Módulo 4. Wi-Fi / Red remota con identidad

1. WPA3-EAP-TLS + RADIUS

En las redes inalámbricas empresariales, el control de acceso constituye uno de los elementos más importantes para garantizar la seguridad de la infraestructura. A diferencia de los entornos domésticos, donde la autenticación suele basarse en una contraseña compartida, las organizaciones requieren mecanismos que permitan identificar de manera individual a cada usuario o dispositivo que intenta conectarse a la red. Este control resulta particularmente relevante en entornos donde múltiples equipos, dispositivos móviles y sistemas corporativos acceden simultáneamente a los recursos de la organización.

Los estándares modernos de seguridad inalámbrica incorporan mecanismos que permiten integrar la autenticación de red con sistemas de identidad y con infraestructuras de criptografía de clave pública. En este contexto, el protocolo **WPA3-Enterprise** combinado con el método de autenticación **EAP-TLS** permite implementar modelos de acceso a redes Wi-Fi basados en certificados digitales. Este enfoque elimina la dependencia de contraseñas compartidas y permite establecer un proceso de autenticación mutua entre el dispositivo cliente y el servidor de autenticación de la red.

La autenticación mediante certificados se apoya en una infraestructura de clave pública (*Public Key Infrastructure,* PKI), donde cada dispositivo o usuario posee un certificado digital emitido por una autoridad de certificación confiable. Durante el proceso de conexión, el cliente presenta su certificado al servidor de autenticación, que verifica su validez antes de

conceder acceso a la red. Este mecanismo permite establecer una cadena de confianza entre el dispositivo solicitante, el servidor RADIUS que gestiona la autenticación y la autoridad que emitió el certificado.

Dentro de este modelo, el servidor **RADIUS (Remote Authentication Dial-In User Service)** actúa como un componente central en la arquitectura de autenticación. Este servidor recibe las solicitudes de conexión provenientes de los puntos de acceso inalámbricos, valida la identidad del cliente mediante el protocolo EAP y consulta, cuando corresponde, los sistemas de directorio de la organización para determinar las políticas de acceso aplicables. Además, registra los eventos de autenticación y genera información que puede utilizarse para el monitoreo y la auditoría de accesos a la red.

En esta unidad analizaremos los componentes que permiten implementar redes Wi-Fi empresariales basadas en identidad. En primer lugar, se examinará el uso de certificados digitales para autenticar dispositivos o usuarios en redes WPA3-Enterprise mediante el método EAP-TLS. Luego se estudiará la integración del servidor RADIUS con sistemas de directorio corporativos, que permiten centralizar la gestión de identidades y políticas de acceso. Posteriormente se abordarán los mecanismos de rotación y revocación de certificados dentro de una infraestructura PKI y su impacto en la seguridad de la red inalámbrica. Finalmente, se analizará el papel de los registros de autenticación generados por el servidor RADIUS como herramientas fundamentales para el monitoreo de la actividad de la red y la detección de incidentes de seguridad.

Certificados por dispositivo/usuario.

En las redes inalámbricas empresariales modernas, la autenticación basada en certificados digitales constituye uno de los mecanismos más robustos para controlar el acceso a la infraestructura. A diferencia de los modelos basados en contraseñas compartidas, donde todos los usuarios utilizan una misma clave para conectarse a la red, el uso de certificados permite identificar de manera individual a cada dispositivo o usuario que solicita acceso. Este enfoque resulta especialmente adecuado en entornos corporativos donde múltiples equipos, dispositivos móviles y sistemas automatizados requieren conectividad segura a la red inalámbrica.

El estándar WPA3-Enterprise, combinado con el método de autenticación EAP-TLS (Extensible Authentication Protocol – Transport Layer Security), permite implementar este modelo de acceso basado en identidad criptográfica. En este esquema, cada cliente que intenta conectarse a la red posee un certificado digital emitido por una autoridad de certificación confiable. Durante el proceso de autenticación, el dispositivo presenta su certificado al servidor de autenticación, que verifica su validez antes de permitir el acceso a la red inalámbrica (Aruba Networks, 2023).

El funcionamiento de EAP-TLS se apoya en un proceso de autenticación mutua entre el cliente y el servidor. Esto significa que ambas partes validan su identidad mediante certificados digitales antes de establecer una sesión segura. El cliente verifica que el servidor de autenticación presenta un certificado válido emitido por una autoridad confiable, mientras que el servidor valida el certificado presentado por el dispositivo o usuario que solicita acceso. Este mecanismo reduce significativamente el riesgo de

ataques de suplantación o de interceptación de credenciales durante el proceso de conexión.

