CORPORACIÓN CENTROAMERICANA DE SERVICIOS DE NAVEGACIÓN AÉREA (COCESNA)

Gestión de Ciberseguridad COCESNA

CRC-FMTO-006

Presentar las iniciativas emprendidas en COCESNA para el fortalecimiento de la ciberseguridad

OBJETIVO

AGENDA

Gestión de Ciberseguridad Corporativa

- Iniciativas de Ciberseguridad
- Marco Normativo

Gestión de Ciberseguridad - Infraestructura OT

- Actividades de Ciberseguridad OT

Gestión de Ciberseguridad - Infraestructura TI

- Gestión Infraestructura TI
- Servicios TI

COCESNA

TEMA 1:
Gestión de Ciberseguridad Corporativa

Perspectiva Estratégica

COMITÉ ESTRATEGICO

COMITÉ OPERATIVO

Plan Estratégico Corporativo -
OBJETIVO ESTRATEGIO

Fortalecer el posicionamiento como un organismo especializado en la prestación de servicios aeronáuticos a nivel internacional.

OBJETIVO ESPECIFICO

Implementar Ciberseguridad acorde a las buenas prácticas del sector aeronáutico y tecnológico.

ACTIVIDADES ESPECIFICAS

Marco Normativo

a) Alineación de las TIC'S con los objetivos estratégicos y la razón del negocio

b) Promover una Arquitectura TIC integrada, estandarizada, segura, flexible y armonizada

c) Gestionar las TIC'S a nivel corporativo en base al análisis de riesgos y/o su costo beneficio

d) Enfoque en mejora y aprovechamiento de recursos

e) Proveer información segura, confiable e integra para la toma de decisiones

f) Aplicar las Tecnologías de Información y Comunicaciones para la Innovación

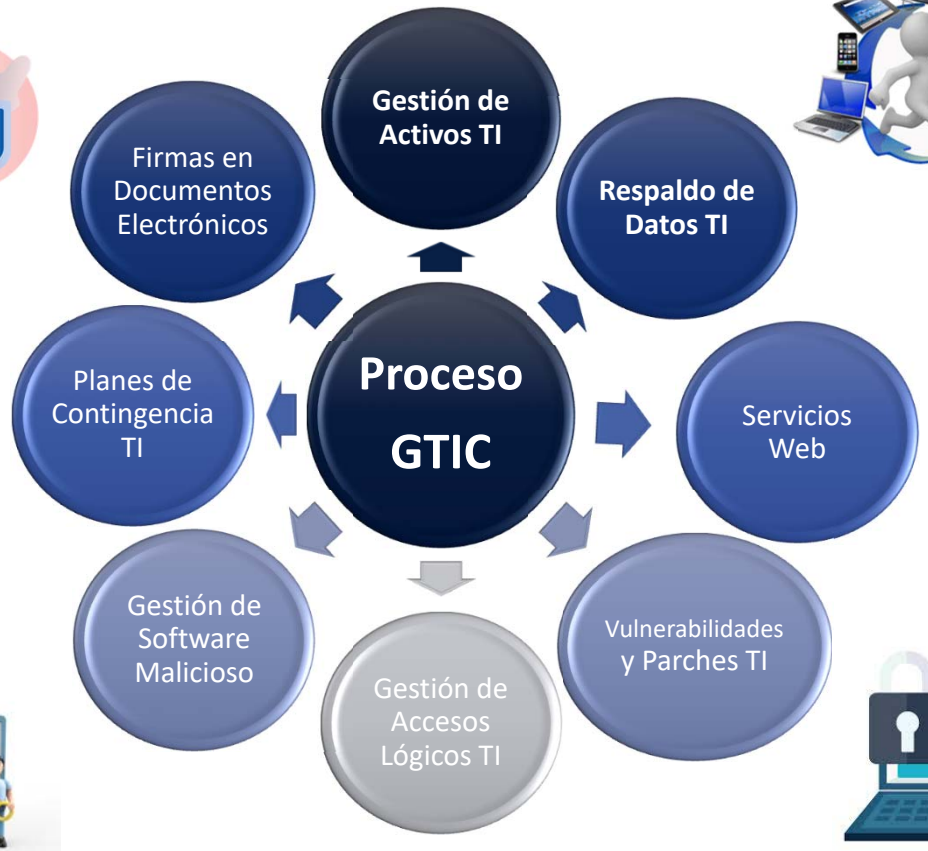
g) Promover una cultura de seguridad de la información y/o ciberseguridad

