Recepción: 13-11-2018 Aprobación: 10-01-2019

Garantía de disponibilidad en infraestructuras críticas CNS/ATM

Availability assurance on critical CNS/ATM infrastructures

Guillermo Brito Acuña[1]guillermo.brito@aeronav.avianet.cu

Resumen

Hoy las infraestructuras críticas controlan cada vez más sistemas importantes para la economía o el correcto funcionamiento de los gobiernos. El aumento de la dependencia tecnológica hace que aumenten los riesgos asociados a ellos. Por lo que gestionarlos correctamente, identificarlos, mitigarlos o asumirlos resulta de vital importancia. El presente documento muestra el procedimiento utilizado en nuestra infraestructura crítica de Comunicación, Navegación, Vigilancia y Gestión del Tráfico Aéreo (CNS/ATM). Mediante el cual se han gestionado posibles manifestaciones de riesgos que amenazan la disponibilidad de estas infraestructuras que atendiendo a sus niveles de criticidad tienen una exigencia de disponibilidad superior al 99%. El procedimiento es útil para garantizar la correcta gestión de riesgo ante amenazas surgidas por modificaciones realizadas a la infraestructura, previendo posibles fallos y el actuar ante ello en los planes de contingencias y reducción de desastres.Se muestran también los resultados obtenidos mediante la aplicación de esta propuesta en la infraestructura.

Palabras claves: Gestión de Riesgos, Infraestructuras Criticas, Garantía de Disponibilidad.

Abstract

Critical infrastructure and security software control today more and more relevant systems for the economy and the proper functioning of governments. By the increase of the technological dependence, increase the risks related to them. Then the proper management, identification, mitigation and assumption of these risks are of capital importance. This document shows the procedure used in our critical infrastructure for Communication, Navigation, Surveillance and Air Traffic Management(CNS/ATM). With this procedure we managed the possible manifestations of risks threatening the availability of these infrastructures, which due to their level of importance require availability higher than 99%. The procedure is useful to assure the proper risk management by threats that arise from modifications on the infrastructure, anticipating possible failures and acting accordingly in the contingency and risk reduction plans. The results obtained by the application of this proposal on software related to meteorological variables in aerodromes und data publication systems from the Cuban aeronautical information service are also shown.

[1]Ingeniero SRSA, Especialista en Seguridad Informática. Empresa Cubana de Navegación Aerea. Cuba

Recepción: 13-11-2018 Aprobación: 10-01-2019

Keywords: Risk Management, Critical Infrastructures, AvailabilityAssurance.

Introducción

Por infraestructura crítica se entiende aquellas instalaciones, redes y tecnologías, cuya interrupción o destrucción puede tener una repercusión importante en la salud, la economía o el eficaz funcionamiento de los gobiernos(Casanovas, Boiero, & Tapia, 2015). En estos sistemas se evidencia que las amenazas informáticas no sólo comprometen el mundo digital, sino que también son un riesgo mayor, para el mundo físico (Prieto, 2014). Su seguridad se relaciona con la calidad, es una actividad del aseguramiento que se centra en la identificación y evaluación de los peligros potenciales que podrían afectarlas y ocasionar que falle (Pressman, 2010).La sociedad se encuentra vinculada innegablemente a estas tecnologías; sin embargo, un uso tan amplio hace que existan grandes riesgos en cada una de las aplicaciones tecnológicas.

Los riesgos evolucionan y aumentan con la tendencia al uso de tecnologías (Norma Martínez y Porcelli, 2015)**.** Atendiendo a esta problemática se hace evidente la necesidad de identificar y reducir la mayor cantidad de estos riesgos, sobre todo en infraestructuras críticas. Para ello se identifica la infraestructura como un sistema compuesto por tres actores principales: los usuarios, los equipos de comunicaciones y los software. La interacción entre ellos conlleva asociado riesgos que en caso de manifestarse atentarían contra el objeto de la infraestructura. El presente artículo, pretende exponer la experiencia obtenida mediante la implementación de un procedimiento que garantice la disponibilidad ante modificaciones de cualquier índole que se realicen sobre nuestras infraestructuras.

