Guía de auditoria para routers Cisco

	Directivas de Contraseña
o	Utilizar contraseñas de “enable” con cifrado md5 enable secret 5 $1$8$KTOREWTlwrewbxAFlbrsWGRm1
o	**Activar el servicio de cifrado** service password-encryption

	Servicios del ruteador
o	**Servicios abiertos** **Objetivo:** Para propósitos de administración mantener activos estos servicios. 2. Snmp 3. tacacs 4. ssh 5. ospf 6. bgp 7. telnet
o	**Servicios que deben deshabilitarse** • cdp • http • bootp • directed broadcast • proxy arp • finger • tcp small servers • udp small servers • source routing

	Registro de sucesos
o	**Configurar la fecha y hora del sistema**
o	**Activar registro de eventos de seguridad localmente** service timestamps log datetime localtime service timestamps debug datetime localtime loggin buffered 10000 **Activar registro de eventos de seguridad a un servidor remoto** **:** 1. En el ruteador loggin IP_servidor loggin facility local1 loggin trap informational

o	loggin buffered 10000

	Control de Acceso
	Control AAA aaa new-model aaa authentication login default tacacs+ enable tacacs-server host *IP-servidor* tacacs-server key *llave*
o	**Autenticación local de usuarios**
o	login authentication default
o	**Autenticación remota de usuarios** login authentication default
o	**Autenticación de superusuario** aaa authentication enable default tacacs+ enable
o	**Niveles de autorización** aaa authorization commands 1 default tacacs+ ok aaa authorization commands 15 default tacacs+ ok
o	**Registro de la actividad de administradores** accounting exec default start-stop tacacs+ ok aaa accounting commands 15 default start-stop tacacs+ ok
o	**Control de conexiones remotas** access-list 1 permit *ip-permitida* access-list 1 permit *ip-permitida* access-list 1 deny any line vty 0 4 access-class 1 in
o	**Control de ruteo** 1. Configurar ACL access-list 100 deny ip 10.0.0.0 0.255.255.255 any access-list 100 deny ip 192.168.0.0 0.0.255.255 any access-list 100 deny ip 172.16.0.0 0.15.255.255 any access-list 100 deny ip 224.0.0.0 15.255.255.255 any access-list 100 deny ip 169.254.0.0 0.0.255.255 any access-list 100 deny ip 127.0.0.0 0.255.255.255 any access-list 100 permit ip any any 2. Aplicar ACL int Serial 0 ip access-group 100 in
o	**Tiempos de conexión** En consola: exec-timeout 15 0 En las vty: exec-timeout 15 0
o	**Monitoreo por SNMPv3** **Objetivo: Monitorer parámetros del ruteador usando snmp version 3** snmp-server group monitor v3 auth read adminview

	snmp-server view adminview internet included snmp-server user monitor monitor v3 encrypted auth md5 password access 40

	Software de seguridad adicional
o	Tacacs+ ok

Otros	
o	ip subnet-zero ok ip cef distributed ok no service pad ok pad ok