EasyChair Preprint

№ 10955

Testing of a Business Continuity and Contingency Plan for Edge Device Failure.

Ibrahin Piñero Pérez and Guillermo Brito Acuña

September 23, 2023

//UCIENCIA/23
CONVENCIÓN CIENTÍFICA INTERNACIONAL

Temática: III Taller Internacional de Ciberseguridad

Prueba de un plan de contingencia y continuidad de negocio para fallo de dispositivo de borde.

Testing of a business continuity and contingency plan for edge device failure.

Ibrahin Piñero Perez [1], **Guillermo Brito Acuña** [2]

[1] Empresa Cubana de Navegación Aérea. UEB Navegación Aérea Camagüey.ibrahin.pinero@cmw.aeronav.avianet.cu
[2] Empresa Cubana de Navegación Aérea. Nivel Central. guillermo.brito@aeronav.avianet.cu

---

Resumen

Un plan de contingencia y continuidad del negocio es un documento que contiene procedimientos y responsabilidades para la recuperación de un sistema teniendo en cuenta el análisis de las necesidades, impactos y riesgos de una organización. El objetivo de este trabajo fue comprobar un plan de contingencia y continuidad del negocio ante fallo de dispositivo de borde de red, mediante un programa de prueba, entrenamiento y ejercicio aplicado al personal de la entidad, para validar la planificación de la contingencia e identificar aspectos de mejora del plan. Se empleó un estudio no experimental, aplicado de forma transversal, con alcance descriptivo y con un enfoque cuantitativo. Para el estudio se obtuvo una muestra no probabilística por conveniencia y se utilizaron como técnica recolección de datos la observación, de tipo participativa y estructurada. Como instrumento se diseñaron 2 listas de cotejo con escala dicotómica para evaluar la planificación de la contingencia y las características del dispositivo de borde de red. Como resultado de la investigación se obtuvo la conformidad en la mayoría de los indicadores y categorías evaluadas, existiendo no conformidades en las categorías de Redundancia y Disponibilidad del dispositivo de borde. Como conclusión se comprobó que es buena la identificación y documentación de los aspectos de la planificación de las contingencias contenidos en el plan, pero es necesario mejorar por parte de prestador de servicios de conectividad las características de redundancia del dispositivo de borde de red para poder cumplir con los tiempos de recuperación establecidos por la entidad.

Palabras clave: plan, contingencia, continuidad, dispositivo de borde, redundancia.

Abstract

A contingency and business continuity plan is a document that contains procedures and responsibilities for the recovery of a system taking into account the analysis of the needs, impacts and risks of an organization. The objective of this work was to verify a contingency and business continuity plan in the event of a network edge device failure, through a test, training and exercise program applied to the entity's personnel, to validate the contingency planning and identify aspects plan improvement. A non-experimental study was used, applied cross-sectionally, with a descriptive scope and a quantitative approach. For the study, a non-probabilistic sample was obtained for convenience and observation, participatory and structured, were used as the data collection technique. As an instrument, 2 checklists with a dichotomous scale were designed to evaluate contingency planning and the characteristics of the network edge device. As a result of the investigation, compliance was obtained in most of the indicators and categories evaluated, with non-conformities in the Redundancy and Availability categories of the network edge device. In conclusion, it was verified that the identification and documentation of the aspects of contingency planning

contained in the plan is good, but it is necessary to improve by the connectivity service provider the redundancy characteristics of the network edge device in order to comply with the recovery times established by the entity.

Keywords: *plan, contingency, continuity, edge device, redundancy.*

Introducción

Cualquier organización o entidad está expuesta a incidentes que pueden provocar una parada de su actividad y ser un obstáculo para la continuidad de su negocio. Un plan de contingencia es un documento que proporciona procedimientos y responsabilidades para recuperar un sistema planificando actividades antes, durante y después de una eventualidad grave. Puede activarse independientemente de otros planes o como parte de un esfuerzo de recuperación mayor coordinado con un plan de recuperación y desastres (DRP), plan de continuidad de las operaciones (COOP) y/o plan de continuidad del negocio (BCP). (National Institute of Standards and Technology (NIST), 2010)

Los planes de contingencias son una parte de los planes de continuidad del negocio donde se establecen las respuestas o tratamiento de las incidencias teniendo en cuenta el análisis de las necesidades y los riesgos de una organización para la respuesta a incidentes y la recuperación ante desastres. (Organización Internacional de Normalización (ISO), 2013) La continuidad del negocio es la capacidad de una organización de continuar entregando sus productos o servicios a niveles aceptables previamente establecidos para que cuando producto de una interrupción el elemento primario falle, el alterno esté disponible. Es la disciplina clave que permite crear y mejorar la resiliencia de las organizaciones para absorber, adaptarse y dar respuesta a cualquier cambio progresivo o súbito. (Rodríguez-Rojas, 2021)