Garantía de disponibilidad en infraestructuras críticas CNS/ATM

Necesidad de Implementación

Las infraestructuras pueden ser consideradas sistemas compuestos por 3 actores principales, el software, los usuarios y los equipos de comunicaciones. Se identificó una variable que atenta contra el buen desenvolvimiento del mismo y está considerado un riesgo para la infraestructura general. Este es la capacidad de los actores principales de variar con el tiempo. Los usuarios causan bajas y altas, además de estar constantemente influenciados por otras tecnologías. Los equipos de comunicaciones tienen un cronograma de cambio, mantenimiento, además de ser afectados por incidentes o roturas no planificadas y el software en consecuencia de las exigencias de los organismos rectores y acuerdos internacionales y posibilitar mejoras en los servicios brindados, ganado en usabilidad y adecuación funcional, cambian y se modernizan.

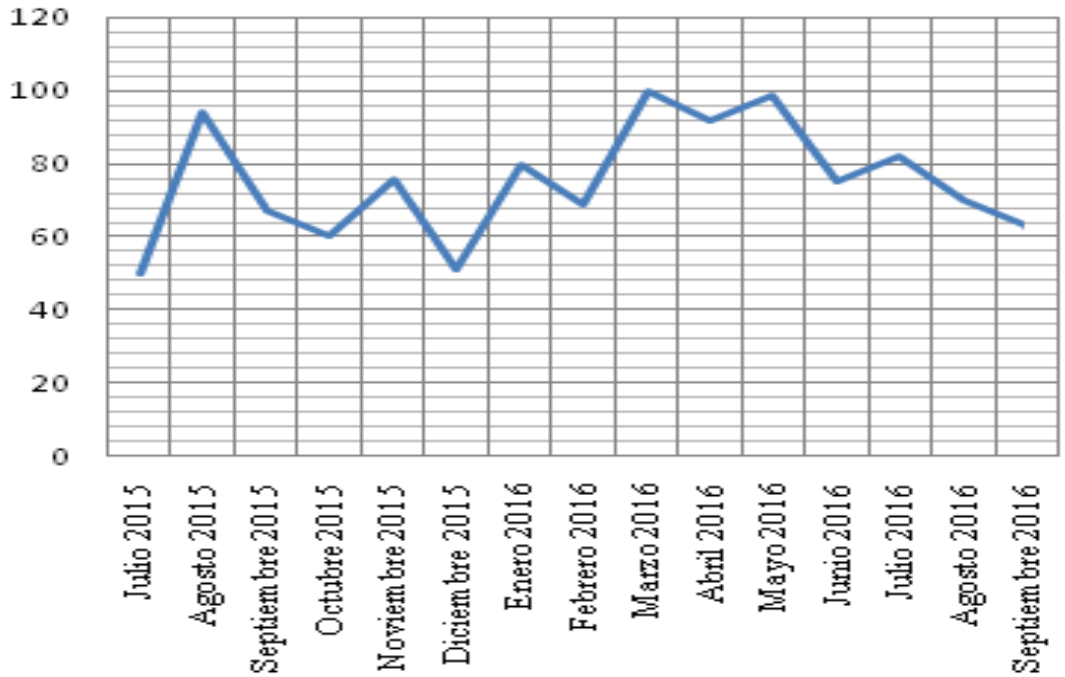
Esta variabilidad puede atentar contra los indicadores de seguridad establecidos en la (ISO/IEC 27001, 2015). Como es el caso de la disponibilidad de la información ósea la capacidad del sistema o componente de estar operativo y accesible para su uso cuando se requiere. En el caso de las infraestructuras críticas CNS/ATM la disponibilidad es calculada a partir de las sumatoria de horas disponibles entre las horas de disponibilidad ideal. En el caso de la aeronavegación la OACI exige que esta se mantenga superior al 99% diario. En el caso del sistema donde se realizó el

Recepción: 13-11-2018 Aprobación: 10-01-2019

experimento requería una disponibilidad de 12504 horas diarias, donde se garantizara la disponibilidad de 521 equipos que brindan soporte a la navegación aérea. Con una afectación general de solo 100 horas entre todos los equipos se afectaría los indicadores de disponibilidad de la infraestructura.

Todos los equipos son propensos a sufrir deterioros y roturas, por lo que es imposible subir los indicadores de disponibilidad al 100% y atendiendo a que muchos de estos equipos se encuentran geográficamente distantes, resulta conveniente disminuir el tiempo de demora de una interrupción. Muchas veces, las interrupciones son planificadas por corresponder a mejoras del equipamiento, software o configuración de los activos de la infraestructura la correcta ejecución de estas mejoras garantizan un mejor servicio y con ello la disponibilidad de la infraestructura. También ocurre que se cometen errores que se manifiestan luego de implementados los cambios sobre estas infraestructuras e implican una reinversión en transporte, un descenso en la calidad de los servicios y en general un riego para el dominio de la infraestructura.