En términos operativos, el proceso de autenticación involucra varios componentes que trabajan de manera coordinada dentro de la infraestructura de red. El dispositivo que intenta conectarse a la red inalámbrica actúa como suplicante, mientras que el punto de acceso inalámbrico funciona como intermediario en el proceso de autenticación. El punto de acceso envía la solicitud de autenticación al servidor RADIUS, que es responsable de validar el certificado del cliente y determinar si el acceso debe concederse.

El servidor RADIUS verifica el certificado presentado por el cliente utilizando la información proporcionada por la infraestructura de clave pública de la organización. Esta verificación incluye comprobar que el certificado fue emitido por una autoridad de certificación confiable, que no ha expirado y que no ha sido revocado. Si todas estas condiciones se cumplen, el servidor autoriza al punto de acceso a permitir la conexión del dispositivo a la red (Smallstep, 2023).

El uso de certificados permite implementar distintos modelos de autenticación según las necesidades de la organización. En algunos casos, los certificados se asignan a usuarios individuales, permitiendo identificar a cada persona que accede a la red independientemente del dispositivo que utilice. En otros entornos, los certificados se emiten directamente a dispositivos específicos, lo que permite controlar qué equipos están autorizados para conectarse a la infraestructura inalámbrica. Esta flexibilidad permite adaptar las políticas de acceso a distintos escenarios operativos.

En organizaciones donde se utilizan dispositivos corporativos administrados, el modelo de certificados por dispositivo facilita la implementación de políticas de seguridad centralizadas. Los equipos pueden recibir automáticamente certificados durante el proceso de provisión del dispositivo, lo que permite que se autentiquen de forma transparente al conectarse a la red. Este enfoque elimina la necesidad de que los usuarios introduzcan credenciales manualmente y reduce el riesgo de exposición de contraseñas.

Otro aspecto relevante del uso de certificados en redes Wi-Fi empresariales es la posibilidad de integrar el proceso de autenticación con sistemas de gestión de identidades o con plataformas de administración de dispositivos. Cuando el certificado del dispositivo se vincula con la identidad del usuario o con la política de seguridad del equipo, el sistema puede aplicar reglas de acceso más precisas basadas en la identidad y el estado del dispositivo.

El uso de EAP-TLS también contribuye a proteger el proceso de autenticación frente a ataques comunes en redes inalámbricas, como el robo de credenciales o los intentos de suplantación de puntos de acceso. Debido a que el proceso de autenticación se basa en certificados digitales y en el establecimiento de un canal TLS seguro, los atacantes no pueden capturar contraseñas reutilizables ni interceptar credenciales que puedan ser utilizadas posteriormente.

Sin embargo, la implementación de este modelo requiere comprender adecuadamente la cadena de confianza que interviene en el proceso de autenticación. Cada certificado presentado por un cliente debe poder verificarse mediante una autoridad de certificación reconocida por el servidor de autenticación. Esta cadena de confianza garantiza que los certificados utilizados dentro de la red provienen de una fuente confiable y que los

dispositivos que los presentan han sido previamente autorizados por la organización.

Comprender esta cadena de confianza resulta fundamental para diseñar infraestructuras Wi-Fi seguras basadas en identidad. Cuando los certificados se gestionan correctamente, el sistema puede identificar con precisión qué dispositivo o usuario intenta acceder a la red y aplicar las políticas de seguridad correspondientes. Este enfoque establece las bases para otros mecanismos de gestión del ciclo de vida de los certificados, como su rotación periódica y su revocación en caso de pérdida o compromiso del dispositivo, aspectos que se analizarán en los apartados siguientes de la unidad.

Integraciones con directorios

En las infraestructuras de red empresariales, la autenticación de los dispositivos que intentan conectarse a la red inalámbrica no suele gestionarse de manera aislada. En la mayoría de las organizaciones, los sistemas de autenticación se integran con directorios corporativos, donde se almacenan las identidades de usuarios, dispositivos y grupos organizacionales. Esta integración permite centralizar la administración de identidades y aplicar políticas de acceso coherentes en diferentes servicios de la infraestructura tecnológica.

En entornos que utilizan autenticación **WPA3-Enterprise con EAP-TLS**, el servidor RADIUS actúa como intermediario entre la red inalámbrica y los sistemas de identidad de la organización. Cuando un dispositivo solicita acceso a la red, el punto de acceso transmite la solicitud de autenticación al servidor RADIUS, que valida el certificado presentado por el cliente. Una vez verificada la autenticación criptográfica, el servidor puede consultar un directorio corporativo para determinar las políticas de autorización asociadas a la identidad del usuario o del dispositivo.

