Organización de Aviación Civil Internacional
Oficina para Norteamérica, Centroamérica y Caribe

NOTA DE ESTUDIO

NACC/DCA/11 — NE/28 **Rev.**
06/06/23

Undécima Reunión de Directores de Aviación Civil de Norteamérica, Centroamérica y Caribe (NACC/DCA/11)

Varadero, Cuba, 28 al 30 de junio de 2023

Cuestión 4 del Orden del Día: **Implementación regional NAM/CAR de seguridad operacional/navegación aérea**

4.2 Implementación de asuntos de navegación aérea

Cuestión 5 del Orden del Día: **Implementación regional NAM/CAR de seguridad de la aviación/facilitación**

INICIATIVAS DE CIBERSEGURIDAD - COCESNA

(Presentada por Belice, Costa Rica, El Salvador, Guatemala, Honduras y Nicaragua)

RESUMEN EJECUTIVO

Dar a conocer las principales actividades implementadas por COCESNA en materia de Ciberseguridad.

Acción:	Las acciones sugeridas se presentan en la Sección 5.
Objetivos Estratégicos:	• Objetivo estratégico 1 – Seguridad Operacional • Objetivo estratégico 2 – Capacidad y eficiencia de la navegación aérea • Objetivo estratégico 3 – Seguridad de la aviación y facilitación • Objetivo estratégico 4 – Desarrollo económico del transporte aéreo • Objetivo estratégico 5 – Protección del medio ambiente

1. Introducción

1.1 El presente documento tiene como finalidad el dar a conocer las principales iniciativas que COCESNA ha emprendido en materia de Ciberseguridad.

2. Iniciativas de Ciberseguridad

2.1 En materia de ciberseguridad COCESNA inició con el establecimiento de un Objetivo Especifico dentro del PEC orientado *a* **"Implementar Ciberseguridad acorde a las buenas prácticas del sector aeronáutico y tecnológico"**, integrado como parte del objetivo estratégico de *"Fortalecer el posicionamiento como un organismo especializado en la prestación de servicios aeronáuticos a nivel internacional"*. La finalidad es transmitir la relevancia que COCESNA asigna al tema, incorporando iniciativas encaminadas a su implementación dentro de las cuales se presentan en la **Ilustración 1**.

Ilustración 1 - Gestión de Ciberseguridad COCESNA

2.2 A continuación, se detallan las iniciativas emprendidas por COCESNA en materia de Ciberseguridad:

a) **Marco Normativo**: Se desarrollo un marco normativo en materia de ciberseguridad, en el que se estableció la línea base de la gestión a nivel Corporativo, y que incluye lo siguiente:

- Principios de las Tecnologías de la Información y Ciberseguridad,
- Manual de Gestión de Tecnologías de la Información y Ciberseguridad (MGTI),
- Políticas de Tecnologías de la Información y Ciberseguridad (PTIC).

b) **Socialización**: Considerando que la mayor parte de los incidentes de ciberseguridad son ocasionados por factores humanos, se estableció dentro de las iniciativas de acción, la formación de competencias de los colaboradores. Inicialmente se socializó el marco normativo, posteriormente a nivel de boletines periódicos sobre indicadores y boletines eventuales con recomendaciones de ciberseguridad.

c) **Grupos de Ciberseguridad**: Se establecieron grupos de trabajo para la implementación de las iniciativas de ciberseguridad a nivel Corporativo, los cuales se describen en la **Ilustración** 2.