La figura ilustra el comportamiento de las afectaciones de la disponibilidad en la infraestructurashasta el momento de implementado el procedimiento. Con ello se pretende disminuir la cantidad de horas de interrupción, las cuales según el registro histórico tienen una media cercana a 80 horas diarias ósea 2400 horas de interrupción mensual de las 375000 horas ideales de disponibilidad, dejando un índice de maniobrabilidad de 600 horas mensuales, lo cual deja un margen de reacción de menos de q hora diaria,



Capacitación de Implicados

Recepción: 13-11-2018 Aprobación: 10-01-2019

La primera acción en la implantación del procedimiento, es la capacitación de los diferentes actores. Atendiendo que está diseñado para infraestructuras con redes WAN ampliamente distribuidas, los actores a capacitar son:

Administradores de Red y Sistemas y Jefe de Comunicaciones: Son los responsables de implementar las medidas para garantizar la seguridad en su subconjunto de la red. Son actores con un profundo conocimiento de la infraestructura y sus sistemas. En conjunto con los especialistas de seguridad informática, velan por la seguridad de la misma y son los responsables de las configuraciones de equipos de comunicaciones y sus accesos. Es primordial que conozcan las leyes, resoluciones y buenas prácticas para su dominio de trabajo, la capacitación en este sentido, potencia generalizar y homogenizar el conocimiento y ubicarlo en el contexto para aplicar en infraestructuras críticas.

Especialistas de Seguridad Informática: El artículo 83 de (RAC 10, 2016), faculta a los ESI para organizar, controlar, supervisar y evaluar el cumplimiento de la base legal en materia de seguridad informática, en su sector de la infraestructura. Su conocimiento del procedimiento de control debe ser profundo y detallado, por lo que se recomienda un análisis exhaustivo de las lista de verificaciones establecidas en los controles. Es el responsable de encontrar las vulnerabilidades, amenazas y riesgos mediante los controles que realiza. Debe tener un amplio conocimiento de la red y sus sistemas. En conjunto con los administradores de redes y sistemas, velan por la seguridad, analizan los riesgos, analizan incidentes y mejoran los planes de contingencia. Es un rol vital para el marco de trabajo en general que está facultado para vulnerar la infraestructura y tiene acceso a todos los servicios que se prestan, siendo el responsable de análisis de información forense y pruebas de penetración.

Directivos: Estos actores, son los responsables de garantizar la misión de la infraestructura. Son los principales interesados en la reducción de riesgos, cumplimiento de la legalidad y garantizar la disponibilidad y seguridad en la red. Su conocimiento de redes y sistemas no es profundo, pero si son los principales interesados en el buen funcionamiento de ellas. Es importante su capacitación para permitir la implantación del marco de trabajo y sus procedimientos derivados así como contribuir a los controles en las diferentes aéreas y su aseguramiento logístico. Además concientizar la importancia que tienen en la reducción de riesgos y amenazas a través del plan de mejoras que tienen los sistemas de la calidad implantados que normalmente son los responsables de gestionar.

Procedimiento de Garantía de Disponibilidad ante Modificación en la Red

El procedimiento está pensado para gestionar los riesgos asociados con modificaciones en sistemas, equipos y software no incluidos en los mantenimientos preventivos o correctivos que se realizan en la infraestructura. Se documentan las acciones, posibles soluciones ante incidentes y posibles repercusiones del cambio implementado en caso de fallo. Aplica en los casos donde existe la necesidad de modificar el equipamiento activo, las configuraciones o software de algunos de los componentes de la infraestructura, de forma no planificada. Por tanto este procedimiento excluye los mantenimientos planificados, las actualizaciones

Recepción: 13-11-2018 Aprobación: 10-01-2019

periódicas de software y las interrupciones puntuales de la infraestructura, siempre que no allá una modificación del hardware o la configuración.

Dado el caso, los especialistas o ingenieros confeccionan el Control para la Garantía de Disponibilidad ante Modificación en la Red. Este debe documentar la cantidad de sistemas, software y equipos que se pretenden modificar. Además el lugar de la modificación, el propósito que se persigue con la misma y los requerimientos indispensables para realizarla. Se registran también el grupo de tareas necesarias para alcanzar la modificación de manera exitosa, incluyendo tareas de respaldo y medición. Atendiendo que estas tareas pueden afectar la disponibilidad de la infraestructura se documentan las fechas de inicio y final de las tareas propuestas. Esto permite en caso de afectación preparar la contingencia y con ello disminuir el impacto de las mismas.