Los directorios corporativos suelen implementarse mediante servicios basados en el protocolo **LDAP (Lightweight Directory Access Protocol)** o mediante plataformas de gestión de identidades como **Active Directory.** Estos sistemas almacenan información estructurada sobre los usuarios de la organización, incluyendo identificadores, pertenencia a grupos, atributos organizacionales y políticas de acceso. La integración entre el servidor RADIUS y el directorio permite utilizar esta información para definir qué recursos de red puede utilizar cada identidad autenticada (FreeRADIUS, 2024).

Cuando un servidor RADIUS se integra con un directorio LDAP o con Active Directory, el proceso de autenticación puede incluir varias etapas de verificación. En primer lugar, el sistema valida el certificado presentado por el cliente mediante la infraestructura de clave pública. Luego, el servidor consulta el directorio corporativo para comprobar si la identidad asociada al certificado corresponde a un usuario o dispositivo autorizado dentro de la organización. Finalmente, el sistema aplica las políticas de acceso definidas para esa identidad, que pueden incluir restricciones de red, asignación de segmentos específicos o control del tipo de recursos accesibles.

Esta integración permite que la red inalámbrica forme parte del mismo ecosistema de identidad utilizado por otros servicios de la organización, como aplicaciones empresariales, sistemas de correo electrónico o plataformas de acceso remoto. De esta manera, los administradores pueden gestionar identidades desde un único repositorio y aplicar políticas coherentes en distintos componentes de la infraestructura tecnológica.

Otro aspecto relevante de la integración con directorios es la posibilidad de utilizar **grupos organizacionales** para definir políticas de acceso diferenciadas. En muchos entornos empresariales, los usuarios se agrupan según su rol dentro de la organización, su departamento o el tipo de dispositivo que utilizan. El servidor RADIUS puede consultar estos grupos durante el proceso de autenticación y aplicar configuraciones de red específicas según la pertenencia del usuario a determinados grupos.

Por ejemplo, un dispositivo perteneciente al personal administrativo puede recibir acceso a segmentos de red distintos a los asignados a equipos de visitantes o dispositivos de laboratorio. Estas políticas permiten aplicar el principio de segmentación de red y limitar el acceso de cada usuario únicamente a los recursos necesarios para su actividad.

La integración con directorios también facilita la administración del ciclo de vida de las identidades dentro de la red. Cuando un usuario se incorpora a la organización, su identidad puede registrarse en el directorio corporativo y asociarse a un certificado que permitirá la autenticación en la red inalámbrica. De manera similar, cuando un usuario abandona la organización o cambia de función, las políticas de acceso pueden modificarse directamente en el directorio sin necesidad de reconfigurar individualmente cada componente de la red.

Además de facilitar la administración, esta arquitectura permite mejorar la trazabilidad de los accesos a la red. Los registros generados por el servidor RADIUS pueden incluir información proveniente del directorio corporativo, como el identificador del usuario o el grupo al que pertenece. Esta información resulta útil para el monitoreo de la actividad de la red y para la investigación de incidentes de seguridad.

Desde una perspectiva operativa, la correcta integración entre el servidor RADIUS y los sistemas de directorio requiere configurar adecuadamente los conectores de autenticación y los atributos utilizados durante el proceso de consulta. Los administradores deben definir qué atributos del directorio se utilizarán para identificar al usuario o dispositivo, así como las reglas que determinan qué políticas de red se aplicarán en cada caso. Una configuración incorrecta puede provocar errores de autenticación o asignaciones de acceso inconsistentes dentro de la red.

En conjunto, la integración con directorios constituye un componente fundamental en la arquitectura de redes Wi-Fi empresariales basadas en identidad. Al vincular la autenticación criptográfica proporcionada por EAP-TLS con la información almacenada en los sistemas de identidad corporativos, las organizaciones pueden implementar mecanismos de control de acceso más precisos, administrar identidades de manera centralizada y aplicar políticas de seguridad coherentes en toda la infraestructura de red. Esta integración también establece las bases para gestionar de manera efectiva el ciclo de vida de los certificados y las

identidades, aspectos que se analizarán en los próximos apartados de la unidad.

Rotación y revocación

En las redes inalámbricas empresariales que utilizan autenticación basada en certificados, la seguridad del sistema depende en gran medida de la correcta gestión del **ciclo de vida de los certificados digitales.** Estos certificados permiten identificar de forma criptográfica a los dispositivos o usuarios que acceden a la red, pero su validez no es permanente. Para mantener la integridad de la infraestructura de autenticación, las organizaciones deben aplicar mecanismos de r**otación periódica y revocación de certificados**, que permitan renovar las credenciales antes de su expiración y retirar inmediatamente aquellas que ya no deben ser consideradas confiables.

