 <p>AERONÁUTICA CIVIL UNIDAD ADMINISTRATIVA ESPECIAL</p>	MODELO		
	Título: Seguridad de la Información de la Unidad Administrativa Especial de Aeronáutica Civil.		
	CAPITULO III. ESTANDARES		
Clave: GINF-6.0-21-01	Versión: 02	Fecha: 28/05/2018	Pág.: 1 de 4

ES-09 CONFIGURACIÓN DE SEGURIDAD EQUIPOS ACTIVOS DE RED

1. Normatividad Relacionada

NO-07 Responsabilidad de Usuarios
 NO-11 Administración de Cuentas
 NO-12 Registro de Eventos
 NO-13 Comandos Especiales y Administración de Componentes Tecnológicos
 NO-14 Administración y Configuración de Parámetros de Seguridad
 NO-15 Nombres de Usuario
 NO-16 Usuarios Privilegiados
 NO-17 Usuarios Genéricos
 NO-19 Administración de Accesos a Componentes Tecnológicos
 ES-03 Contraseñas de Acceso
 ES-04 Parámetros de Acceso
 ES-05 Registro de Eventos

2. Objetivos


Establecer los patrones de configuración de seguridad base que deben tener los equipos activos de red LAN/WAN de la UAEAC.

3. Componentes Tecnológicos Afectados

Todos los equipos activos de red LAN/WAN de la UAEAC.


4. Descripción

- Los equipos activos de red LAN/WAN deben tener como mínimo la siguiente configuración:
 - ✓ La contraseña del usuario Administrador debe ser diferente a la que trae por defecto el equipo activo de red.
 - ✓ Cada equipo de red debe tener asignada una dirección IP fija.
 - ✓ Desconexión automática de sesiones de administración de los equipos activos de red inactivas: 30 segundos.
 - ✓ Cualquier cambio en la configuración del dispositivo de red debe ser autorizado aplicando el procedimiento de control de cambios establecidos.
 - ✓ Los registros de eventos y auditoría de las conexiones de administración a los equipos activos de red deben estar habilitados y deben contener como mínimo:
 - Inicio del sistema y terminación

 <p>AERONÁUTICA CIVIL UNIDAD ADMINISTRATIVA ESPECIAL</p>	MODELO			
	Título: Seguridad de la Información de la Unidad Administrativa Especial de Aeronáutica Civil.			
	CAPITULO III. ESTANDARES			
Clave: GINF-6.0-21-01	Versión: 02	Fecha: 28/05/2018	Pág.: 2 de 4	

- Inicio y cierre de sesión
 - Intentos fallidos de conexión
 - Cambios en cuentas locales y privilegios asignados
 - Cambios en el software y la configuración
 - Cambios en el estado de la red y la interfaz
 - Conexiones de red / netflow
 - Importar y exportar datos desde o hacia el equipo de red
 - Reglas de filtrado, si aplica
- ✓ Copia de seguridad (backup) de la configuración: Semanal.
 - ✓ La contraseña de las comunidades SNMP debe ser diferente a la que trae por defecto el equipo.
 - ✓ Cumplir el procedimiento de almacenamiento de contraseñas de administración y contraseñas de comunidades SNMP para ser usadas en caso de emergencia.
 - ✓ Todas las contraseñas almacenadas en equipos de red deben estar encriptadas.
 - ✓ El reloj del dispositivo de red debe estar sincronizado con un servidor NTP.
 - ✓ Deshabilitar el protocolo SNMP (Simple Network Management Protocol), si es necesario, debe utilizarse la última versión y todo el acceso de SNMP debe filtrarse a través de ACL's.
 - ✓ Deshabilitar los servicios innecesarios en los equipos de red. Algunos servicios típicos que se pueden deshabilitar son:
 - CDP (Cisco Discovery Protocol)

CDP es propiedad de Cisco y se usa para identificar dispositivos en un segmento LAN. Se considera un riesgo de seguridad tanto por la información que comparte como por los ataques de denegación de servicio. Si se usa, debe estar deshabilitado en todas las interfaces que no sean de confianza.
 - LLDP (protocolo de descubrimiento de capa de enlace)

 AERONÁUTICA CIVIL UNIDAD ADMINISTRATIVA ESPECIAL	MODELO		
	Título: Seguridad de la Información de la Unidad Administrativa Especial de Aeronáutica Civil.		
	CAPITULO III. ESTANDARES		
Clave: GINF-6.0-21-01	Versión: 02	Fecha: 28/05/2018	Pág.: 3 de 4

LLDP es similar a CDP. Sin embargo, este protocolo permite la interoperabilidad entre otros dispositivos que no son compatibles con CDP. LLDP también se usa para reconocimiento y mapeo de red y se debe tratar de la misma manera que CDP. Deshabilitar LLDP en todas las interfaces que se conectan a redes que no son de confianza.

- Servicios TCP y UDP

Los servicios como: echo, discard, daytime y chargen rara vez se usan y pueden aprovecharse para lanzar ataques de denegación de servicio.

- Finger

Finger es un servicio de búsqueda de usuario remoto que muestra qué usuarios están conectados a un dispositivo. También podría revelar procesos en ejecución. Finger también es vulnerable a ataques de denegación de servicio.

- Servidor IP BOOTP

Un servidor IP BOOTP puede distribuir imágenes del sistema y, por lo tanto, puede ser utilizado para descargar el software del dispositivo. Deshabilitarlo evitará que el dispositivo actúe como servidor BOOTP.

- Servicio de identificación


Identd, identifica la sesión TCP de un usuario. Se puede utilizar para generar una lista de nombres de usuario que pueden ser útiles para un atacante.

- HTTP / HTTPS

Se recomienda utilizar HTTPS para labores de administración, debido a que HTTP envía contraseñas y contenido en texto claro. Si no requiere administración vía Web, deshabilite esta funcionalidad.

- Configuración de inicio remoto

El servicio permite que un dispositivo cargue la configuración desde un servidor TFTP remoto que utiliza protocolos de archivos de transferencia inseguros.

 <p>AERONÁUTICA CIVIL UNIDAD ADMINISTRATIVA ESPECIAL</p>	MODELO		
	Título: Seguridad de la Información de la Unidad Administrativa Especial de Aeronáutica Civil.		
	CAPITULO III. ESTANDARES		
Clave: GINF-6.0-21-01	Versión: 02	Fecha: 28/05/2018	Pág.: 4 de 4

- TFTP

TFTP permite conexiones al dispositivo para transferir archivos. Si se utiliza para instalación por primera vez, se debe enlazar el cliente TFTP a la interfaz de bucle invertido y desactivarlo cuando finalice.

- Telnet

Debe estar deshabilitado debido a que envía información en texto claro.

- DHCP

DHCP (Dynamic Host Configuration Protocol) se utiliza para asignar direccionamiento dinámico. Deshabilitar si no se usa.

- PAD (Packet Assembler/Disassemble)

Es compatible con el ensamblador de paquetes X.25. Deshabilitar si no se usa.