Principios de las TIC

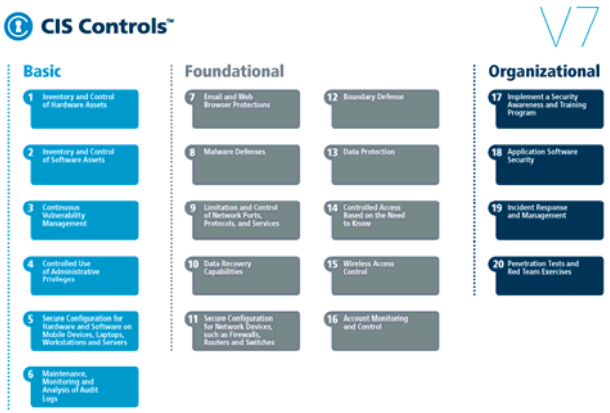
…Marco Normativo

1. Manual de Gestión de Tecnologías de la Información (MGTI)
2. Políticas de Tecnologías de la Información y Ciberseguridad (PTIC)
3. Proceso de Gestión de Tecnologías de la Información y Ciberseguridad (GTIC)

…Marco Normativo



Basados en Normativas Establecidas/ Buenas Practicas



…Marco Normativo

Socialización

- Marco Normativo
- Procesos SGC
  - Control de documentos
  - Finanzas
  - Compras
  - Talento Humano
  - Riesgos
  - Mantenimiento Aeronáutico
  - Seguridad Física

Iniciativas de Ciberseguridad

- Nombramientos GEC y GTC
- CYSECP
- Marco Normativo OACI
- Asistencia Técnica Ciberseguridad Cibernetika/USTDA
- Firma electrónica y Firma Digital
- Acuerdos con Partes interesadas (NDA, DPA, SLA)
- Boletines de Ciberseguridad

TEMA 2:
Gestión de Ciberseguridad Infraestructura OT

COCESNA

Actividades de Ciberseguridad OT

a) Ejecución de Auditorías Externas de Ciberseguridad (INDRA)

b) Cierre de brechas de seguridad detectadas en las Auditorías de Ciberseguridad en conjunto con la Gerencia de Tecnología Informática y proveedores externos

c) Participación en los Grupos Estratégicos y Táctico de Ciberseguridad de Cocesna

d) Análisis de Aplicaciones utilizadas por el personal técnico para brindar mantenimiento de forma remota a los Sistemas CNS/ATM

e) Análisis y Definición de Políticas de Utilización de Dispositivos de Almacenamiento Externo en los Sistemas CNS/ATM

f) Análisis y Establecimiento de Políticas de Ciberseguridad para el Acceso Remoto por parte de Proveedores Externos para labores de Mantenimiento o Monitoreo de los Sistemas CNS/ATM

g) Capacitación e implementación de los Servidores de Password Manager en cada una de las Estaciones Regionales

h) Participación en Webinars y reuniones organizados por la OACI y en el Grupo de la OACI de Ciberseguridad de la Oficina NACC de la OACI.

i) Participación en la Definición de las Especificaciones Técnicas del Proyecto propuesto para ser desarrollado en conjunto con la Universidad de San Diego y la empresa Cibernética para diagnostico y mejora en la Ciberseguridad de COCESNA.

Auditoría Externa de Ciberseguridad Sistemas CNS/ATM

Efectuada en Diciembre 2019
Por Minsait una compañía de Indra

Se utilizó del Marco de Ciberseguridad del NIST

Fuente: Marco Ciberseguridad del NITS.