El ciclo de vida de un certificado dentro de una infraestructura de clave pública (*Public Key Infrastructure*, PKI) incluye varias etapas: emisión, distribución, uso, renovación y revocación. Durante la emisión, una autoridad de certificación genera un certificado digital que vincula una identidad —como un usuario o un dispositivo— con una clave pública. Este certificado se instala posteriormente en el dispositivo cliente y se utiliza durante el proceso de autenticación EAP-TLS para demostrar su identidad ante el servidor RADIUS (IETF, RFC 5280).

La **rotación de certificados** consiste en reemplazar los certificados existentes por otros nuevos antes de que alcancen su fecha de expiración. Este proceso forma parte de las prácticas habituales de gestión de seguridad en infraestructuras PKI. Al limitar el período de validez de los certificados, las organizaciones reducen el tiempo durante el cual una credencial

comprometida podría ser utilizada por un actor malicioso. Además, la rotación periódica permite actualizar parámetros criptográficos y aplicar políticas de seguridad más recientes sin interrumpir el funcionamiento del sistema de autenticación.

En entornos empresariales, la rotación de certificados suele automatizarse mediante sistemas de gestión de identidades o plataformas de administración de dispositivos. Estos sistemas pueden generar nuevas solicitudes de certificado, distribuir las credenciales actualizadas a los dispositivos y retirar las versiones anteriores sin requerir intervención manual de los usuarios. La automatización del proceso reduce errores de configuración y facilita la administración de grandes volúmenes de dispositivos conectados a la red.

La **revocación de certificados**, por su parte, se aplica cuando una credencial deja de ser confiable antes de alcanzar su fecha de expiración. Esto puede ocurrir en situaciones como la pérdida o robo de un dispositivo, la detección de un compromiso de credenciales o la finalización de la relación laboral de un usuario. En estos casos, el certificado asociado a la identidad afectada debe marcarse como inválido dentro de la infraestructura PKI para evitar que continúe siendo utilizado durante el proceso de autenticación.

La revocación se gestiona mediante mecanismos definidos dentro de los estándares de certificación digital. Uno de los métodos tradicionales consiste en utilizar l**istas de revocación de certificados** (*Certificate Revocation Lists*, CRL), que contienen un registro de los certificados que han sido anulados por la autoridad de certificación. Los servidores de autenticación consultan estas listas durante el proceso de validación para comprobar si el certificado presentado por el cliente se encuentra revocado.

Otro mecanismo utilizado en infraestructuras modernas es el **Online Certificate Status Protocol (OCSP).** En este modelo, el servidor de autenticación consulta en tiempo real el estado de un certificado mediante un servicio que responde si la credencial es válida, revocada o desconocida. Este enfoque permite obtener información más actualizada sobre el estado de los certificados y reduce la dependencia de listas de revocación que deben actualizarse periódicamente.

Comprender la diferencia entre CRL y OCSP resulta importante para evaluar el comportamiento del sistema ante incidentes de seguridad. Mientras que las listas de revocación pueden presentar retrasos entre la revocación del certificado y su distribución a los sistemas de validación, los mecanismos basados en OCSP permiten verificar el estado del certificado en tiempo real. La elección entre ambos métodos depende de las características de la infraestructura PKI y de los requisitos operativos de la organización.

En el contexto de redes Wi-Fi empresariales, la correcta gestión de la revocación resulta especialmente relevante cuando un dispositivo autorizado se pierde o es robado. Si el certificado instalado en ese dispositivo continúa siendo válido, el equipo podría seguir autenticándose en la red inalámbrica incluso si el acceso al sistema operativo está protegido por un mecanismo de bloqueo local. Por esta razón, las políticas de seguridad recomiendan revocar inmediatamente los certificados asociados a dispositivos comprometidos para impedir su utilización en el proceso de autenticación de red.

Además de prevenir accesos no autorizados, la revocación de certificados también contribuye a mantener la integridad de la cadena de confianza utilizada durante la autenticación EAP-TLS. Cuando el servidor RADIUS valida el certificado presentado por un cliente, no sólo verifica su firma criptográfica y su fecha de expiración, sino también su estado dentro de la infraestructura

PKI. Esta verificación asegura que únicamente los certificados activos y autorizados puedan utilizarse para acceder a la red.

