

PROCOLO

PROVINCIAL DE CIBERSEGURIDAD

Estándar de IT: Estándar de Seguridad de Red Inalámbrica 802.11

09
CAPÍTULO



Estándar de TI: Estándar de Seguridad de Red Inalámbrica 802.11

1.0 Propósito y Beneficios

El propósito de este estándar es establecer controles para redes inalámbricas 802.11 con el fin de minimizar los riesgos a la confidencialidad, integridad y disponibilidad de la información y para soportar el acceso seguro a recursos y servicios a través de redes inalámbricas.

Las redes inalámbricas 802.11 permiten a los usuarios de dispositivos inalámbricos la flexibilidad de moverse físicamente por un entorno inalámbrico manteniendo la conectividad a la red. Si bien las redes inalámbricas 802.11 están expuestas a muchos de los mismos riesgos que las redes cableadas, también están expuestas a riesgos adicionales exclusivos de las tecnologías inalámbricas. Este estándar describe los controles adicionales necesarios para el uso de redes inalámbricas.

2.0 Alcance

Este estándar se aplica a todas las redes inalámbricas 802.11 que almacenan, procesan, transmiten datos o se conectan a una red o sistema, incluidas las redes administradas y alojadas por terceros en nombre de la organización.

Los tipos de redes inalámbricas 802.11 abarcados incluyen:

- Internas: estas redes inalámbricas están conectadas directamente a los recursos internos de tecnología de la información y solo están disponibles para usuarios autenticados.
- Públicas (autenticadas): estas redes inalámbricas no están conectadas a recursos internos de tecnología de la información y el acceso está limitado a usuarios autenticados.
- Públicas (no autenticadas): estas redes inalámbricas no están conectadas a recursos internos de tecnología de la información y están disponibles para que cualquiera las use sin autenticación.

3.0 Declaración de Información

1. Las redes inalámbricas 802.11 deben seguir todos los requisitos de la Política de seguridad de la información, incluida, entre otras, una evaluación de riesgos antes de la implementación.
2. Todas las instalaciones inalámbricas deberán estar autorizadas por el MPEyM cuyos datos atravesarán la red inalámbrica.
3. La documentación del plan de seguridad, según lo exige el Estándar del ciclo de vida de desarrollo de sistemas seguros, debe incluir, como mínimo, el nombre del departamento, todas las ubicaciones de AP, todas las ubicaciones de infraestructura inalámbrica de soporte, la subred en la red cableada y el identificador de conjunto de servicios (SSID).
4. Los AP y otros dispositivos inalámbricos de soporte deben colocarse en una ubicación físicamente protegida que minimice las oportunidades de robo, daño o acceso no autorizado.
5. Se debe gestionar la cobertura de la red inalámbrica para restringir la capacidad de conectarse fuera de los límites aprobados.
6. El SSID de las redes inalámbricas 802.11 debe, si o si, cambiarse de la configuración predeterminada que tiene de fábrica.
7. El SSID no debe incluir información que indique la ubicación, tecnología o detalles del fabricante de la red inalámbrica (por ejemplo, Server-Rm-WiFi-Access, Wifi-Rm70 y Cisco-2400-WiFi). El SSID tampoco debe incluir información que indique el tipo de datos que atraviesan la red.
8. Se debe utilizar un sistema inalámbrico de detección de intrusos (IDS) en todas las redes inalámbricas internas.
9. Las redes inalámbricas públicas deben estar, como mínimo, separadas física o lógicamente de la red interna o configurada para hacer un túnel hacia un punto final seguro fuera de la red interna. El diseño debe incluirse en el plan de seguridad documentado.
10. Los esquemas de direccionamiento lógico utilizados para la red inalámbrica deben diferir de los utilizados para la red cableada para poder distinguir eficazmente las conexiones de clientes entre las dos redes
11. Si bien se puede acceder a los servidores y recursos compartidos de información a través de una red inalámbrica, no deben conectarse directamente a una red inalámbrica.
12. APs de redes inalámbricas públicas autenticadas o internas deben configurarse para proporcionar la configuración de cifrado más segura disponible.

Como mínimo, se debe utilizar acceso protegido Wi-Fi (WPA) 2 – Estándar de cifrado avanzado (AES).

13. El modo personal WPA2 no debe utilizarse para redes internas.
14. El modo personal WPA2, con el acceso protegido Wi-Fi (WPS) deshabilitado, se puede utilizar para puntos de acceso públicos autenticados que no se conectan a redes internas.
15. Los AP que utilizan frases de contraseña (como los AP configurados para usar el modo personal WPA2) deben usar frases de contraseña que cumplan con el estándar de tokens de autenticación y deben tener al menos 14 caracteres de longitud y cambiarse como mínimo cada seis meses.
16. Las frases de contraseña utilizadas por los AP deben cambiarse desde la configuración predeterminada de fábrica.
17. No se debe poder acceder directamente a la consola de administración de la red inalámbrica desde la red inalámbrica.
18. Se debe utilizar la autenticación 802.1X, específicamente el Protocolo de autenticación extensible (EAP), para todos los dispositivos que se conectan a las redes inalámbricas internas. Los encargados de seguridad deben utilizar el método EAP-TLS siempre que sea posible. No se permite el uso de EAP ligero (LEAP) ni el uso de los siguientes mecanismos de autenticación EAP: EAP-MD5 (resumen de mensajes), EAP-OTP (contraseña de un solo uso) y EAP-GTC (tarjeta token genérica).
19. Los dispositivos cliente inalámbricos que se conectan a redes inalámbricas internas deben configurarse para validar los certificados emitidos por el servidor de autenticación durante el proceso de autenticación.
20. Los dispositivos cliente inalámbricos deben configurarse para utilizar configuraciones de privacidad de identidad durante el proceso de autenticación, cuando sea técnicamente posible.
21. Se requiere autenticación de usuario individual, de acuerdo con el Estándar de token de autenticación, para las redes inalámbricas internas.

4.0 Cumplimiento

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

5.0 Definiciones de términos clave

Término	Definición
WPA	Wi-fi Protected Access, es una tecnología de seguridad para redes del estándar WiFi, desarrollado para sanear las falencias en autenticación y encriptación de WEP.
WPA2	Wi-fi Protected Access 2, es una tecnología de seguridad para redes del estándar WiFi, revisión de la WPA original, creado con el propósito de suplir algunas de las falencias del mismo.
WPA3	Wi-fi Protected Access 2, es una tecnología de seguridad para redes del estándar WiFi, a diferencia de la anterior, registra nuevos dispositivos a través de procesos que no requieren el uso de una contraseña compartida, haciendo uso de código QR o etiquetas NFC, entre otras mejoras de seguridad.
WPS	WiFi Protected Setup, es un estándar de red seguro para la creación de una red doméstica inalámbrica.
WEP	Wired Equivalent Privacy, es un sistema de cifrado para el estándar IEEE 802.11 como protocolo para redes del estándar WiFi, uno de los primeros intentos de brindar confidencialidad en las redes inalámbricas. En desuso por vulnerabilidades de seguridad.
SSID	Service Set Identifier, es la identificación asociada a una red de área local inalámbrica, del estándar WiFi, para que un cliente o usuario pueda diferenciarla de otras.

6.0 Historial de revisiones

Fecha	Descripción de Cambio	Crítico
02/07/2024	Draft final del documento	Alejandro Castro Pablo Zalazar

7.0 Documentos relacionados

Estándar de seguridad para dispositivos móviles

Estándar de cifrado