El análisis de impacto del negocio (BIA) como proceso de la continuidad del negocio permite caracterizar los componentes del sistema, los procesos, los recursos y sus interdependencias. Su propósito es correlacionar el sistema con la misión crítica, los procesos comerciales y los servicios proporcionados y, en base a esa información, caracterizar las consecuencias de una interrupción. Los resultados de BIA son necesarios para determinar los requisitos y prioridades de la planificación de la contingencia y para el desarrollo de las estrategias de recuperación ante situaciones de crisis. (NIST, 2010) La gestión de los riesgos permite identificar, controlar y mitigar los riesgos de un sistema de información durante el ciclo de vida del desarrollo del sistema. En el desarrollo de un plan de contingencias y continuidad del negocio la implementación de un marco de gestión de riesgos permite prevenir o reducir la probabilidad de amenazas naturales, humanas y ambientales y limitar las consecuencias de los riesgos antes de una interrupción del sistema. (NIST, 2018)

El plan de contingencia y continuidad del negocio, no es operativo hasta que no ha sido sometido a una prueba. No es necesario esperar a que ocurra un incidente real para evaluar si contamos con una respuesta confiable, antes de ese momento, se deberá probar, evaluar y actualizar periódicamente para tener al personal capacitado según sus funciones

y responsabilidades; disponer de acciones ejercitadas y validadas; y contar con sistemas y sus componentes probados para garantizar su operatividad. (NIST, 2006)

A través de la revisión bibliográfica fueron analizadas las investigaciones y aplicaciones realizadas por otros autores de las distintas normas y estándares existentes relacionados con el objeto de estudio. La implementación de un modelo u otro depende de la capacidad, nivel de madurez, tamaño y la existencia de recursos necesarios para la planificación y el desarrollo del plan. Se pueden implementar diferentes modelos de manera complementaria acorde a las necesidades existentes. (Becerra, Benavides, Camacho, & Obando, 2021) Se decide emplear para el cumplimiento del requisito establecido en el Anexo 17: Seguridad de la Información en la Gestión de la Continuidad del Negocio, de la norma ISO/IEC 27001 de 2013: Sistema de Gestión de Seguridad de la Información, el marco de trabajo de Ciberseguridad NIST, serie 800 y sus publicaciones especiales NIST SP 800-84 y NIST SP 800-34 Rev1. Se tendrán en cuentas otras métricas para la evaluación de la continuidad del negocio, análisis de impacto, confiabilidad, disponibilidad y mantenibilidad. Además, a través del presente trabajo se aportarán las evidencias necesarias para el cumplimento de las capacidades definidas en los objetivos de: Planificación de la respuesta, Mitigación y Planificación de la recuperación definidas en el modelo de Madurez de Ciberseguridad Aeronáutica aplicado en la entidad, en su etapa C Gestionada. (Brito-Acuña, 2023)

Como antecedente a la investigación, como se muestra en la Figura 1 el Aeropuerto Internacional Ignacio Agramonte y Loynaz, de Camagüey contaba con un dispositivo de borde de red ubicado en la Terminal Nacional como único enlace a las redes de transporte y datos del prestador del servicio de conectividad del municipio de Camagüey para todas las redes de las entidades de la Aviación Civil de Cuba que radican en el aeropuerto.