En conjunto, los mecanismos de rotación y revocación constituyen elementos fundamentales para mantener la seguridad de las redes inalámbricas basadas en autenticación por certificados. Al gestionar adecuadamente el ciclo de vida de las credenciales digitales, las organizaciones pueden garantizar que los dispositivos autorizados mantengan acceso legítimo a la infraestructura mientras que las credenciales comprometidas o obsoletas se eliminan del sistema de autenticación. Estos procesos también facilitan la administración segura de grandes entornos de dispositivos conectados y preparan la infraestructura para registrar y analizar los eventos de autenticación generados durante el funcionamiento de la red.

Figura 1: Buenas prácticas para la gestión de certificados en redes Wi-Fi empresariales

Fuente: elaboración propia.

Log de autenticación

En las redes inalámbricas empresariales basadas en autenticación mediante **WPA3-Enterprise y EAP-TLS,** el registro de eventos de autenticación constituye un componente fundamental para el monitoreo de la seguridad de la infraestructura. Cada intento de conexión a la red genera información que permite reconstruir el proceso de autenticación, identificar el origen de las solicitudes de acceso y detectar comportamientos que puedan indicar incidentes de seguridad. Estos registros se conocen como **logs de autenticación** y forman parte del funcionamiento normal del servidor RADIUS.

Cuando un dispositivo intenta conectarse a una red inalámbrica protegida mediante autenticación 802.1X, el punto de acceso envía la solicitud al servidor RADIUS para su validación. Durante este proceso, el servidor registra distintos eventos asociados a la autenticación, incluyendo el identificador del cliente, la dirección MAC del dispositivo, la dirección IP del punto de acceso que originó la solicitud, el resultado del proceso de autenticación y la marca temporal del evento. Esta información permite comprender cómo se produjo

cada intento de acceso y facilita el análisis posterior de la actividad de la red (Cisco, 2016).

Los registros generados por el servidor RADIUS pueden incluir tanto eventos de autenticación exitosa como intentos fallidos de conexión. Los eventos exitosos indican que el certificado presentado por el cliente fue validado correctamente y que el servidor autorizó al punto de acceso a permitir la conexión del dispositivo. Por el contrario, los registros de autenticación fallida pueden reflejar diversos tipos de problemas, como certificados expirados, certificados revocados, errores en la cadena de confianza o intentos de acceso por parte de dispositivos no autorizados.

El análisis de estos registros permite a los administradores de red identificar situaciones anómalas que podrían indicar intentos de compromiso de la infraestructura. Por ejemplo, múltiples intentos fallidos de autenticación desde un mismo dispositivo o desde una misma dirección MAC pueden señalar configuraciones incorrectas o posibles intentos de acceso indebido. Del mismo modo, la aparición de solicitudes de autenticación provenientes de dispositivos desconocidos puede indicar la presencia de equipos no autorizados intentando conectarse a la red.

Además de su utilidad para la detección de incidentes, los logs de autenticación permiten reconstruir la actividad de la red en caso de que se produzca un evento de seguridad. Si se detecta un dispositivo comprometido o un comportamiento anómalo dentro de la infraestructura, los registros del servidor RADIUS pueden utilizarse para identificar cuándo se produjo la autenticación, desde qué punto de acceso se realizó la conexión y qué identidad se utilizó durante el proceso. Esta información resulta fundamental para llevar adelante investigaciones técnicas y comprender el alcance de un incidente.

La calidad y el nivel de detalle de los registros generados por el servidor RADIUS dependen en gran medida de la configuración aplicada en el sistema. En algunos entornos, los registros pueden limitarse a indicar si la autenticación fue aceptada o rechazada. Sin embargo, en infraestructuras empresariales se recomienda habilitar registros más detallados que incluyan información sobre el proceso de negociación del protocolo EAP, la validación del certificado y los atributos utilizados durante la autorización del acceso. Estos registros detallados facilitan el diagnóstico de problemas y permiten identificar con mayor precisión el origen de los eventos de autenticación.

Los logs de autenticación también pueden integrarse con sistemas de monitoreo y análisis de seguridad, como plataformas de **Security Information and Event Management (SIEM).** Estos sistemas recopilan eventos provenientes de distintos componentes de la infraestructura tecnológica y permiten correlacionar la información generada por el servidor RADIUS con registros de otros sistemas de la organización. Al combinar estas fuentes de información, los equipos de seguridad pueden obtener una visión más completa del comportamiento de la red y detectar patrones de actividad que podrían pasar desapercibidos si se analizaran los registros de forma aislada.