Auditoría Externa de Ciberseguridad Sistemas CNS/ATM

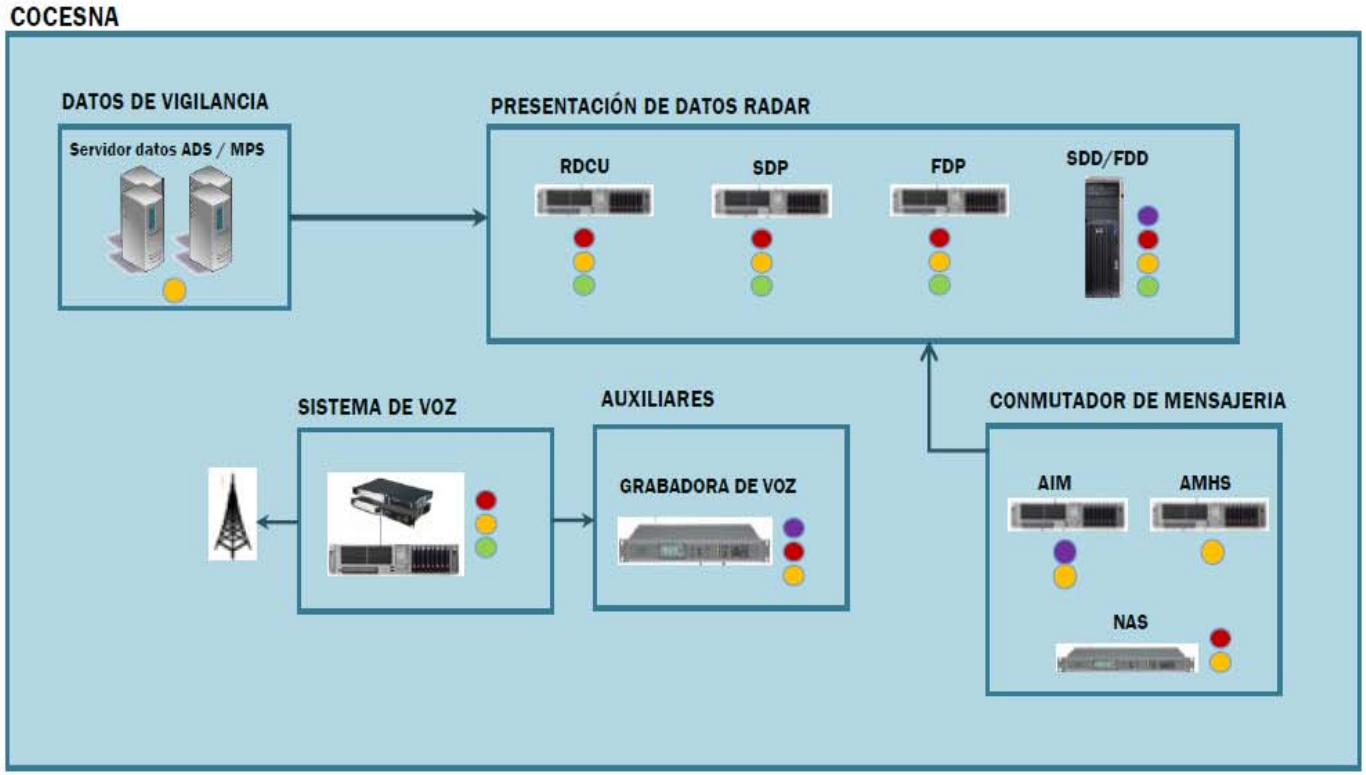
7 Documentos

RESULTADOS GENERALES ETHICAL

- Vulnerabilidades asociadas a usuarios y credenciales por defecto en equipos de red aeronáutica.
- Se encontraron servicios innecesarios activos en dispositivos y servidores que permitiría ver información del equipo

