda normalmente de nuevo. Reiniciar los servicios interrumpidos en el sitio principal.		
Retiro:	Una vez restaurados los servicios, el equipo de crisis se retira asignando un equipo que se encargará de los siguientes puntos: 1- Mantener el firewalls actualizado para reducir ataques. 2- Realizar la denuncia correspondiente al Equipo de Respuesta a Emergencias Cibernéticas. 3- Evaluar qué organización externa a la organización podría ayudar con este tipo de incidentes.		
Comunicación:	Comunicación interna: La Dirección del NIC a través del correo electrónico institucional, se encargará de poner en conocimiento de la situación y las medidas a ser adoptadas. Comunicación externa: La Dirección del NIC a través de la página institucional y las redes sociales, dará aviso a los clientes si el servicio de alta, modificación y consultas se encuentran con inconvenientes, finalmente dará nuevamente aviso cuando se reestablezca el servicio.		
Materiales vitales:	Inventario de infraestructura y configuraciones. Registro de contraseñas de los diferentes servicios.		
Registro:	Registrar en la tabla histórica de amenazas y referenciar.		

- **Registro histórico de amenazas y riesgos, Acciones tomadas**

En base a lo recomendado por COBIT, se propone la tabla 2, se utilizará para registrar los incidentes ocurridos, de esta manera se tendría fácil acceso a los datos de los eventos sucedidos y sirve como guía y experiencia en caso de necesidad.

Esta información se debería completar a medida que el plan de continuidad está siendo ejecutado:

Tabla 2.
Registro histórico de Amenazas y Riesgos.

Fecha	Vulnerabilidad	Amenaza	Riesgo	Acciones tomadas

Conclusión

Realizar un Plan de Continuidad del Negocio no es una tarea fácil, se requiere de un amplio conocimiento relacionado a las tareas, procesos y/o servicios que brinda la organización.

Fueron identificados los riesgos y las amenazas, fue analizada la estructura organizacional y las vulnerabilidades existentes y en base a estas fueron realizadas recomendaciones de mejora. Se realizó un estudio de la situación actual de la organización y se pudo determinar que se encuentra débil en cuanto a gestión de riesgo, ya que no cuenta con un procedimiento documentado que indique los pasos a seguir en casos de desastres.

Fueron evaluados los procesos y los productos para determinar su criticidad y el tiempo máximo de recuperación teniendo en cuenta como parámetro principal al cliente y la importancia que la disponibilidad de estos servicios puede tener para ellos.

Finalmente fue presentada una propuesta de BCP adecuada y adaptada al NIC.PY, asimismo fue agregada una propuesta de registro histórico de las amenazas y riesgos que ayudará a tener disponible la información para la utilización en caso de necesidad y también servirá como experiencia. Para llegar a esto, fue realizado un relevamiento de la información necesaria, y se tuvo en cuenta las recomendaciones de la guía de buenas prácticas de COBIT2019 y la guía de implementación de un plan de continuidad comercial publicada por ICANN.

La propuesta presentada para un BCP cumple con 100% de las recomendaciones de ICANN así como también 100% de las prácticas recomendadas por COBIT 2019 en los aspectos relativos a plan de contingencias.

Estar preparados para responder ante una eventualidad, es el factor complementario crítico que puede determinar el éxito o fracaso de cualquier organización.

Referencias Bibliográficas

Bautista, M. (2014). *Marco de Referencia para la Formulación de un Plan de Continuidad de Negocio para TI, un caso de estudio.* Obtenido de Revista Técnica «Energía», 10(1): https://doi.org/10.37116/revistaenergia.v10.n1.2014.116

Bevan, T. (2019). *ISO 22301:2019 Guía de Implementación de la Continuidad del Negocio.* Obtenido de NQA UK Auditor: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-22301-Guia-de-implantacion.pdf

Elliot, D., Swartz, E., & Herbane, B. (2010). *Business Continuity Management: A Crisis Management Approach (2nd ed.).* Nueva York, EE.UU.: Routledge.

Ferrer, R. (2013). *Metodología para la Gestión de la Continuidad del Negocio.* Obtenido de https://cintel.co/wp-content/uploads/2013/05/Metodolog%C3%ADa-para-la-Gesti%C3%B3n-de-la-Continuidad-del-Negocio.pdf

Gomes, P., Cadete, G., & Mira Da Silva, M. (2017). Using Enterprise Architecture to Assist Business Continuity Planning in Large Public Organizations. *IEEE 19th Conference on Business Informatics (CBI)*, 1-10. Obtenido de https://doi.org/10.1109/cbi.2017.30

ICANN. (2019). *Business continuity implementation guidance to small ccTLD operators: .* Obtenido de Country Code Names Supporting Organisation. (s. f.).: https://ccnso.icann.org/en/announcements/announcement-17dec19-en.htm

ISACA¹. (2018). *COBIT 2019, Implementación y optimización de una solución de gobierno de información y tecnología.* Schaumburg, IL, EE.UU.

ISACA[2]. (2018). *COBIT 2019, Diseño de una solución de gobierno de Información y Tecnología.* Schaumburg, IL, EE.UU.

ISACA[3]. (2018). *COBIT 2019, Introducción y Metodología.* Schaumburg, IL, EE.UU. .

ISACA[4]. (2018). *COBIT 2019, Objetivos de gobierno y gestión.* Schaumburg, IL, EE.UU. .

ISO/TC 292. (2019). *ISO 22301:2019 Seguridad y resiliencia - Sistemas de gestión de la continuidad del negocio – Requisitos.* Obtenido de https://www.isotc292online.org/

KPMG. (2016). 2016 Global BCM Program Benchmarking Study. *KPMG LLP y Continuity Insights*. Obtenido de https://home.kpmg/kz/en/home/media/press-releases/2016/09/program-benchmarking-study.html

Mansoori, B., Rosipko, B., Erhard, K., & Sunshine, J. (2013). Design and Implementation of Disaster Recovery and Business Continuity Solution for Radiology PACS. *Journal of Digital Imaging 27(1)*, 19–25. Obtenido de https://doi.org/10.1007/s10278-013-9625-4

Saavedra, L. (2013). *NCh-ISO 22301–2013-044.* Obtenido de https://es.scribd.com/document/405785850/3-NCh-ISO-22301-2013-044-pdf