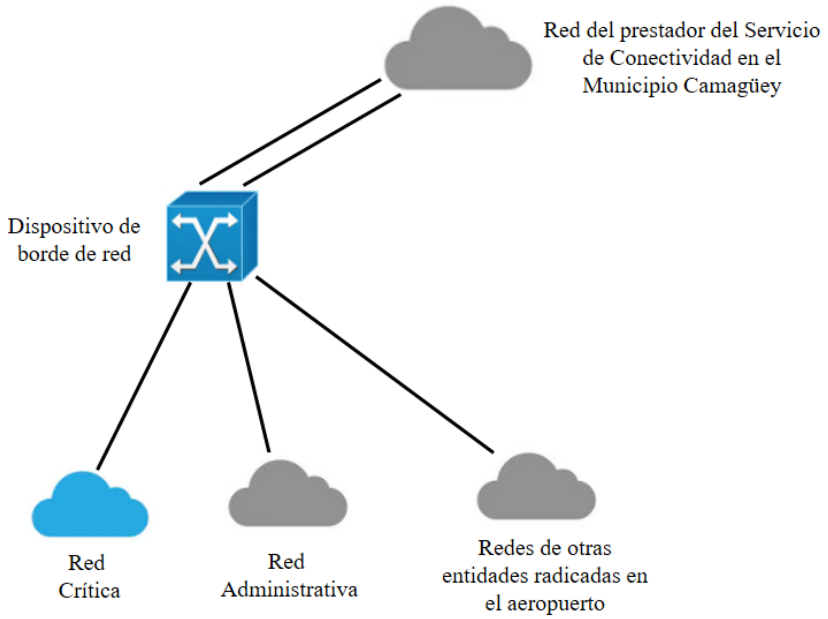

Figura 1: Esquema lógico de la red del aeropuerto.

La UEB Navegación Aérea Camagüey perteneciente a la Empresa Cubana de Navegación Aérea (ECNA, SA) cuenta con una red crítica que da soporte a los servicios de navegación aérea tales como: control del tránsito aéreo de aeródromo y área (ATS); comunicación, navegación y vigilancia (CNS) e información aeronáutica y meteorológica (AIS-MET). Entre los procesos críticos que se vieran afectados con una falla de este dispositivo se encuentran: el envío y recepción de información radar, la telefonía en función del tránsito aéreo, él envió y recepción de mensajería aeronáutica, el monitoreo de la estación VHF ubicada en Florida, y la consulta del banco de datos meteorológicos. Además, este dispositivo brinda soporte a otros servicios no críticos de la UEB y otras entidades del aeropuerto como son: correo electrónico, intranet, internet, videoconferencia, entre otros.

Aunque se disponía de un plan de contingencia para garantizar la continuidad de las operaciones ante una falla de este dispositivo, existían carencias en la documentación del mismo y no existían evidencias de la realización de pruebas, ejercicios y/o entrenamiento al personal de la entidad que validaran las acciones de contingencias descritas en este plan, lo que podría afectar la respuesta para la continuidad de los servicios críticos prestados por la entidad, conduciendo a cuantiosas pérdidas económicas, aumento del estrés de los controladores de tránsito aéreo en turno, limitaciones en el uso del espacio aéreo cubano y así como otras afectaciones morales, a la imagen y reputación de la empresa como proveedores de Servicios de Navegación Aérea.

Por todo lo antes expuesto se propone como objetivo de investigación, comprobar un plan de contingencia y continuidad del negocio ante fallo de dispositivo de borde del prestador del servicio de conectividad, mediante un programa de prueba, entrenamiento y ejercicio aplicado al personal de la UEB, para validar la planificación de las contingencias e identificar aspectos de mejora del plan.

Métodos y técnicas empleadas

Para la elaboración del presente artículo se empleó un diseño no experimental en el cual no se realiza la manipulación deliberada de las variables y sólo se observa el fenómeno en su ambiente natural para después analizarlo. Fue aplicado de manera transversal recolectando los datos en un sólo momento para evaluar una situación, evento, fenómeno o contexto en un punto del tiempo. (Hernández, Fernández, & Baptista, 2014)

Considerando que el tema de investigación tuvo sustento teórico suficiente, se procedió a realizar una investigación con alcance descriptivo donde se mide o recoge información de manera independiente o conjunta sobre los conceptos o las variables a las que se refieren y su objetivo no es indicar cómo se relacionan éstas. (Hernández, Fernández, & Baptista, 2014) Teniendo en cuenta las características y necesidades de investigación se trabajó con un enfoque cuantitativo donde el conocimiento debe ser objetivo, y se genera a partir de un proceso deductivo donde a través de la medicación numérica y el análisis estadístico inferencial se prueban las hipótesis previamente formuladas. (Hernández, Fernández, & Baptista, 2014)

La población de estudio como un conjunto finito o infinito de elementos con características comunes para las cuales serán extensivas las conclusiones de la investigación, (Arias, 2012) fue de 50 personas que laboran en la entidad y otros técnicos y especialistas del prestador del servicio de conectividad contratado. Para la selección de la muestra como una parte o el subconjunto de la población que poseen las mismas características y se reproducen de la manera más exacta posible, (Arias, 2012) se obtuvo a partir de un muestreo no probabilístico dado que no puede calcularse mediante la probabilidad y, por lo tanto, no requiere de operaciones estadísticas ni tampoco se pueden generalizar los resultados que se deriven de ella. (Hernández, Fernández, & Baptista, 2014) Se les solicitó a los trabajadores de la entidad y otros especialistas seleccionados del prestador del servicio de conectividad que formaran parte de la investigación. El tamaño de la muestra fue determinado por conveniencia permitiendo elegir de manera arbitraria cuántos participantes puede haber en el estudio. El tipo de muestra fue de expertos logrando reunir a los especialistas de los distintos procesos que son afectados por la contingencia. (Hernández O., 2021)