Auditoría Externa de Ciberseguridad Sistemas CNS/ATM

Vulnerabilidades Detectadas en los

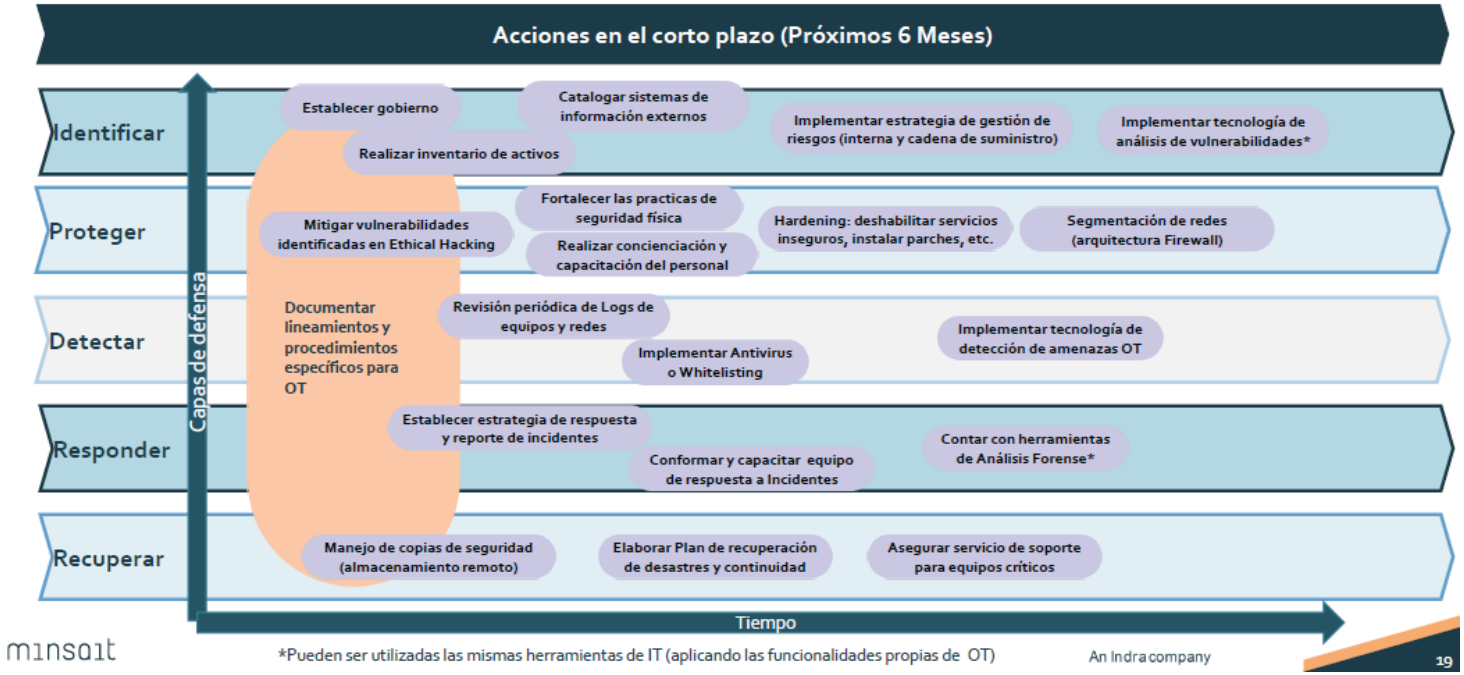


Vulnerabilidades principales:

- Servicios y protocolos inseguros
- Ausencia de parches
- Credenciales por defecto
- Versiones de componentes software inseguros
- Gestión de backups inadecuada
- Usuarios compartidos

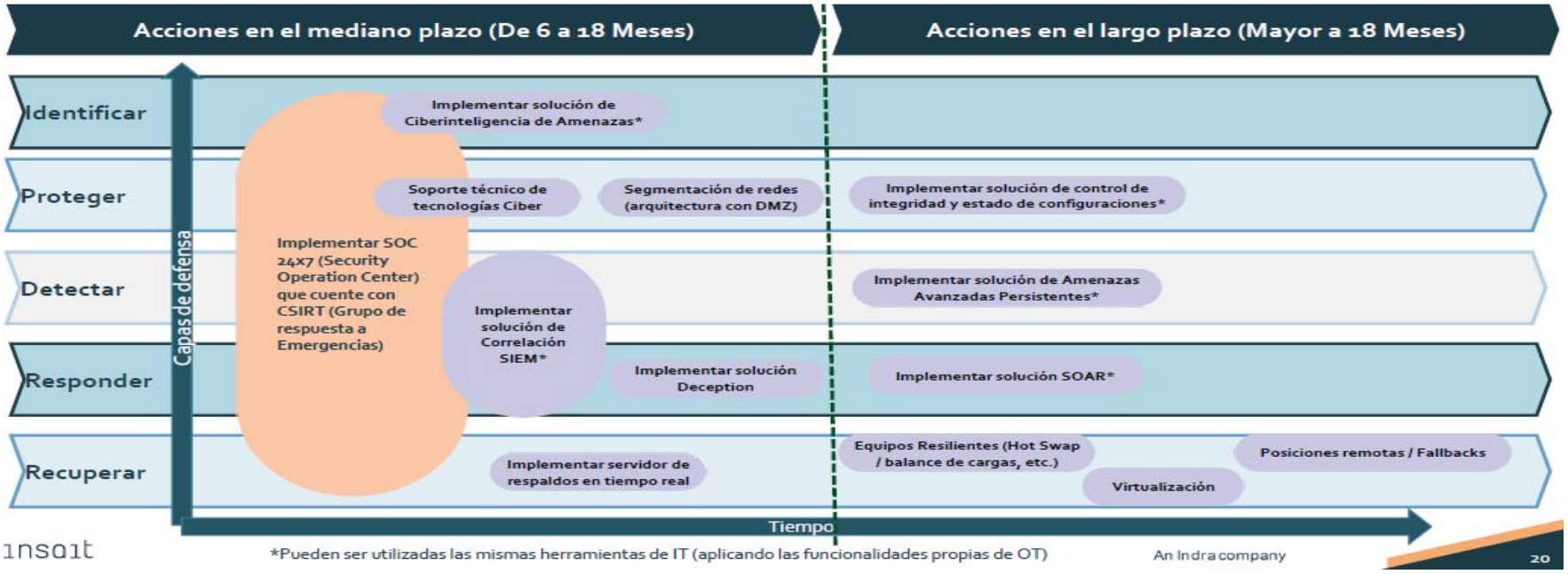
Auditoría Externa de Ciberseguridad Sistemas CNS/ATM