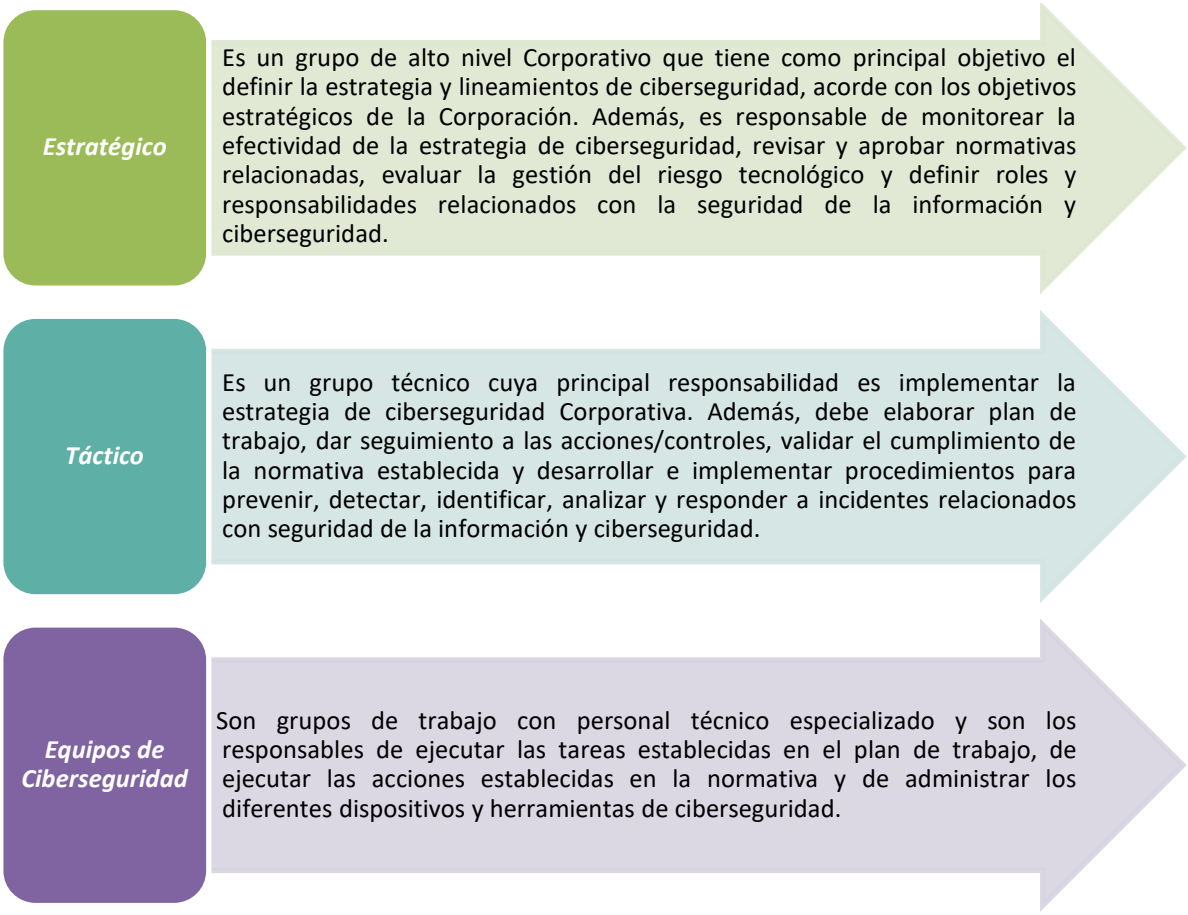

Ilustración 2 - Grupos de Ciberseguridad COCESNA

d) **Proceso Gestión TI y Ciberseguridad:** Se elaboró un proceso en el que se establecieron los procedimientos, rutinas, formatos, instructivos y demás para la administración de la gestión TI y de ciberseguridad a nivel Corporativo, además, estas fueron integradas en el SGC. Dentro de las principales actividades que se normaron dentro del proceso se encuentran:

- Gestión de Activos TI;
- Respaldo de Datos TI;
- Servicios Web;
- Vulnerabilidades y Parches TI;
- Gestión de Accesos Lógicos TI;
- Gestión de Software Malicioso;
- Planes de Contingencia TI;
- Firmas en Documentos Electrónicos;
- Gestión de riesgos en Ciberseguridad;
- Concienciación en Ciberseguridad;
- Gestión de incidentes TI;
- Transferencia de Activos de Información;
- Actualización de SLA.

e) **Ciberseguridad en la Gestión del Proceso OT:** La infraestructura de OT es el pilar tecnológico de la organización, compuesto por equipos y sistemas de OT interconectados, que constituyen el soporte fundamental para el sistema ATM y las operaciones. Se están realizando las siguientes actividades e iniciativas en el entorno OT de COCESNA para mitigar en la medida de lo posible las amenazas de ciberseguridad y mejorar la protección de la infraestructura de Tecnología Operativa (OT):

- Auditorías internas/externas de Ciberseguridad en Sistemas CNS/ATM;
- Participación en grupos de Ciberseguridad;
- Análisis de aplicaciones utilizadas en el ambiente OT
- Implementación de la herramienta Password manager
- Implementación de políticas de Ciberseguridad para acceso remoto a los equipos OT.
- Implementación de Políticas de utilización de dispositivos de Almacenamiento en el ambiente OT.
- Administración y monitoreo de la Red de Acceso
- Segmentación de la Red de Acceso a nivel lógico

f) **Procesos SGC**: Considerando que la ciberseguridad es un elemento integral dentro de la gestión Corporativa, se realizó un análisis y se establecieron una serie de elementos de ciberseguridad que debían integrarse en los procesos ya establecidos en el SGC, dentro de los cuales podemos destacar los presentados a continuación en la **Ilustración** 3.