La técnica de recolección de datos seleccionada fue la observación la cual consiste en el registro sistemático, válido y confiable de comportamientos y situaciones observables, a través de un conjunto de categorías y subcategorías. Por sus características se clasificó como participante ya que el investigador se integra al grupo investigado como uno más de ellos y estructurada porque contiene aspectos muy puntuales a observar. Como instrumento de recolección de datos se empleó la lista de cotejo o de verificación para estimar la presencia o ausencia de características o atributos relevantes en la planificación y ejecución del plan de contingencia. (Hernández, Fernández, & Baptista, 2014) Las listas de verificación fueron diseñadas con una escala de valoración dicotómica (Conforme o No Conforme) y se asignó un identificativo a cada indicador (ítem) según la categoría (dimensión) a la que pertenece para su representación univoca. Las listas de verificación descritas en las tablas: Tabla 1 y Tabla 2 fueron elaboradas a partir del instrumento antes mencionados y formaron parte de los eventos de prueba del programa de TT&E diseñado.

Los puntajes correspondientes a los valores de respuesta de las listas de cotejo se analizaron con respecto a cada categoría y de forma general. Para la validez de los datos a evaluar fueron seleccionados las categorías e indicadores teniendo en cuenta los requisitos de NIST 800-34 rev1 para la planificación de las contingencias y otras métricas seleccionadas. Para confiabilidad de los datos se realizó una prueba piloto para comprobar que los resultados obtenidos estaban con correspondencia con los investigados.

La técnica que se empleó para el procesamiento de los datos fue la estadística descriptiva como rama de la estadística que formula recomendaciones de cómo resumir, de forma clara y sencilla, los datos de una investigación en cuadros, tablas, figuras o gráficos. (Rendón-Macías, Villasís-Keeve, & Miranda-Novales, 2013) permitiendo el análisis e interpretación de los resultados según las categorías e indicadores evaluados a través de las listas de verificación diseñadas. La herramienta empleada para el procesamiento de los datos fue el software Excel de Microsoft Office.

Programa de TT&E

El programa de prueba, entrenamiento y ejercicio (TT&E por sus siglas en inglés) diseñado incluyó 2 pruebas escritas a través del instrumento de recolección de datos seleccionado, estos eventos fueron diseñados teniendo en cuenta las 4 fases descritas por NIST 800-84 y para su cumplimiento se establecen los roles de: Coordinador del plan, el cual tiene la responsabilidad del desarrollo, implementación y mantenimiento de los planes; y el Coordinador del programa TT&E, quien es responsable de desarrollar el plan TT&E y coordinar los eventos.

Antes de cada evento se realiza una capacitación para informar al personal sobre la realización del evento y son brindados los conocimientos necesarios para participar en las pruebas a desarrollar: como son los objetivos, materiales, formulas, herramientas y el plan descrito. (NIST, 2006) Para el diseño del evento a desarrollar se deberá analizar la necesidad, el tema a abordar, el alcance, los objetivos, los participantes y la logística necesaria. Luego de ser elaborados los materiales a desarrollar durante el evento, se deberá contar con la aprobación de la dirección de la entidad para su realización. De cada una de las pruebas son registrados los siguientes datos: nombre de la prueba, objetivo de prueba, fecha de ejecución, evaluadores y participantes. Posterior al desarrollo cada evento se realiza un informe sobre el cumplimiento de los criterios de evaluación pre-definidos a partir de los objetivos trazados y es discutido con la dirección. A continuación, se describen las dos listas de verificación elaboradas.