Hoja de Ruta para disminuir el GAP normativa a corto plazo



Auditoría Externa de Ciberseguridad Sistemas CNS/ATM

Hoja de Ruta para disminuir el GAP normative a mediano y largo plazo



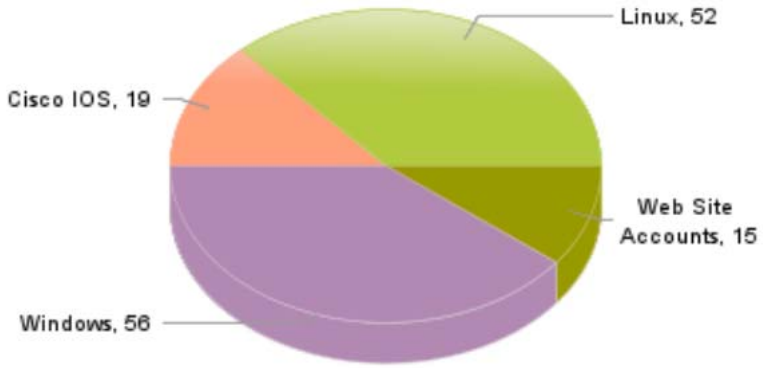
Implementación del Password Manager para accesar los Sistemas CNS/ATM

Se implementó un Servidor de Password Manager en cada una de las Gerencias de Estación para controlar el acceso remoto a los equipos sistemas de Navegación, Comunicaciones, Vigilancia, Automatización, Meteorología, Energía y Sistemas Auxiliares

Ejemplo de Implementación Gerencia de Estación Honduras

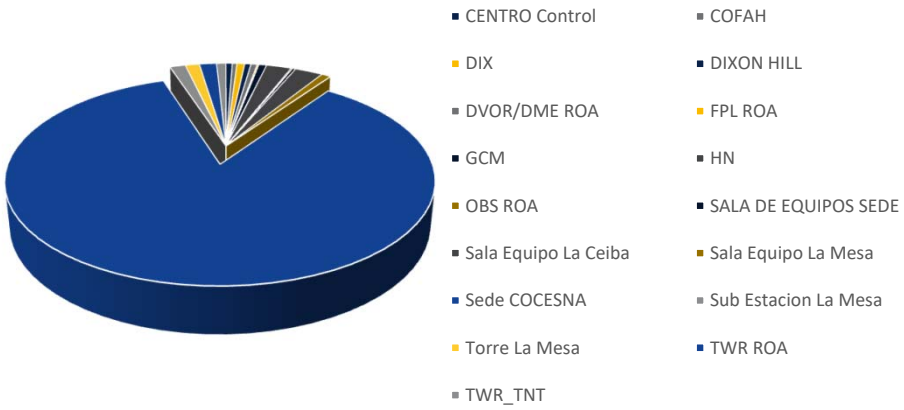
- Cantidad total de recursos : 115
- Número total de contraseñas : 142
- Número total de usuarios : 681
- Cantidad total de tipos de recursos : 83