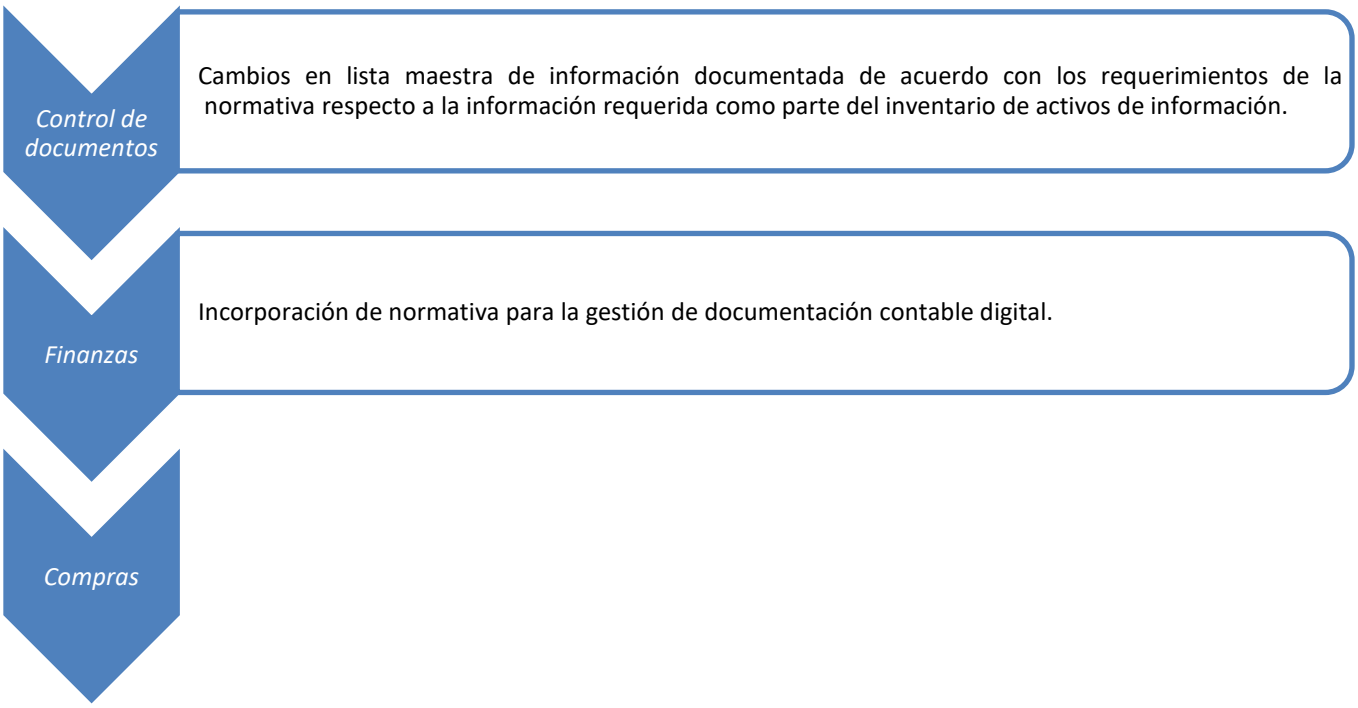

Ilustración 3 - Procesos SGC

g) **Gestión Técnica de Ciberseguridad**: Hace referencia a la aplicación de las medidas técnicas en la administración de dispositivos y herramientas especializadas para cumplimiento del marco normativo, dentro de las cuales podemos destacar:

- *Gestión de Riesgo Tecnológico*: Está relacionado con la evaluación de los riesgos y la aplicación de medidas para garantizar la continuidad de las operaciones, como ser:
  - ✓ Planes de contingencia y continuidad;
  - ✓ Infraestructura de sitio alterno;
  - ✓ Pruebas periódicas de planes de contingencia y continuidad;
  - ✓ Respaldos de datos.

- *Infraestructura de ciberseguridad*: Está relacionado con la administración técnica de los dispositivos y de las herramientas de ciberseguridad, como ser (Sin ser limitativas)
  - ✓ Antivirus;
  - ✓ Antispam;
  - ✓ Firewall;
  - ✓ Web Aplication Firewall (WAF);
  - ✓ Escaneo de vulnerabilidades;
  - ✓ Vídeo vigilancia;
  - ✓ Soporte remoto;
  - ✓ Encriptación de datos;
  - ✓ Borrado seguro.

- *Gestión de activos TI*: Relacionado con la administración de los equipos y dispositivos tecnológicos que incluye:
  - ✓ Ciclo de vida de los activos TI (Planificación, provisión, administración, descargo);
  - ✓ Clasificación de activos TI;
  - ✓ Identificación de activos críticos;
  - ✓ Inventario de Hardware;
  - ✓ Inventario y asignación de licencias de Software;
  - ✓ Gestión de parches.

