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

NOTA DE ESTUDIO

NACC/DCA/12 — NE/16
03/07/24

Doceava Reunión de Directores de Aviación Civil de Norteamérica, Centroamérica y Caribe (NACC/DCA/12)

Placenta, Belize 09-11 Julio 2024

Cuestión 3 del Orden del Día: **Seguridad de la Aviación (AVSEC) y Facilitación (FAL)**

Iniciativas de Ciberseguridad

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

RESUMEN EJECUTIVO	
Dar a conocer las principales actividades implementadas por COCESNA en materia de Ciberseguridad	
Acción:	Informar a los participantes acerca de las iniciativas de ciberseguridad implementadas por COCESNA
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
Referencias:	• Objetivo específico sobre ciberseguridad de COCESNA

1. Introducción

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

2. EJES DE LA CIBERSEGURIDAD

La Ciberseguridad en COCESNA estará sustentada en tres ejes principales e integrados entre sí para la adecuada protección de la plataforma tecnológica de COCESNA y sus componentes electrónicos los cuales se describen en la **Ilustración 1**.

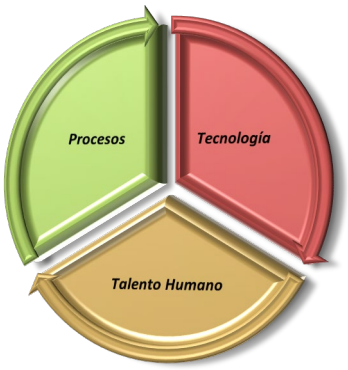

Ilustración 1- Ejes de la Ciberseguridad en COCESNA

a) **Personas**: Fortalecer competencias en temas de ciberseguridad a los funcionarios y empleados involucrados en la prestación de servicios.
b) **Procesos**: Elaboración de lineamientos, manuales, procedimientos, entre otros, así como la adopción y adaptación de mejores prácticas que permitan regular, controlar y monitorear la ciberseguridad dentro de la Corporación.
c) **Tecnología**: Fortalecer mediante herramientas tecnológicas el ciclo de vida de la gestión en ciberseguridad mediante las funciones de identificación, protección, detección, respuesta y recuperación ante posibles ciber amenazas.

3. Iniciativas de Ciberseguridad

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 2**.

Ilustración 2 - Gestión de Ciberseguridad COCESNA

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

a) **Objetivo Específico PEC:** Como parte del compromiso de COCESNA con el fortalecimiento de la ciberseguridad, se ha establecido dentro del Plan Estratégico de COCESNA 2020-2025 (PEC), el siguiente objetivo específico relacionado "Implementar Ciberseguridad de acuerdo con las buenas prácticas en el sector aeronáutico y tecnológico", dentro del cual se enmarcan las iniciativas y actividades que desarrolla COCESNA en materia de ciberseguridad.

b) **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).

c) **Ciberseguridad en Procesos SGC**: Considerando que la ciberseguridad es un elemento integral dentro de la gestión Corporativa, se realizó un análisis y se ejecutaron una serie de actividades para fortalecer el Sistema de Gestión de COCESNA (SGC), dentro de las cuales se puede destacar:

i. **Ciberseguridad en la Gestión de Procesos OT:** La infraestructura de Tecnología Operacional (OT) es el pilar tecnológico de la Corporación, compuesta por una gran variedad de equipos OT y diversos sistemas interconectados entre sí, que constituyen el soporte fundamental del sistema ATM y de

las operaciones en la prestación de los servicios de navegación aérea. En el entorno OT de COCESNA se están llevando a cabo las siguientes actividades e iniciativas para mitigar al máximo las amenazas de ciberseguridad y mejorar la protección de la infraestructura OT:

- Auditorías internas/externas de Ciberseguridad en Sistemas CNS/ATM;
- Participación en grupos de Ciberseguridad;
- Análisis de aplicaciones utilizadas en el entorno OT
- Implementación de herramienta para administración de cuentas privilegiadas.
- Implementación de políticas de ciberseguridad para el acceso remoto a equipos OT.
- Implementación de políticas de uso de dispositivos de almacenamiento externo en el entorno OT.

ii. **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.

iii. **Otros Procesos SGC**: Además del desarrollo o fortalecimiento de procesos específicos de ciberseguridad a nivel técnico OT/IT, considerando que la ciberseguridad es un elemento integral en la gestión Corporativa, se identificaron e incorporaron una serie de elementos de ciberseguridad a otros procesos del SGC, dentro de los cuales podemos destacar los presentados a continuación en la **Ilustración 3**.