Distribución de recursos por Sistema Operativo



Implementación del Password Manager para accesar los Sistemas CNS/ATM

Ejemplo de Implementación Gerencia de Estación Honduras



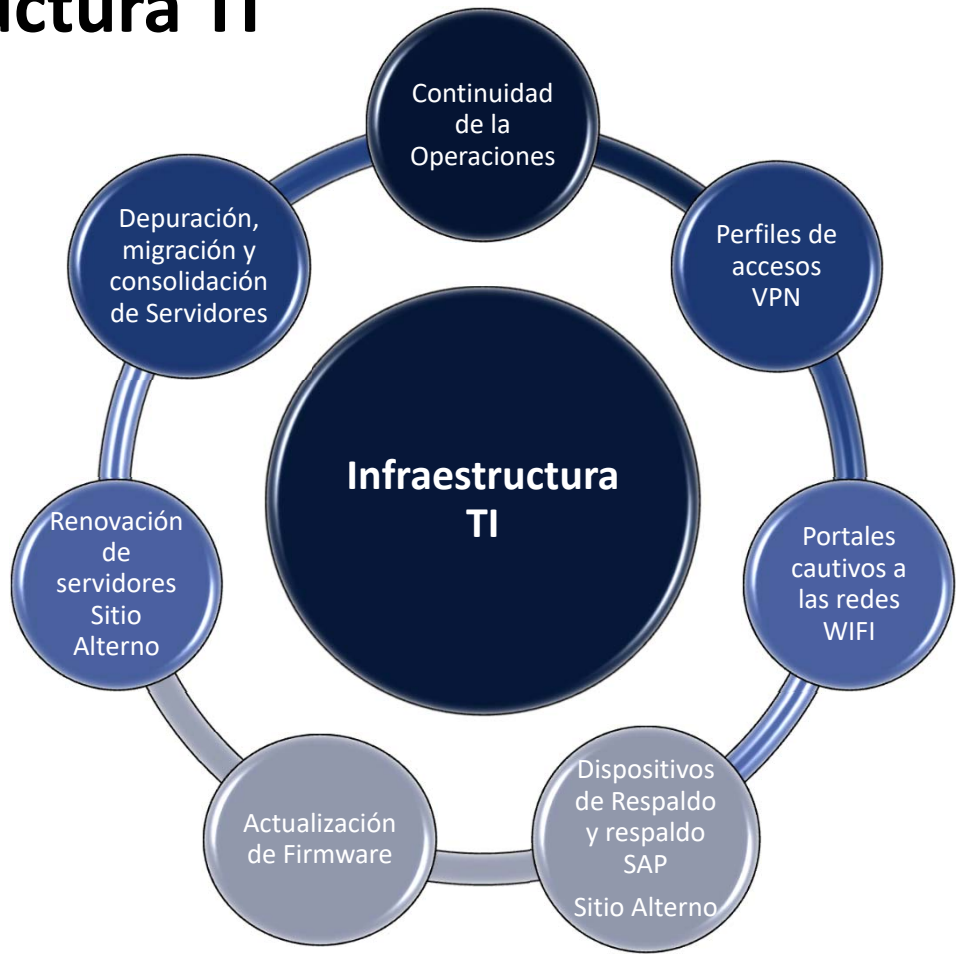
Contraseñas Asignadas por Sitio

Etiquetas de fila	Cuenta de Location
CENTRO Control	4
COFAH	3
DIX	5
DIXON HILL	4
DVOR/DME ROA	4
FPL ROA	1
GCM	5
HN	16
OBS ROA	1
SALA DE EQUIPOS SEDE	2
Sala Equipo La Ceiba	18
Sala Equipo La Mesa	6
Sede COCESNA	605
Sub Estacion La Mesa	10
Torre La Mesa	9
TWR ROA	11
TWR_TNT	6
Total general	**710**

