COMANDANCIA GENERAL
ARMADA DE REPÚBLICA DOMINICANA

6496

10 MAR 2022

"M E M O R Á N D U M"

Al : *Inspector General, Armada de República Dominicana.*

Intendente General, Armada de República Dominicana.

Director General de Tecnología de la Información y la Comunicación (TIC), Armada de República Dominicana.

Director de Planificación y Desarrollo, Armada de República Dominicana.

Cortésmente, por medio del presente, se les designa miembros del comité de continuidad (CONTI), a los fines de crear los políticas y procedimientos necesarios para la protección de nuestro sistema de información y comunicación ante eventualidades que pongan en riesgo dicho sistema.

RAMÓN GUSTAVO BETANCES HERNÁNDEZ
Vicealmirante, ARD.
Comandante General de la Armada de República Dominicana.

Anexo: ***Oficio No. 044, de fecha 09-03-2022, relativo al asunto y anexo.***

JGR
AC/ jr.-
Copia al: *Subcomandante General, ARD.*
Inspector General, ARD.

DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN

Municipio Santo Domingo Este, PSD.
09 de marzo de 2022.

Núm. 044/2022.

Al : Comandante General de la Armada de República Dominicana.

Del : Director de Tecnología de la Información y Comunicación (TIC), Armada de República Dominicana.

Asunto : Solicitud de creación del Comité de Continualidad (CONTI), ARD.

Anexo : Copia de la Norti - A7.

1.- Respetuosamente nos dirigimos a ese superior despacho, con la finalidad de solicitar la interpocision de sus buenos oficios, a fin de que sea creado el Comité de Continuidad (CONTI), cuya creación es recomendada por la Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC), conforme a lo establecido en el literal (d) de la sub-sección 4.01.3 de la norma NORTI A7, sobre seguridad de las TIC, a los fines de que este, según las funciones que les son inherentes, cree las políticas y procedimientos necesarios para la protección de nuestro sistema de información y comunicación ante aventualidades que pongan en riesgo dicho sistema.

2.- Asimismo, de ser aprobada la presente solicitud, salvo su mejor parecer, recomendamos que dicho comité este conformado por parte de los miembros que actualmente conforman el Comité de Implementación y Gestión de Estándares de las Tecnologías de la Información y Comunicación (CIGETIC), por su vinculación en los asuntos relacionados a la rama que precedentemente describimos,

1.- Inspector General, ARD., (Coordinador).
2.- Director de Tecnologia TIC., ARD., (Miembro).
3.- Intendente General, ARD., (Miembro).
4.- Director del la Dirección de Planificación y Desarrollo, ARD., (Miembro).

CESAR RICARDO REYES RAMIREZ
Capitán de Navío, (DEM), ARD.

DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y LA COMUNICACIÓN (DTIC) R. D.

Presidencia de la República

OFICINA PRESIDENCIAL DE TECNOLOGÍAS
DE LA INFORMACIÓN Y COMUNICACIÓN

NORTIC A7

2016

NORMA PARA LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN EN EL ESTADO DOMINICANO

Santo Domingo, República Dominicana

(d) Los organismos deben disponer de los mecanismos necesarios para generar alertas y notificaciones cuando los sistemas críticos dejen de esta disponible y poder atenderlos antes de que afecten los niveles operativos del organismo.

(e) Deben hacerse análisis históricos periódico para identificar posibles ocurrencias que no han sido resueltas en su causa raíz.

Sub-sección 4.01.2. Gestión de la capacidad

(a) Dentro de los procedimientos operativos del organismo deben disponerse de procedimientos y recursos tecnológicos para dar seguimiento al uso de los recursos de TIC y poder identificar cualquier variación importante que demanden los usuarios o sistemas.

(b) Deben generarse los informes periódicos pertinente para identificar tendencias y proyecciones de posibles necesidades para poder actuar de manera oportuna en el aumento de la capacidad.

(c) Deben disponerse de los mecanismos necesarios para generar alertas y notificaciones cuando estas variaciones alcancen ciertos niveles de uso antes de que se lleguen a condiciones de criticidad.