Otro aspecto importante en la gestión de logs de autenticación es la capacidad de conservar los registros durante períodos de tiempo adecuados. Mantener un historial de eventos permite analizar tendencias de acceso, identificar cambios en el comportamiento de los dispositivos y disponer de información relevante para auditorías de seguridad. Las políticas de retención de registros suelen definirse en función de los requisitos operativos de la organización y de las normativas aplicables en materia de seguridad de la información.

En la práctica, una configuración insuficiente de los registros de autenticación puede dificultar significativamente la investigación de incidentes de seguridad. Si el servidor RADIUS no registra información suficiente sobre las solicitudes de acceso, los administradores pueden encontrar dificultades para determinar qué dispositivo intentó conectarse, qué certificado fue utilizado o desde qué punto de acceso se originó la conexión. Por esta razón, las buenas prácticas de administración recomiendan configurar los sistemas de autenticación de manera que generen registros completos y detallados del proceso de autenticación.

En conjunto, los logs de autenticación constituyen una herramienta fundamental para el monitoreo de redes Wi-Fi empresariales basadas en autenticación por certificados. Al registrar de manera sistemática los eventos generados durante el proceso de autenticación, el servidor RADIUS proporciona información valiosa para el diagnóstico de problemas, la detección de incidentes y la mejora continua de las políticas de seguridad aplicadas a la infraestructura inalámbrica. Estos registros también desempeñan un papel clave en los procesos de respuesta a incidentes, que serán analizados en la siguiente unidad de la lectura.

Tips para administrar autenticación Wi-Fi basada en certificados

- **Verificar la cadena de confianza** entre el cliente, el servidor RADIUS y la autoridad de certificación antes de

habilitar el acceso a la red.

- **Asignar certificados individuales a dispositivos o usuarios,** evitando el uso de credenciales compartidas en la infraestructura inalámbrica.
- **Revocar inmediatamente los certificados** de dispositivos reportados como extraviados o comprometidos.
- **Configurar registros detallados en el servidor RADIUS** para identificar intentos de autenticación y posibles incidentes.
- **Revisar periódicamente los logs de autenticación** para detectar comportamientos anómalos o patrones de acceso inusuales.

CONTINUAR

2. Casos y respuestas

En las infraestructuras de red basadas en autenticación por identidad, los mecanismos de seguridad no se limitan únicamente a verificar quién puede acceder a la red. También resulta necesario contar con procedimientos que permitan **responder de manera adecuada cuando se produce un incidente de seguridad** o cuando una credencial de acceso deja de ser confiable. Las redes inalámbricas empresariales que utilizan autenticación basada en certificados y control de acceso mediante servidores RADIUS requieren mecanismos que permitan identificar rápidamente situaciones anómalas y aplicar acciones correctivas para proteger la infraestructura.

En entornos donde múltiples dispositivos y usuarios acceden a la red mediante credenciales digitales, pueden presentarse distintos escenarios que afectan la seguridad del sistema. Entre ellos se encuentran el compromiso de credenciales, la pérdida o robo de dispositivos autorizados, la necesidad de invalidar sesiones activas o la detección de comportamientos sospechosos en los registros de autenticación. Cada uno de estos escenarios requiere procedimientos específicos que permitan limitar el impacto del incidente y restablecer las condiciones normales de operación de la red.

Las arquitecturas modernas de seguridad recomiendan que las organizaciones dispongan de **procedimientos de respuesta estructurados**, que definan cómo actuar ante distintos tipos de incidentes relacionados con el acceso a la red. Estos procedimientos suelen incluir mecanismos para revocar credenciales comprometidas, aislar dispositivos afectados, invalidar

sesiones activas y analizar los registros generados por los sistemas de autenticación. La aplicación sistemática de estos procesos permite reducir el tiempo de exposición ante un incidente y minimizar los riesgos asociados a accesos no autorizados.

Los sistemas de autenticación basados en certificados facilitan la aplicación de estas medidas porque permiten gestionar de forma centralizada la validez de las credenciales utilizadas por los dispositivos. Cuando se detecta que una credencial puede haber sido comprometida, la organización puede revocar el certificado correspondiente dentro de la infraestructura de clave pública y evitar que el dispositivo continúe autenticándose en la red. Este mecanismo permite retirar rápidamente el acceso a dispositivos o usuarios afectados sin necesidad de modificar la configuración general de la infraestructura.