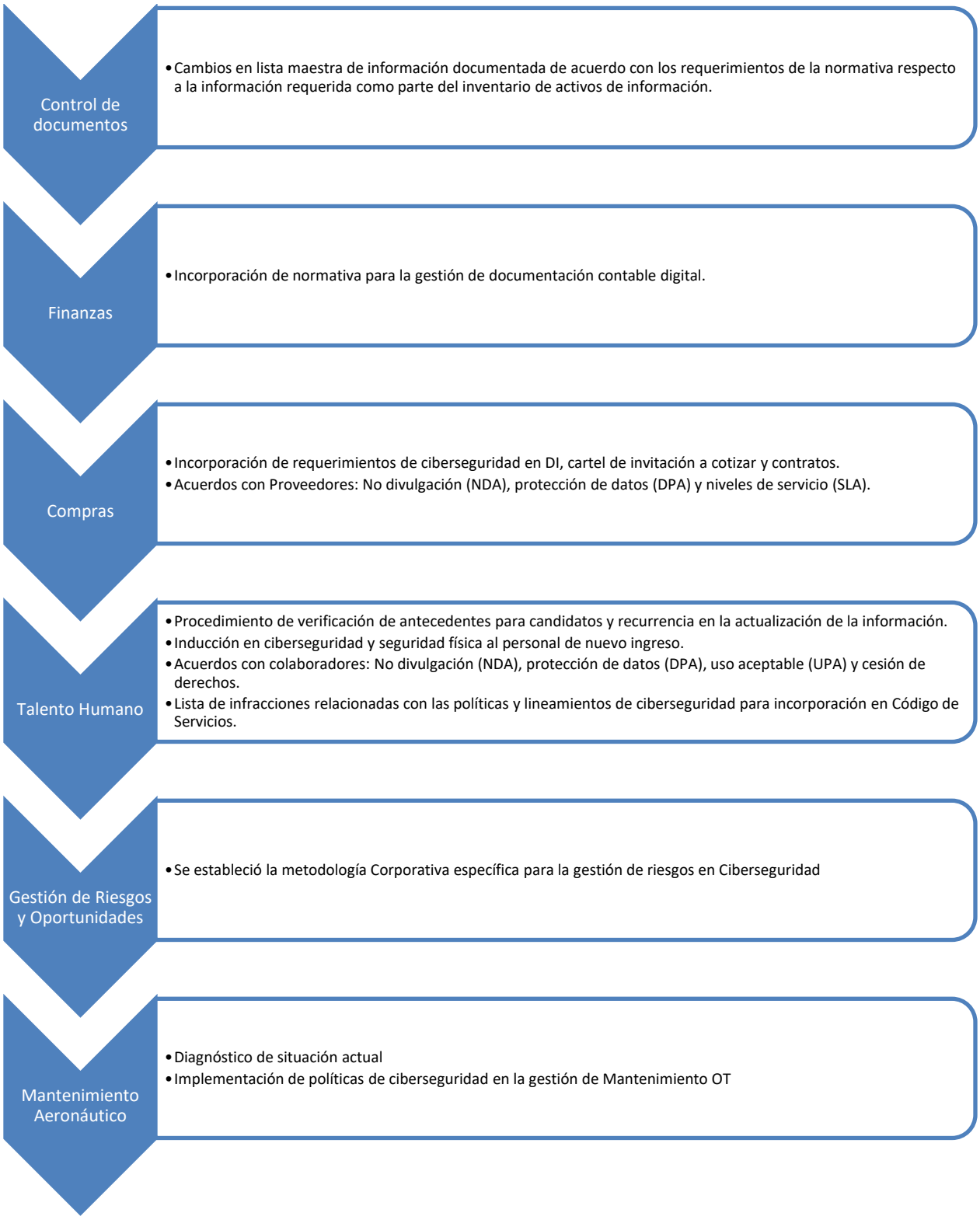

Ilustración 3 - Procesos SGC

iv. **Diagnóstico NIST:** COCESNA realizará una evaluación de la efectividad de los controles implementados para la protección de amenazas cibernéticas contra sistemas críticos, la cual se basa en el marco de gestión del NIST, a través del cual se verificarán los cinco dominios del estándar (Como se muestra en la **Ilustración 4**) con sus respectivos controles.

Ilustración 4 - Marco de ciberseguridad del NIST versión 1.1

- **Identificar:** Definir y documentar los diferentes sistemas que posee la corporación según su criticidad basándose en los datos y funcionamiento de cada uno para la operación y funcionamiento y disponibilidad de las actividades operativas de COCESNA identificando los riesgos de ciberseguridad según acceso, datos, activos y proveedores involucrados.

