Organización de Aviación Civil Internacional

NOTA DE ESTUDIO

AN-Conf/13-WP/279[1]
27/9/18
(Español e inglés únicamente)

DECIMOTERCERA CONFERENCIA DE NAVEGACIÓN AÉREA

Montreal, Canadá, 9 al 19 de octubre de 2018

COMITÉ A

Cuestión 5 del orden del día: **Cuestiones emergentes**
5.4: **Ciberresiliencia**

CIBERRESILIENCIA AERONAUTICA

(Presentada por COCESNA)

RESUMEN

En esta nota de estudio COCESNA quiere destacar su interés en el tema de la Ciberresilicencia, como soporte de una organización para tener la capacidad de enfrentar condiciones adversas, ante un eventual ataque contra los activos esenciales para el funcionamiento de las agencias, empresas o administraciones y los propósitos de su razón de ser.

Medidas propuestas a la Conferencia: Se invita a la Conferencia a:
a) Recomendar a toda la comunidad aeronáutica estar debidamente preparados para generar una respuesta efectiva a los ciberincidentes que se puedan presentar en las operaciones diarias;
b) Reconocer la importancia de desarrollar el Gobierno de Ciberseguridad para hacerle frente a las amenazas cibernéticas; y
c) Tratar las ciberamenazas, a través de las adecuadas tácticas, técnicas y procedimientos basados en normas y buenas prácticas de nivel mundial.

1. INTRODUCCIÓN

1.1 La ciberresilencia es la capacidad de una empresa para anticipar, aguantar, recuperarse y evolucionar para mejorar sus capacidades al enfrentarse a condiciones adversas, situaciones límite o ataques contra los activos necesarios para funcionar. Una empresa ciberresiliente realiza un alineamiento de las prioridades de ciberseguridad con la misión y metas del negocio.

1.2 Los ciberincidentes amenazan tanto los activos como los procesos críticos de las empresas, por lo tanto, el objetivo de la ciberresiliencia es asegurar que dichos procesos siguen disponibles a un nivel aceptable incluso durante un incidente. Para conseguir dicho objetivo es vital que se entienda y prioricen las necesidades de los grupos de interés, se identifiquen los procesos críticos del negocio requeridos para alcanzar la misión y metas establecidas por la empresa. Un marco de gobierno de TI puede ayudar a mitigar parte de los riesgos de la ciberseguridad.

[1] Las versiones en español e inglés fueron proporcionadas por COCESNA.

1.3 COCESNA ha establecido la ejecución de un proyecto para la implementación de un Marco de Gobierno y Gestión TIC, cuyo objetivo es lograr generar el valor esperado de las inversiones TIC que se realizan, mediante el establecimiento de buenas prácticas y el fortalecimiento de las capacidades de la empresa (habilitadores). Lo anterior ayuda a obtener valor óptimo de las Tecnologías de Información manteniendo un balance entre los beneficios, riesgos y recursos. Dentro de este marco se elaboró el Plan Estratégico de Tecnologías de Información y las Comunicaciones (PETIC). La creación de valor como se define en COBIT5, supone un balance entre la obtención de beneficios, la optimización de los riesgos y la optimización de los recursos.

2. ANÁLISIS

2.1 Dentro de las mejoras identificadas con el establecimiento del Marco de Gobierno y Gestión TIC se realizó un diagnóstico de Seguridad de la Información tomando como referencia la norma ISO 27000, como resultado se obtuvo un análisis de brechas y un plan de acción que viene a fortalecer y garantizar la disponibilidad, integridad y confidencialidad de los datos.

2.2 Para un adecuado cumplimiento con las normativas de seguridad de información se han desarrollado una serie de políticas y procedimientos que ayuden con la regulación de herramientas HW y SW, así como una adecuada clasificación de la información, controles de acceso robustos, respuesta a incidentes de seguridad, respaldo de la información, etc. Las estrategias y actividades a desarrollar en el Plan Estratégico de las Tecnologías de Información y las comunicaciones se resumen en:

- La consideración que las personas también pueden causar o contribuir significativamente a un incidente, se ha definido un plan de capacitación a los empleados de COCESNA, respecto a seguridad de la información y las amenazas persistentes a las cuales están expuesto por parte de los atacantes.

- Realizar un diagnóstico de ciberseguridad tomando como referencia el marco de trabajo de ciberseguridad para infraestructuras críticas, elaborado por el Instituto Nacional de Estándares y Tecnología (NIST), las funciones básicas del marco están orientadas a Identificar, Proteger, Detectar, Responder y Recuperar.

- Fortalecer la estructura organizacional mediante una unidad de Ciberseguridad, la que se hará cargo de gestionar el riesgo cibernético para incrementar y fortalecer el valor del negocio mediante una adecuada estrategia que permita una adecuada ciberresiliencia en la corporación. Esta Unidad tendrá el objetivo de detectar, analizar y responder a incidentes de seguridad cibernética de forma oportuna ante cualquier intento de ataque en redes, servidores, bases de datos, aplicaciones, sitio web, etc.

2.3 Debido a la necesidad de proveer los conocimientos necesarios en materia de ciberseguridad se ha seleccionado a un grupo de empleados para recibir la capacitación sobre Fundamentos de Ciberseguridad (CSX) promovido por la asociación de auditoría y control de sistemas de información (ISACA), el cual ha sido desarrollado en colaboración con expertos de ciberseguridad de las compañías líderes en todo el mundo.

3. CONCLUSIÓN

3.1 La ciberseguridad evoluciona a nivel mundial llegando a transformarse en unas de las disrupciones tecnológicas realmente impactantes, es por eso que se debe estar debidamente preparados y generar una respuesta efectiva a los ciberincidentes que se puedan presentar en las operaciones diarias.

3.2 COCESNA está en proceso de desarrollar el Gobierno de Ciberseguridad para hacerle frente a las amenazas cibernéticas, estableciendo un marco que guíe el desarrollo y mejora continua de la estrategia de Ciberseguridad orientada a la creación de valor. Mediante el Gobierno de de Ciberseguridad se estará dando un adecuado tratamiento a las ciberamenazas, permitiendo contar con las adecuadas tácticas, técnicas y procedimientos basados en normas y buenas prácticas de nivel mundial.

— FIN —