Tabla 1. Lista de verificación para la comprobación de las características del dispositivo de borde de red

Id	Indicadores a evaluar	Escala		Observación cuantitativa
		C	NC	
Categoría: Mantenibilidad				
MA1	Se conoce el tiempo de uso del dispositivo.			
MA2	Es monitoreado su funcionamiento.			
MA3	Ha tenido interrupciones del servicio.			
MA4	Se le han realizado mantenimientos preventivos/correctivos.			
Categoría: Redundancia				
RE1	Dispone de características de redundancia internas (fuente de alimentación, controlador, fan, etc.) .			
RE2	Dispone de respaldo eléctrico (UPS, Banco de Baterías, G.E.).			
RE3	Dispone de una salva de su configuración.			
RE4	Dispone de medios de respaldo para su sustitución.			
RE5	Cuenta con más de un enlace externo.			
Categoría: Disponibilidad				
DI1	Se conoce el Tiempo Medio a la Falla (MTTF).			
DI2	Se conoce el Tiempo Medio de Recuperación (MTTR).			
DI3	Se conoce del Tiempo Medio entre Falla (MTBF).			

DI4	Conoce la Disponibilidad del dispositivo.			
DI5	Conoce la Confiabilidad del dispositivo.			
DI6	Existen medidas encaminadas a mejorar su disponibilidad y confiabilidad.			
Categoría: Proveedores				
PR1	Existen Acuerdos de Niveles de Servicio (SLA).			
PR2	Existen Acuerdos de Niveles Operativos (OLA) que apoyen al SLA.			
PR3	Se cumplen los niveles de servicios acordados.			
PR4	Son identificados y tratados asuntos para el Plan de Mejoras al Servicio (SIP).			

Tabla 2. Lista de verificación para la comprobación de la planificación de la contingencia

Id	Indicadores a evaluar	Escala		Observación cuantitativa
		C	NC	
Categoría: Políticas de planificación de contingencias				
PO1	Están identificados los requisitos legales o reglamentarios.			
PO2	Existe una política para la planificación de la contingencia.			
PO3	Existe respaldo económico para el cumplimiento de esta política.			
PO4	El personal conoce lo establecido en la políticas.			
Categoría: Análisis Impacto de Negocio				
AI1	Están identificado los procesos críticos afectados.			
AI2	Están evaluados los tipo de impactos para cada uno de estos procesos.			
AI3	Está determinado el Tiempo de Inactividad Máximo Tolerable (MTD).			
AI4	Está determinado el Tiempo Objetivo de Recuperación (RTO).			
AI5	Está determinado el Tiempo Punto Objetivo de Recuperación (RPO).			
AI6	Están identificados los recursos necesarios para la recuperación.			
AI7	Existen estrategias de recuperación.			
AI8	Se consideras sitios alternos para la recuperación.			
Categoría: Análisis de riesgos				
AR1	Están identificados los recursos por niveles de criticidad.			
AR2	Están identificados los amenazas que pudieran afectar estos recursos.			
AR3	Están evaluados los riesgos a partir de las amenazas según probabilidad ocurrencia y los niveles de impacto, riesgo y tolerancia.			
AR4	Existe tratamientos para los riesgos de mayor impacto donde se establece su estrategia, las acciones y responsables.			
AR5	Existe tratamientos para los riesgos residuales.			
AR6	Existen controles preventivos según riesgos.			

Categoría: Plan de contingencia				
PC1	Están determinados los posibles escenarios de contingencia.			
PC2	Existen acciones en las 3 fases: antes (Activación y Notificación) durante (Recuperación) y después (Reconstitución) del evento disruptivo.			
PC3	Se han desarrollado manuales y procedimientos para cada escenario de desastre identificado.			
PC4	Se han determinados las estrategias de contingencias ante los posibles escenarios.			
PC5	Están identificados los recursos necesarios para cada escenario.			
PC6	Se han definido los roles, responsabilidades y suplentes.			
PC7	Están descritos los números de contacto (actualizados) del personal con responsabilidad.			
Categoría: Pruebas y mantenimiento del plan				
PM1	Se realizan capacitaciones al personal sobre el plan de contingencia y continuidad de Negocio.			
PM2	Se realizan pruebas, ejercicios, entrenamientos del plan de contingencia y continuidad de negocio.			
PM3	Se identifican aspectos de mejora durante las comprobaciones.			
PM4	Se documentan los cambios y se generalizan los resultados.			

Resultados y discusión

Para el desarrollo de la primera prueba elaborada a través de la Tabla 1 intervinieron como evaluador: el Especialista de Ciberseguridad y como participantes: el Especialista Principal del Proceso 7 Soporte Tecnológico, el Administrador de Red y el Técnico de Guardia. Como personal externo a la entidad participó un Técnico y 2 Especialistas pertenecientes al prestador del servicio de conectividad, para un total de 7 participantes. De un total de 19 indicadores a evaluar, fueron conformes: 12 y no conformes: 7, para un 63 % de conformidad, considerándose como un resultado no conforme ya que se registran incumplimientos en la mayoría de las categorías evaluadas.