- **Proteger:** Verificar los niveles de accesos en los diferentes sistemas y las medidas de ciberseguridad implementadas (firewall, WAF, encriptación, entre otros) así como los procesos de mantenimiento, parcheo de sistemas y aplicativos sean ejecutados para contener eventos de ciberseguridad.

- **Detectar:** Validar el monitoreo correcto de todos los sistemas oportunamente y la configuración de las diferentes alertas de toda actividad sospechosa, asegurando que todos los interesados estén informados, validando los marcos normativos de la corporación y mejores prácticas tecnológicas, así como mejoras a nivel de configuración u otros aplicados.

- **Responder:** Investigar sobre los planes de respuestas de los diferentes tipos de incidentes que se tienen mapeados, las actividades que se realizan para prevenir la expansión de un evento mitigando sus efectos y los análisis posteriores con el fin de ejecutar acciones correctivas de mejora continua.

- **Recuperar:** Verificar procesos y procedimientos de recuperación ante incidentes, asegurando la reputación de la corporación.

Para aplicar el formulario de evaluación desarrollado, se incorporará a las visitas de supervisión técnica una actividad relacionada con la validación de la efectividad de los controles de ciberseguridad, para posteriormente modelar los resultados de las verificaciones y las evidencias recolectadas, a fin de establecer un plan de acción con actividades, responsables, recursos e inversiones necesarias para aumentar el nivel de madurez del marco NIST en la Corporación.

d) **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 5**.