Sub-sección 4.01.3. Gestión de incidentes

(a) Los organismos gubernamentales deben de implementar un Programa de Gestión de Incidentes (PGI), que les permita responder lo antes posible a un incidente con fines de restaurar el servicio o solucionar el problema, así como evitar que el impacto se extienda a otras áreas de recursos del organismo o fuera.

(b) Este programa debe crear un comité de trabajo multidisciplinario que contenga representantes de alto nivel de cada una de las áreas funcionales más importantes del organismo.

(c) Deben crearse los procedimientos y políticas necesarios para los principales escenarios a experimentar los cuales deben estar escritos, probados y aprobados por la dirección.

(d) Los incidentes de seguridad de información deben ser notificados al Departamento de Investigaciones de Crímenes y Delitos de Alta Tecnología (DICAT), cuando se encuentren indicios que puedan ser una evidencia criminal según lo establece la Ley No. 53-07 sobre crímenes y delitos de alta tecnología.

(e) El organismo debe disponer de procedimientos administrativos y operativos para disparar el proceso de gestión de incidentes tan pronto como se confirmen los eventos o notificaciones que, proviniendo de cualquier fuente, indique que está sucediendo un incidente.

(f) El organismo debe informar a las partes interesadas correspondientes cómo reportar un evento de seguridad o un incidente, esta capacidad de recibir notificaciones debe estar disponible las 24 horas del día 7 días de la semana 365 días al año.

(g) Deben implementarse los formularios necesarios para la recopilación de información pertinentes y los enrutados de llamadas necesarias para que los reportes sean dirigidos a personal activo o en turno fuera de horario.

(h) Debe motivarse al personal a identificar posibles situaciones de riesgo que pueden conducir a un incidente y reportarlos al punto de contacto[31].

(i) Debe elaborarse un procedimiento de escalamiento para que en los casos de que el personal interno no esté en capacidad de manejar el incidente de manera correcta, el caso pueda ser escalado a personas con las capacidades necesarias sin tener que recurrir a procesos de aprobación por tema de costos o cualquier otra autorización que sea necesaria.

Esto permitirá hacer uso de una horas estimadas y pre aprobadas de soporte en caso de ciertos escenarios.

[31] Dentro de la disciplina de Manejo de Incidentes, es el grupo, unidad o persona que tiene el rol de recibir el informe inicial de un evento de seguridad, para examinarlo, evaluarlo, resolverlo o tratarlo y en caso de que este fuera de su alcance de especialización escalarlo a los grupos de tratamiento de incidentes.

(j) Debe disponerse de un proceso de lecciones aprendidas que permitan evaluar las enseñanzas de las cosas que pudieron hacerse diferente, las que funcionaron y las posibles causas raíz de incidente.

(k) Luego de cada evento deben calendarizarse acciones de seguimiento para aquellos casos en que no se pudo resolver la causa raíz.

(l) Debe documentarse el procedimiento para que se active el plan de continuidad para aquellos incidentes que tengan un tiempo estimado de recuperación superior a lo identificado como aceptable para el organismo

SECCIÓN 4.02. Plan de continuidad

La implementación de los procesos de la gestión de la continuidad, es un aspecto de gran importancia dentro del departamento de TIC; esta implementación busca que tanto los servicios del organismo, como los procesos que sustentan las operaciones permanezcan en funcionamiento ante cualquier eventualidad, ya sea externa o interna.

(a) Los organismos gubernamentales deben tener un Comité de Continuidad (CONTI).

(b) La continuidad del organismo debe tener como responsable a la máxima autoridady no al área de TIC.

(c) El CONTI debe estar compuesto por la máxima autoridad del organismo y del departamento TIC, y otras áreas claves para la prestación de servicios.

(d) Los organismos gubernamentales deben tener un plan de continuidad para asegurar la recuperación ordenada y planificada de sus operaciones vitales y sus servicios al ciudadano o demás organismos.

(e) El CONTI debe considerar no solo los aspectos relacionados o dependientes de TIC sino también, y primariamente, los procesos, las personas, las localidades que son vitales para que el organismo pueda seguir proveyendo servicios a la comunidad y al estado.

(f) La seguridad de la información debe estar dentro del plan de la continuidad del organismo.