En la categoría Mantenibilidad todos los indicadores obtuvieron resultados conformes evidenciándose un monitoreo y control del dispositivo por parte del proveedor del Servicio de Conectividad y siendo un elemento positivo para el plan evaluado, indicadores [del MA1 a MA4] de la Tabla 1. Como indicadores no conformes dentro de la categoría de Redundancia se encuentran: [RE1] ya que el dispositivo no cuenta con componentes internos de respaldo, [RE4] no se dispone de otro dispositivo alterno que pueda ser sustituido para en caso de fallo del principal y [RE5] sólo se dispone de una vía de comunicación hacia la red de prestador del servicio de conectividad en el municipio de Camagüey. Positivamente para el plan se dispone de un banco de batería como respaldo eléctrico del dispositivo de borde de red [RE2] y se cuenta con la salva de su configuración [RE3].

Sobre la categoría Disponibilidad no se pudo obtener el valor del indicador MTBR del dispositivo, pero se estima que es elevado según el fabricante y modelo de dispositivo. Para el cálculo y análisis realizado a través de la fórmula de la disponibilidad inherente (Hincapie, 2017) se estimó el MTTR [DI2] en 24 horas considerando un MTBR [DI3] de 1800 horas (30 días), para que no sea afectada la eficacia mensual del proceso de Soporte Tecnológico de la entidad, el indicador de la disponibilidad [DI4] debe ser menor o igual a 99% para los sistemas críticos. No se pudo definir el MTTF [DI1] dado que no existían registros de interrupciones previas. Impactando de forma negativa en el tiempo de recuperación establecido fueron consideradas otras actividades que se representan en la Figura 2 como: traslado al aeropuerto de los especialistas, ubicación y diagnóstico de la falla, localización y espera de los materiales de repuesto, reemplazo de los componentes dañados reinicio y reconfiguración; y otros chequeos funcionales.

Para el análisis de la confiabilidad [DI5] teniendo en consideración el MTBR estimado, se calcula como la probabilidad de que uno u otro de los componentes internos falle (fuente de alimentación, controlador y fan), obteniéndose una mayor confiabilidad si el dispositivo tuviera redundancia a nivel componentes. (Hincapie, 2017) En la categoría Proveedores sólo se señala que, aunque existen Acuerdos de Niveles de Servicio (SLA) y Acuerdos de Niveles Operativos (OLA) que lo complementen, no habían sido identificados y tratados asuntos para el Plan de Mejoras al Servicio (SIP) para lograr sus cumplimientos [PR4].

Para el desarrollo de la segunda prueba, a través de la Tabla 2 participó como evaluador el Especialista de Ciberseguridad Aeronáutica y como participantes los especialistas principales de los procesos: Soporte Tecnológico, Tránsito Aéreo, AIS-MET, el Administrador de Red, 2 Ingenieros en Sistema de Radionavegación y Comunicación Aeronáutica, un Técnico de Guardia para un total de 8 participantes los cuales fueron consultados para evaluar la documentación de la planificación de la contingencia. De un total de 29 indicadores a evaluar, fueron conformes: 24 y no conformes: 5 para un 83 % de cumplimiento considerándose como un resultado conforme ya que se encuentran identificados y documentados los principales aspectos requeridos para la planificación de las contingencias.

En la categoría Políticas de planificación de contingencias se evidencia la conformidad de todos sus indicadores destacándose la declaración de políticas para la planificación de las contingencias tanto a nivel de empresa a través de un Reglamento de Ciberseguridad, Reglamento de Seguridad Operacional, Fichas de Proceso y a nivel de entidad a través de los Planes de Seguridad Informática elaborados, indicadores [de PO1 a PO4] de la Tabla 2. En la categoría Análisis Impacto de Negocio los resultados fueron conformes y se calificó este fallo como un impacto grave para la entidad. Se evidenció la identificación de los procesos críticos declarados en la problemática, los recursos necesarios para la contingencia y la estrategia de recuperación [AI1, AI6 y AI7].

Como se representa en la Figura 2 el RPO [AI5] fue definido en 0 ya que los servicios afectados son ininterrumpidos y no pueden ser restaurados a través de copias de seguridad. El MTD [AI3] fue establecido en 24 horas en

correspondencia con el MTTR antes analizado y el RTO [AI3] fue de 21 horas considerando las actividades de recuperación antes mencionadas. Los indicadores no conformes dentro de esta categoría fueron: [AI2] ya que no fueron valorados, ni documentado los impactos (financiero, moral, legal, etc.) a consecuencia de la interrupción de los servicios críticos afectados; y [AI9] porque no se dispone de un sitio alternativo para la recuperación.