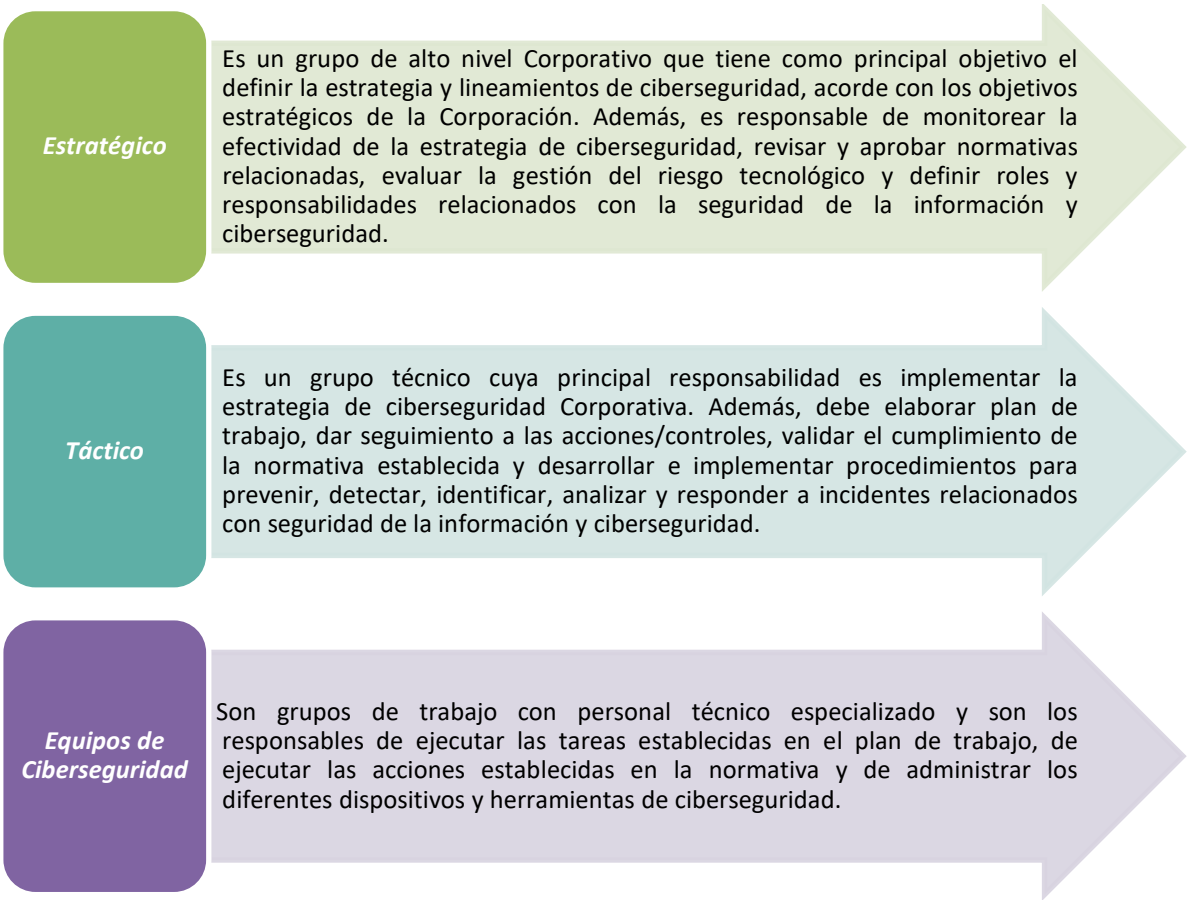

Ilustración 5 - Grupos de Ciberseguridad COCESNA

e) **Formación en Ciberseguridad:** Considerando que la mayoría de los incidentes de ciberseguridad son causados por factores humanos, COCESNA ha identificado la necesidad de capacitar de sus empleados y fortalecer sus ciber competencias con el objetivo de establecer una cultura de ciberseguridad a nivel corporativo, para lo cual se han realizado una serie de actividades tales como:

i. **Socialización**: Inicialmente se socializó el marco regulatorio, con una serie de presentaciones y la participación de todo el personal de la Corporación.

ii. **Boletines**: COCESNA ha implementado comunicados periódicos, presentaciones, charlas y publicaciones en Intranet sobre recomendaciones e indicadores de amenazas en ciberseguridad.

iii. **Concientización en ciberseguridad**: Relacionada con la capacitación del personal de la Corporación, que incluye, entre otras tareas:

- **Inducción**: Nuevo personal, colaboradores actuales, entidades externas, esto incluye el desarrollo de normativa específica relacionada con las actividades de inducción del personal en ciberseguridad;
- **Nivel de formación**: Evaluación permanente de las competencias requeridas en cada puesto de trabajo en el ámbito de la ciberseguridad;
- **Capacitación en Ciberseguridad**: Capacitaciones formales, conferencias, grupos de trabajo, consultas, suscripciones y membresías;

iv. **Cursos personalizados**: COCESNA está en proceso de desarrollar material específico en ciberseguridad y capacitación para fortalecer las habilidades en ciberseguridad de su personal.

La **Ilustración 6** muestra las actividades que COCESNA ha iniciado como parte de la capacitación en Ciberseguridad para lograr una cultura de ciberseguridad a nivel corporativo.