Además de las acciones técnicas aplicadas durante un incidente, los procesos de respuesta también incluyen la **documentación y análisis posterior de los eventos**. Registrar qué ocurrió, cómo se detectó el incidente y qué medidas se adoptaron permite mejorar los procedimientos de seguridad y fortalecer la capacidad de respuesta de la organización ante situaciones similares en el futuro. Estos procesos forman parte de los marcos de gestión de incidentes utilizados en seguridad de la información (ISO/IEC 27035-2, 2023).

En esta unidad se analizarán distintos escenarios relacionados con la seguridad de redes inalámbricas y el acceso a recursos mediante identidades digitales. En primer lugar, se examinará el impacto que puede tener el compromiso de credenciales de autenticación dentro de una infraestructura de red. Luego se abordará la

gestión de incidentes asociados a la pérdida o robo de dispositivos autorizados. Posteriormente se analizarán los mecanismos que permiten invalidar sesiones activas o tokens de autenticación cuando se detecta un riesgo de seguridad. Finalmente, se estudiará la elaboración de informes de incidente y la implementación de planes de mejora orientados a fortalecer las políticas de seguridad de la red.

Compromiso de credenciales.

En las infraestructuras de red que utilizan autenticación basada en identidad, la protección de las credenciales constituye uno de los elementos más importantes para preservar la seguridad del sistema. Las credenciales permiten demostrar que un usuario o dispositivo posee autorización para acceder a la red o a determinados recursos. Cuando estas credenciales se ven comprometidas, existe la posibilidad de que un actor no autorizado utilice esa identidad para obtener acceso a la infraestructura tecnológica de la organización.

El compromiso de credenciales puede producirse por diversas causas. En algunos casos, el problema se origina en el robo o filtración de información de autenticación, como contraseñas o tokens. En otros escenarios, el acceso indebido puede ocurrir cuando un dispositivo autorizado es utilizado por una persona no autorizada. También es posible que un atacante obtenga acceso a credenciales mediante técnicas de ingeniería social o mediante el uso de software malicioso instalado en el dispositivo del usuario.

En redes inalámbricas que utilizan autenticación mediante certificados digitales, el compromiso de credenciales puede manifestarse de forma diferente a los entornos basados en contraseñas. En estos sistemas, la identidad del dispositivo o del usuario se encuentra vinculada a un certificado digital que se utiliza durante el proceso de autenticación EAP-TLS. Si un atacante logra acceder al dispositivo que contiene el certificado o si obtiene una copia de la credencial privada asociada a ese certificado, podría intentar utilizarla para autenticarse en la red (NIST, 2023).

La detección temprana de un posible compromiso de credenciales resulta fundamental para limitar el impacto de un incidente de seguridad. Los sistemas de monitoreo de red y los registros generados por el servidor RADIUS pueden proporcionar indicios sobre actividades anómalas asociadas a una identidad específica. Por ejemplo, intentos de autenticación desde ubicaciones inusuales, cambios en el patrón de conexión de un dispositivo o múltiples intentos de autenticación fallidos pueden indicar que una credencial está siendo utilizada de forma indebida.

Cuando existe sospecha de compromiso de credenciales, las organizaciones deben aplicar procedimientos de respuesta que permitan restringir inmediatamente el acceso asociado a la identidad afectada. En el caso de redes basadas en certificados, una de las medidas más importantes consiste en **revocar el certificado digital** asociado al dispositivo o usuario comprometido. Al revocar el certificado dentro de la infraestructura de clave pública, el servidor de autenticación dejará de aceptar esa credencial durante el proceso de autenticación.

Además de la revocación del certificado, también pueden aplicarse otras medidas complementarias para proteger la infraestructura. Estas medidas pueden incluir el bloqueo temporal de la identidad asociada en el sistema de

directorio, la invalidación de sesiones activas relacionadas con esa credencial y la revisión de los registros de autenticación para identificar accesos que se hayan producido durante el período de compromiso.

Las buenas prácticas de seguridad recomiendan que las organizaciones dispongan de procedimientos claramente definidos para gestionar este tipo de incidentes. Estos procedimientos deben establecer cómo detectar posibles compromisos de credenciales, qué acciones deben realizar los administradores de red y cómo comunicar el incidente dentro de la organización. La existencia de protocolos claros permite actuar con mayor rapidez y reducir el tiempo durante el cual un atacante podría utilizar credenciales comprometidas.

Otro aspecto importante en la gestión de incidentes relacionados con credenciales consiste en analizar el origen del compromiso. En algunos casos, el problema puede estar relacionado con la configuración de los dispositivos utilizados por los usuarios, con la falta de actualizaciones de seguridad o con la instalación de aplicaciones que pueden exponer información sensible. Analizar estas causas permite identificar medidas preventivas que reduzcan la probabilidad de incidentes similares en el futuro.