Estas modificaciones son complejas y habitualmente multidisciplinarias. Por ello el registro tiene un acápite donde se proponen los equipos técnicos, operacionales, de soporte y garantía de la modificación. Las tareas de las que serán responsables y en qué equipo y lugar de la infraestructura la realizará. Estas tareas deben ser consistentes con las tratadas anteriormente. De esta forma cuando se haga la aprobación por el jefe de comunicaciones del área en cuestión, estará comprometiendo oficialmente a la fuerza de trabajo subordinada a él y los aseguramientos necesarios para la tarea.

El documento también deberá recoger un grupo de tareas de verificación, el resultado esperado y obtenido y si la realización de la tarea tiene impacto para la operación. Se documentarán los riesgos en que se incurren estimando la posibilidad de oscurecía e alta media o baja y el impacto en caso de ocurrencia, este último se clasifica como ninguno, menor, mayor o desastroso. Se establecen tareas de mitigación en caso de manifestarse la amenaza, los responsables de mitigarla y las operaciones para validar la estabilidad y el tiempo que se le empleará.Una vez terminado el cambio se deberá documentar el grupo de acciones que deberán realzarse en caso que producto de la manifestación de una amenaza se decida deshacer la modificación. Se documentan los tiempos de las tareas y las observaciones necesarias para llevarlos a cabo. Además de acciones de seguimiento se deberán monitorear para garantizar la disponibilidad luego de la modificación.

Estos datos deberán ser aprobados por el Jefe de Comunicaciones teniendo en cuenta las tareas que garanticen las menores afectaciones a la disponibilidad del servicio y que tenga un plan de respuesta a incidentes coherente con los posibles riesgos que se puedan manifestar y en caso contrario identifique los errores.

Este procedimiento es controlado por el Especialista de Seguridad Informática y busca tener registrados el 100% de las modificaciones no planificadas deben estar documentadas.Se implementó el siguiente documento como plantilla para agilizar el proceso, los números corresponden a las siguientes descripciones de tareas:

Recepción: 13-11-2018 Aprobación: 10-01-2019

Encabezado de la Entidad			
Descripción del Cambio			
Sistema/ Equipos /Software a Cambiar	Versión	No	Lugar
1.	2.	3.	4.
Propósito	5.		
Requerimientos	6.		
Gestión de Tiempo			
Tareas	Desde	Hasta	
7.	8.	9.	
Equipo de Trabajo Operacional, Técnico, Soporte y Garantía			
Nombre y Apellidos	Tareas	Localización	Equipo
10.	11.	12.	13.
Tareas de Verificación			
Tareas	Resultado Esperado	Impacto en la Operación	Observaciones
14	15	16	17

Recepción: 13-11-2018 Aprobación: 10-01-2019

Análisis de Riesgo				
Riesgo	Posibilidad	Impacto	Tareas de mitigación	Responsable
18.	19.	20.	21.	22.
Resultado de Verificación y Estabilidad				
Tareas	Resultado Real	Observaciones (Inicio y Fin)		
23.	24.	25.		
Acciones para Regresar al Estado Inicial				
Tareas	Tiempo Estimado	Observaciones		
26.	27.	28.		
Acciones de Seguimiento				
Tareas	Tiempo	Responsable	Observaciones	