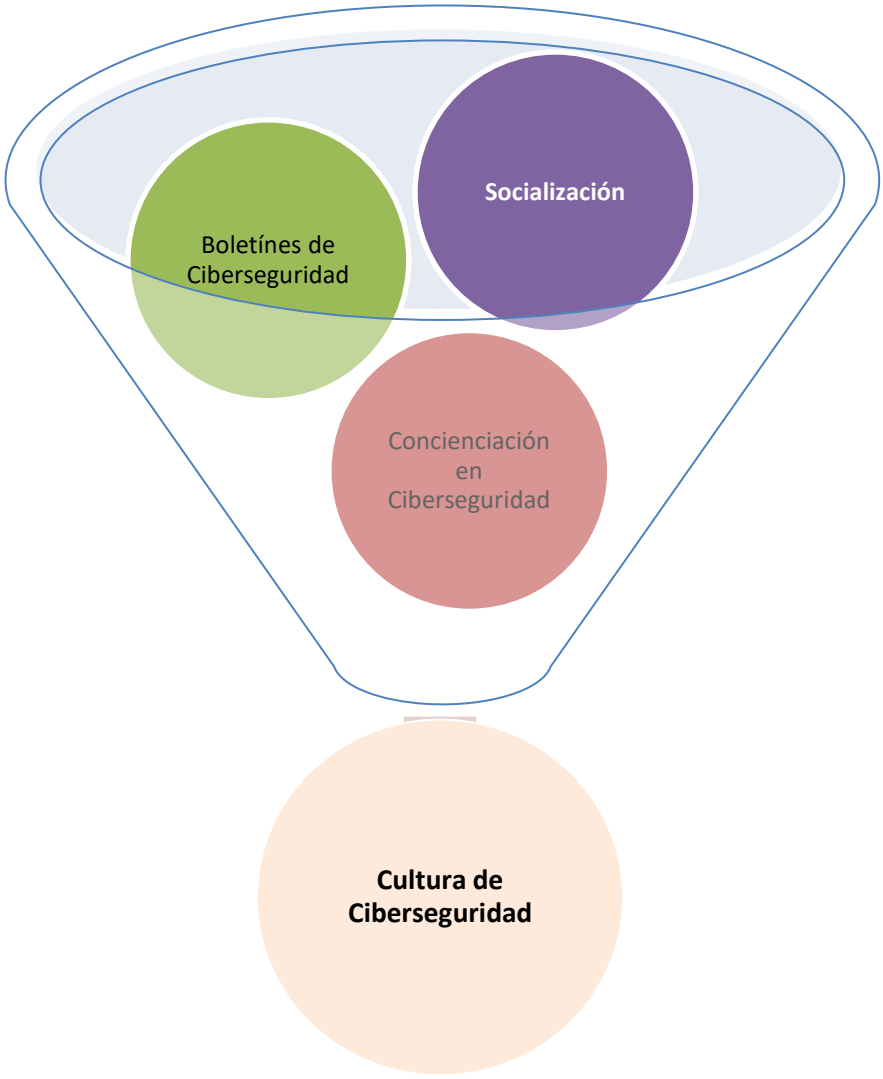

Ilustración 6 - Formación en Ciberseguridad

f) **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:

i. **SOC**: COCESNA está realizando una investigación de mercado para la contratación de servicios de centros de operaciones de ciberseguridad (SOC) para el monitoreo y protección de infraestructuras críticas, atención de incidentes de ciberseguridad y análisis forense.

ii. **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.

iii. **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.

iv. **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.

v. **Modernización de la Plataforma de Comunicación**: Una de las principales iniciativas que COCESNA emprendió a nivel técnico es la actualización de la infraestructura de comunicaciones para brindar servicios de navegación aérea, enfocada especialmente en fortalecer las funcionalidades de ciberseguridad.

La **Ilustración 7** muestra los principales elementos de ciberseguridad a considerar en la modernización de una plataforma de comunicaciones.

Ilustración 7 - Modernización de la Plataforma de Comunicación

vi. **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 8**.

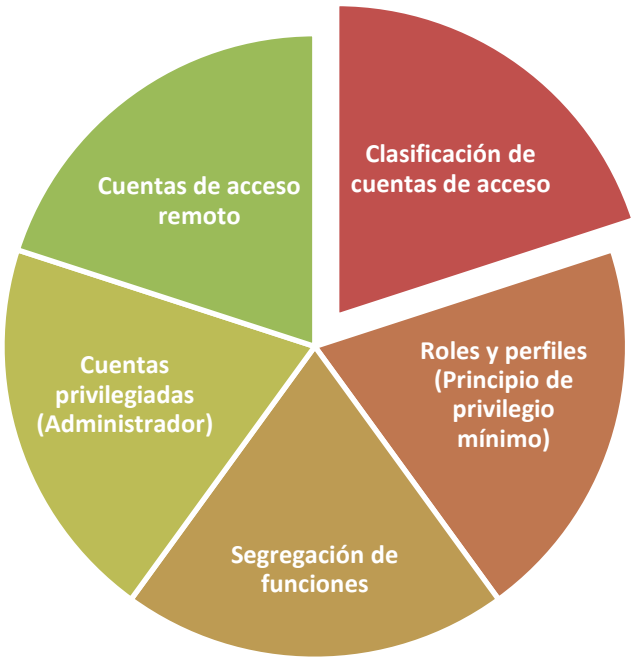

Ilustración 8 - Gestión de Accesos Lógicos en COCESNA

vii. **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.

viii. **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 9** presenta los diversos elementos que se gestionan a través de las mesas de ayuda de COCESNA.

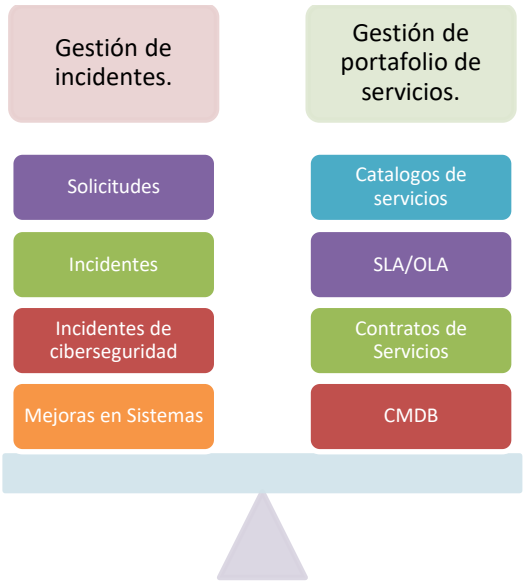

Ilustración 9 - Mesa de Ayuda COCESNA (CATI)

4. Acciones Recomendada:

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

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

— FIN —