TEMA 3:
Gestión Ciberseguridad Infraestructura TI

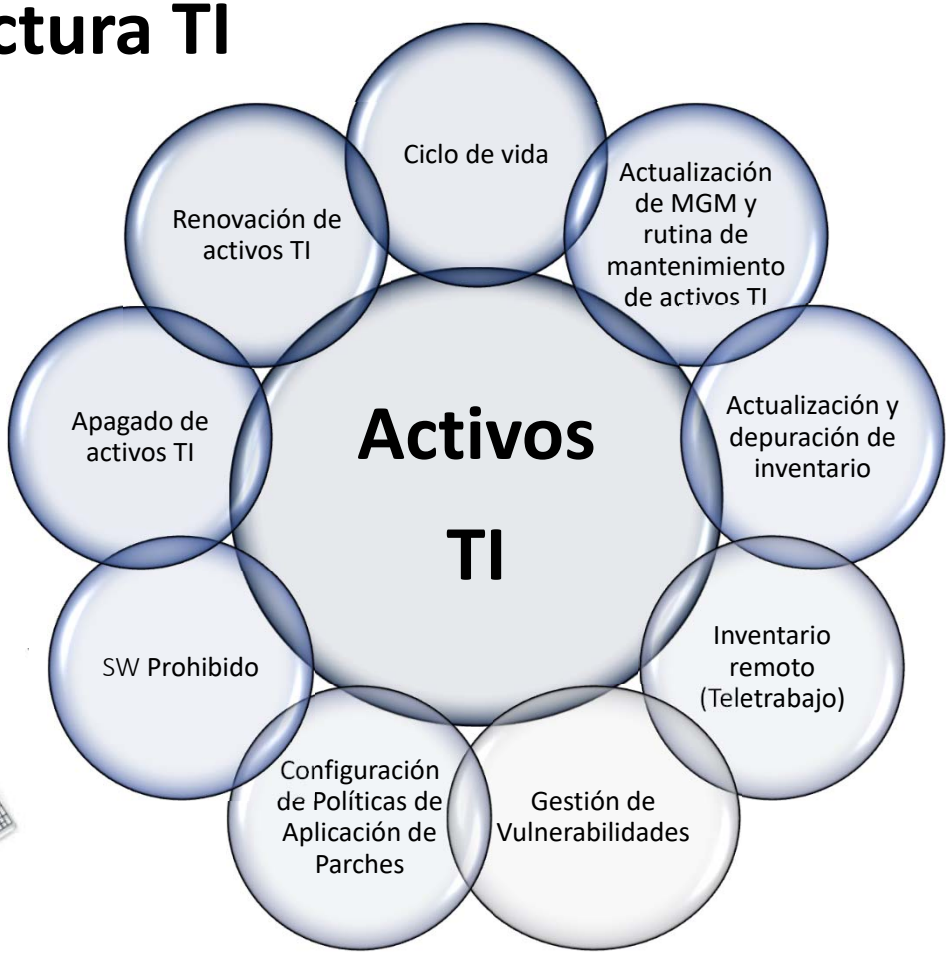
COCESNA

Infraestructura TI



…Infraestructura TI

…Infraestructura TI



…Infraestructura TI

Estadísticas – Métricas

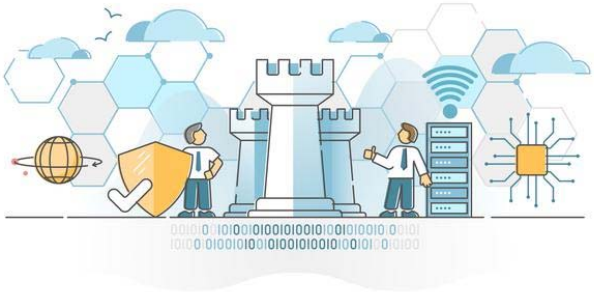
Tráfico	Cantidad de ataques	Aplicaciones peligrosas	Conexión de activos TI	Parches pendientes	Instalación de SW	Alertas O365	Otras Estadísticas

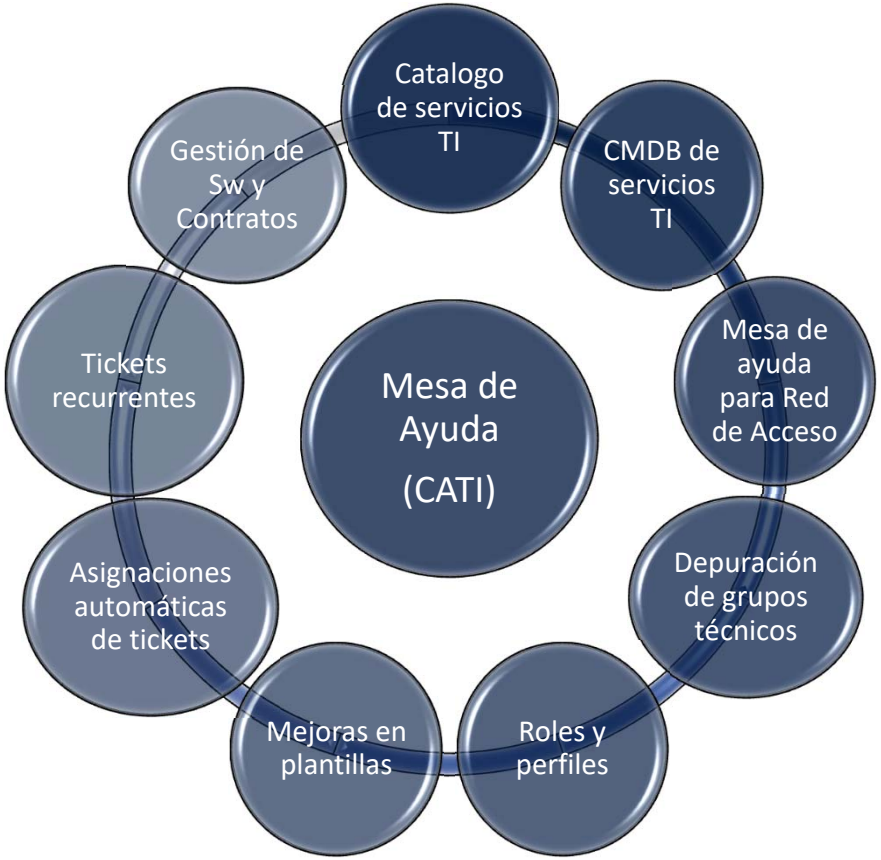
…Infraestructura TI

Infraestructura TI

- Sistemas TI ProVIP, SIAREVO, ERM
- Almacenamiento de documentos de DB
- Migración procesamiento de información Aircon
- Compatibilidad de Sistemas TI con nuevas versiones de SO
- Cluster de almacenamiento Sede
- Incrementos de anchos de banda de Internet
- Enlace de contingencia para Red de Acceso/SNA