- *Control de accesos lógicos*: Relacionado con la administración de cuentas y accesos, tanto de colaboradores, como de entidades externas, gestionando los elementos presentados en la **Ilustración 4.**

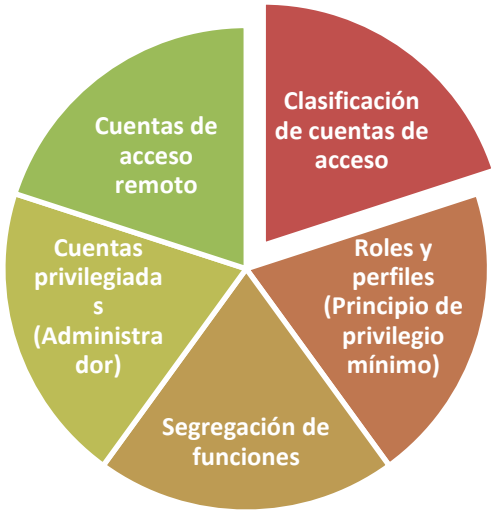

Ilustración 4 - Gestión de Accesos Lógicos en COCESNA

- *Concientización en ciberseguridad*: Relacionado con la formación del personal de la Corporación, que incluye entre otras tareas:
  - ✓ Inducción (Personal de nuevo ingreso, colaboradores actuales, entidades externas);

- ✓ Comunicados (Boletines, presentaciones, charlas, publicaciones Intranet);
- ✓ Nivel de formación: Evaluación permanente de las competencias requerida en cada puesto de trabajo en materia de ciberseguridad;
- ✓ Formación en Ciberseguridad (Capacitaciones, conferencias, grupos de trabajo, consultorías, suscripciones/membresías).

- *Tecnologías en la nube*: Relacionado con las tendencias de la industria sobre prestación de servicios Web y su aplicación de forma segura en COCESNA, dentro de las que destacan:
  - ✓ Nube aeronáutica: Provisión del SIARev SaaS (Software as a Service).
  - ✓ Servicios contratados (Office 365, almacenamiento en nube, trabajo colaborativo, página Web, Sw de gestión de calidad, redes sociales, entre otras).
  - ✓ Nube Hibrida: Integración entre los servicios On-Premise o nube privada (En sitio con infraestructura propia) con los servicios Web o nube pública.
  - ✓ Evaluación de modelos de servicios de Nube para Sistemas SAP.

- *Mesa de Ayuda:* Está asociado con la automatización de la gestión de solicitudes e incidentes, de acuerdo con las mejores prácticas, así somo la generación de estadísticas como apoyo a la toma de decisiones a nivel Corporativo.
  La **Ilustración 5** presenta los diversos elementos que se gestionan a través de las mesas de ayuda de COCESNA.

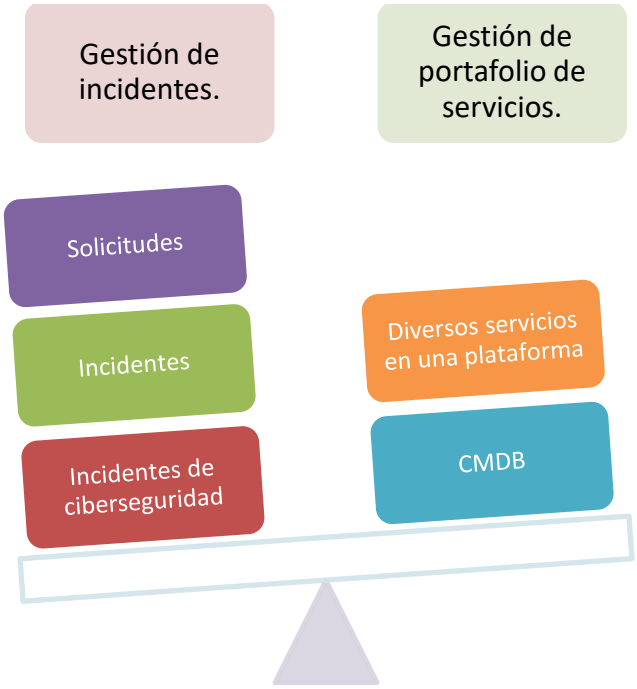

Ilustración 5 - Mesa de Ayuda COCESNA (CATI)

3. Acciones sugeridas

a) Tomar en consideración las iniciativas emprendidas por COCESNA para la implementación de ciberseguridad a nivel Corporativo;

b) Orientar a los Estados y Organizaciones sobre el desarrollo de políticas, establecimiento de metas, desarrollo de planes que fomenten la ciberseguridad en aviación; y

c) Promover el compartir las lecciones aprendidas, y los beneficios obtenidos con sus implementaciones para beneficio de otros Estados y organizaciones.

— FIN —