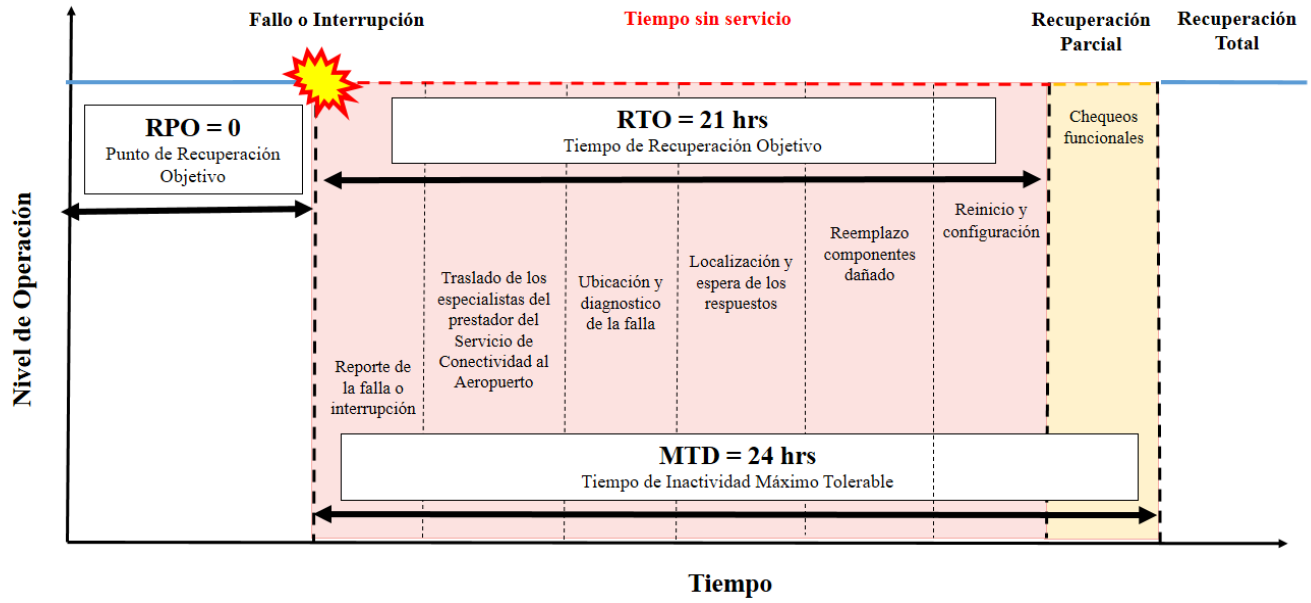

Figura 2. Diagrama de tiempo y nivel de operación del plan elaborado.

En las categorías Análisis de riesgos y Plan de contingencia todos sus indicadores fueron conformes apreciándose una buena identificación, evaluación y tratamiento del riesgo de fallo del dispositivo, clasificándose con un índice de Tolerable (2B) según su severidad y probabilidad [de AR1 a AR6]. Se observó la documentación de las acciones por etapas para los 4 escenarios identificados en el plan en caso de fallos de: fuente interna, controladora, módulo de tarjeta de red y enlaces de fibra óptica; y las responsabilidades del personal técnico y directivos de la entidad según el radio de acción [de PC1 a PC6]. Se evidenció el registro y actualización de los contactos para la notificación y reporte [PC7]. En la categoría Pruebas y mantenimiento del plan fueron no conformes los indicadores [PM2, PM3 y PM4] dado que anterior a esta investigación no se habían realizado pruebas o ejercicios del plan, no se habían identificado posibles mejoras y no se habían documentados los cambios realizados respectivamente.

La implementación de los marcos de trabajo seleccionados estuvo en correspondencia con las características y necesidades de la entidad para una etapa inicial en la comprobación de los planes de contingencia. El análisis y determinación de las métricas relacionadas con el tiempo de inactividad dentro del Análisis de Impacto de Negocio, permiten a la dirección de la entidad una correcta selección de los métodos, procedimientos y tecnologías de recuperación. En caso de no contar con los recursos necesarios, determina el plan de acción para el cumplimiento de estos tiempos definidos en correspondencia con la clasificación del impacto. Coincidiendo con los autores de NIST 800-34, mientras mayor sea el RTO, más costosa será la interrupción, por lo que cada entidad u organización deberá

lograr un equilibrio entre el costo de recuperación y el costo de interrupción según sus características y necesidades. En este sentido para un impacto grave y un RTO definido de 21 horas las estrategias y recursos de recuperación deberán estar en correspondencia con este indicador, afectando este tiempo de recuperación se encuentran las deficientes características de redundancia del dispositivo de borde de red y la localización y espera de los equipos o componentes de repuesto en caso necesitar sustitución.