…Infraestructura TI



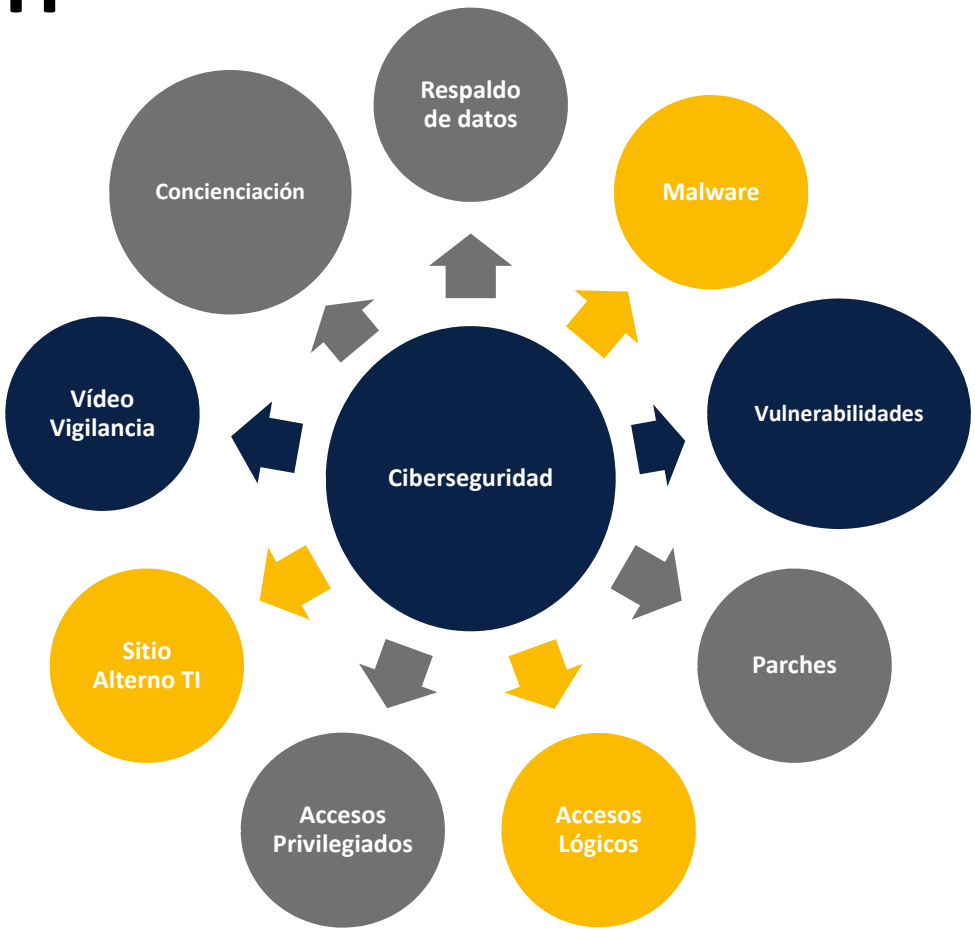


…Infraestructura TI

Servicios Web

- Rutina de publicación de servicios Web
- Nueva página Web
- SW de gestión de documentación digital
- SW de gestión del SGC

Servicios TI



Servicios TI

Comunicación
Gestión de Mantenimiento
Accesos lógicos
Accesos privilegiados (PMP)
Soporte y acceso remoto
Intercambio de información aeronáutica
Alertas automáticas
Mensajería electrónica (Aeronáutica, E-Mail, MI, etc.)
Resguardo de información

Internet (Navegación, VPN, seguridad perimetral)
AD Corporativo
SMTP
Almacenamiento (On Premise y Cloud)
O365
SAP
Aplicaciones Web (WAF, DB, publicación)
Pagina Web
Infraestructura (Servicios y Sistemas TI)
Virtualización
Activos TI
CATI
Ciberseguridad (Malware, vulnerabilidades, parches, accesos privilegiados, respaldo de datos.

COCESNA

Resumen

Resumen

- En esta nueva realidad hiperconectada y con la proliferación exponencial de amenazas cibernéticas, el objetivo de COCESNA como Proveedor de Servicio de Navegación Aérea es de fortalecer sus defensas , perfil y cultura de ciberseguridad para garantizar la seguridad operacional y continuidad del servicio.

- COCESNA continua fortaleciendo la cultura de ciberseguridad en la corporacion mediante la implementacion y seguimiento de una politica de Ciberseguridad con el fin de asegurar la confidencialidad , integridad y disponibilidad de la informacion y bajo una adecuada gestion del riesgo tecnologico .

FIN

¡Muchas Gracias!