Recepción: 13-11-2018 Aprobación: 10-01-2019

Elaborado		Aprobado		Ejecutado	
Nombre	Firma	Nombre	Firma	Nombre	Firma

Recepción: 13-11-2018 Aprobación: 10-01-2019

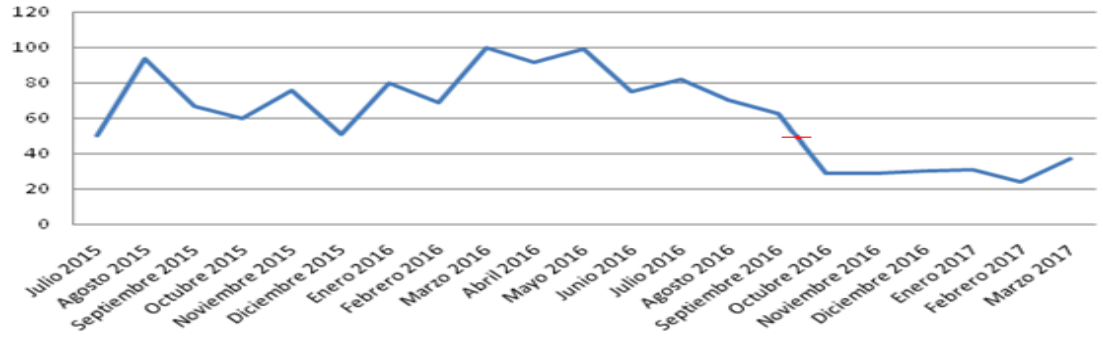
1. Nombre del Sistema, Equipo o Software que se planea modificar
2. Versión de los Sistemas, Equipos o Software que se planea modificar
3. Cantidad de Sistemas, Equipos o Software que se planea modificar
4. Lugar donde se planea realizar la modificación
5. Propósito que se persigue con la modificación
6. Requerimientos necesarios para realizar la modificación de manera exitosa
7. Lista de Tareas para cumplir la modificación exitosamente
8. Desde: Fecha Hora de Comienzo por Tarea
9. Hasta: Fecha Hora de Final por Tarea
10. Nombre y Apellidos de los miembros del equipo
11. Tareas en las que están implicados, (deben coincidir con 7.)
12. Localización en caso de problemas
13. Equipo al que pertenece (Operaciones, Técnico, Soporte y Garantía)
14. Tareas de Verificación
15. Resultado Esperado.
16. Impacto en las Operaciones (Si o No)
17. Observaciones
18. Lista de posibles riesgos
19. Posibilidad de ocurrencia (alta, media, baja)
20. Impacto en la disponibilidad en caso de ocurrencia (ninguno, menor, mayor, desastroso)
21. Lista de tareas de mitigación para cada riesgo
22. Responsables de las tareas anteriores
23. Tareas de Verificación y Seguimiento realizadas
24. Resultado de las tareas
25. Observaciones incluyendo inicio y fin de las tareas
26. Lista de tareas para regresar al estado anterior en caso de fallo
27. Tiempo Estimado por tarea
28. Observaciones
29. Lista de tareas de seguimiento luego de la modificación
30. Tiempo estimado por tarea
31. Responsable por tarea
32. Observaciones

CONCLUSIONES

Este procedimiento está implementado en la infraestructura crítica CNS/ATM. Las mediciones que se exponen corresponden a los resultados obtenidos de los controles y mediciones realizadas en los primeros 6 meses de implementación. Es importante señalar que se implanto en todos las zonas aeroportuarias del país, incluyendo los aeródromos internacionales, nacionales, radares y otros dispositivos y estaciones útiles para la aeronavegación. Se compiló información del 100% de estas instalaciones.

Como resultado del mismo se disminuyó la ocurrencia de afectaciones a la disponibilidad en un porciento superior a la media del periodo analizado. Estableciendo la media a partir de octubre de 2016y hasta marzo de 2017 en 31 horas de interrupción como promedio diario, lo cual da un margen de tiempo cercano a las 70 horas para reaccionar ante posibles interrupciones por otras causas no planificadas.

Recepción: 13-11-2018 Aprobación: 10-01-2019



El gráfico demuestra la mejora en horas disponibles, la cual tuvo un efecto favorecedor incluso desde el periodo de capacitación en septiembre de 2016. También gracias a los registros fue posible determinar la mayor incidencia de riesgos en estas infraestructuras por equipo especializado. Identificar tendencias negativas y generalizar experiencias entre los diferentes actores implicados. Es posible determinar también los tiempos medios de respuesta a incidentes y determinar cuántas afectaciones a la disponibilidad son consecuencia de estas modificaciones.

Referencias

Casanovas, E., Boiero, F., y Tapia, C. (2015). *Fortalecimiento en la Seguridad de Web Services para Aplicaciones Críticas*. Instituto Universitario Aeronáutico, Facultad de Ingeniería.

ISO/IEC 27001, E. I. (2015). *Tecnología de la Información – Técnicas de Seguridad – Sistemas de gestión de seguridad de la información – Requerimientos.* Ginebra: International Organiation for Standardization.

Norma Martínez , A., y Porcelli, A. (2015). Implicancias de las tecnologías informáticas en el ambiente y nuevas tendencias en el desarrollo de la informática verde como aporte al desarrollo sustentable. *Actualidad Jurídica Ambiental* (50).

Pressman, R. S. (2010). *Ingeniería de Software un enfoque práctico.séptima edición* (Vol. S.A. DE C.V). Mcgraw-HILL INTERAMERICANA EDITORES.

Prieto, M. D. (2014, Octubre 13). Detección proactiva de amenazas en infraestructuras críticas. Retrieved Octubre 23, 2015. En *III Congreso Iberoamericano de Ciberseguridad Industrial:* blogthinkbig.com