Conclusiones

Mediante el desarrollo de este trabajo se comprobó que:

El Análisis de Impacto de Negocio y Análisis de Riesgos son procesos fundamentales en la comprobación de la contingencia y continuidad del negocio permite la identificación de las posibles afectaciones y consecuencias del incidente teniendo en cuenta factores financieros, reputación, aspectos legales y regulatorios; son determinados los tiempos de recuperación; y son gestionados proactivamente las amenazas humanas, tecnológicas y ambientales que pudieran provocar la disrupción.

La implementación del programa TT&E diseñado constituye una herramienta eficaz en la comprobación del plan, se mantiene preparado el personal en cuanto a sus funciones y responsabilidades, son validados las estrategias y recursos de recuperación definidos y permite la mejora continua del plan elaborado.

Se puede validar que existe una buena identificación y documentación de los procesos requeridos para la planificación de la contingencia, el personal de la entidad está preparado en sus funciones dentro del plan, pero son deficientes las características de redundancia y disponibilidad del dispositivo de borde de red haciendo imposible el cumplimiento de los tiempos de recuperación establecidos, por lo que será necesario solicitar al prestador del servicio de conectividad mejorar las características de redundancia en los componentes del dispositivo de borde de red, equipos de respaldo y enlaces alternos.

Se recomienda diseñar otros eventos de comprobación como simulacros, pruebas funcionales, etc. que permitan evaluar otros aspectos del plan u otro evaluado; disponer de un sitio alternativo para el envío y recepción de la información de las entidades del aeropuerto en un esfuerzo mayor de recuperación; y emplear las listas de verificación desarrolladas como parte de los controles de Ciberseguridad que se realizan en la entidad.

Referencias

Arias, F. G. (2012). *El Proyecto de Investigación: Introducción a la metodología científica* (6 ed.). Episteme.

Becerra, R., Benavides, J. R., Camacho, H., & Obando, C. J. (2021). Evolución y modelos de implementación de sistemas de gestión de continuidad del negocio. *SIGNOS Investigación en Sistemas de Gestión, 13*(2). doi:https://doi.org/10.15332/24631140.6669

Brito-Acuña, G. (2023). Madurez en ciberseguridad aeronáutica: un marco de trabajo. *DYNA, 90*(227). doi:https://doi.org/10.15446/dyna.v90n227.107420

Hernández, O. (2021). Aproximación a los distintos tipos de muestreo no probabilístico que existen. *Revista Cubana de Medicina General Integral, 37*(3), 2.

Hernández, R., Fernández, C., & Baptista, M. d. (2014). *Metodologia de la Investigación* (6 ed.). McGRAW-HILL.

Hincapie, L. (2017). Metodología de gestión de mantenimiento desde una perspectiva de Confiabilidad-Disponibilidad-Mantenibilidad (CDM) para aplicación en equipos de Tecnología de la Información (TI). Obtenido de https://repositorio.unal.edu.co/handle/unal/62279

National Institute of Standards and Technology (NIST). (2006). *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities* (Special Publication 800-84 ed.). Obtenido de https://csrc.nist.gov/publications/detail/sp/800-84/final

National Institute of Standards and Technology (NIST). (2010). *Contingency Planning Guide for Federal Information Systems* (Special Publication 800-34 Rev. 1 ed.). Obtenido de https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final

National Institute of Standards and Technology (NIST). (2018). *Risk Management Framework for Information Systems and Organizations* (Special Publication 800-37 Rev 2 ed.). Obtenido de https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

Organización Internacional de Normalización (ISO). (2013). *Sistemas de Gestión la Seguridad de la Información (27001).*

Rendón-Macías, M. E., Villasís-Keeve, M. Á., & Miranda-Novales, M. (2016). Estadística descriptiva. *Revista Alergia, 63*(4), 1. Obtenido de https://www.redalyc.org/pdf/4867/486755026009.pdf

Rodríguez-Rojas, Y. (2021). Continuidad del negocio: conceptualización y metodologías de evaluación. *SIGNOS,Investigación en sistemas de gestión., 13*(1). doi:https://doi.org/10.15332/24631140.6337