Los lineamientos de seguridad para la gestión de dispositivos móviles en entornos empresariales también recomiendan implementar controles adicionales que permitan proteger las credenciales almacenadas en los dispositivos. Entre estas medidas se incluyen el uso de mecanismos de cifrado del almacenamiento, la protección mediante autenticación local del dispositivo y la utilización de sistemas de gestión de dispositivos que permitan aplicar políticas de seguridad de manera centralizada (NIST SP 800-124 Rev. 2).

Finalmente, la respuesta a un compromiso de credenciales debe incluir actividades de monitoreo posteriores al incidente. Una vez revocada la credencial afectada y restablecido el acceso mediante nuevas credenciales seguras, resulta necesario observar el comportamiento de la red para verificar que no se produzcan nuevos intentos de acceso indebido asociados a la identidad comprometida. Este seguimiento permite confirmar que las medidas adoptadas han sido efectivas y que la infraestructura de autenticación continúa funcionando de manera segura.

En conjunto, el compromiso de credenciales representa uno de los escenarios de riesgo más relevantes en sistemas de autenticación basados en identidad. La capacidad de detectar rápidamente este tipo de incidentes, revocar las credenciales afectadas y aplicar medidas correctivas adecuadas constituye un elemento fundamental para proteger la infraestructura de red y preservar la integridad de los sistemas de autenticación utilizados por la organización.

Dispositivo extraviado/robo

En las infraestructuras de red que utilizan autenticación basada en certificados y control de acceso mediante identidad, la pérdida o el robo de un dispositivo autorizado constituye un escenario que requiere una respuesta inmediata. Los dispositivos utilizados por los usuarios suelen contener credenciales de autenticación, certificados digitales o tokens que permiten acceder a la red inalámbrica y a otros servicios corporativos. Cuando un

equipo se extravía o es sustraído, existe la posibilidad de que estas credenciales sean utilizadas por personas no autorizadas para intentar acceder a la infraestructura de la organización.

En redes inalámbricas basadas en autenticación **WPA3-Enterprise con EAP-TLS,** los dispositivos autorizados poseen certificados digitales que permiten demostrar su identidad durante el proceso de autenticación. Aunque estos certificados suelen almacenarse de forma segura dentro del sistema operativo del dispositivo, su presencia implica que el equipo puede autenticarse automáticamente en la red si continúa siendo considerado válido dentro de la infraestructura de autenticación. Por esta razón, la pérdida de un dispositivo autorizado debe tratarse como un incidente de seguridad potencial.

Una de las primeras medidas que deben aplicarse cuando se reporta la pérdida o el robo de un dispositivo consiste en **revocar el certificado asociado a ese equipo** dentro de la infraestructura de clave pública de la organización. Al revocar el certificado, el servidor RADIUS dejará de aceptar esa credencial durante el proceso de autenticación EAP-TLS. Esta acción evita que el dispositivo pueda continuar conectándose a la red inalámbrica incluso si el atacante logra acceder al sistema operativo del equipo.

La revocación del certificado debe complementarse con otras acciones de seguridad orientadas a proteger los recursos de la organización. Entre estas acciones puede incluirse la eliminación del dispositivo de los sistemas de gestión de dispositivos corporativos, la desactivación de la cuenta de usuario asociada en el directorio corporativo o la invalidación de sesiones activas que puedan haberse iniciado desde el equipo extraviado. Estas medidas permiten reducir el riesgo de que el dispositivo sea utilizado para acceder a otros sistemas o servicios dentro de la infraestructura.

Las recomendaciones de seguridad para dispositivos móviles en entornos empresariales también destacan la importancia de implementar mecanismos de protección local en los equipos utilizados por los usuarios. Entre estos mecanismos se incluyen el uso de bloqueos de pantalla mediante contraseñas o biometría, el cifrado del almacenamiento interno del dispositivo y la posibilidad de realizar **borrado remoto de información** cuando el equipo se pierde o es robado. Estas medidas contribuyen a proteger los datos almacenados en el dispositivo y dificultan el acceso no autorizado a las credenciales almacenadas en el sistema (NIST SP 800-124 Rev. 2).

Sin embargo, confiar únicamente en los mecanismos de protección local del dispositivo no resulta suficiente para garantizar la seguridad de la infraestructura de red. Incluso si el dispositivo se encuentra protegido mediante un sistema de bloqueo, el certificado instalado en el equipo puede seguir siendo considerado válido por el servidor de autenticación mientras no haya sido revocado dentro de la infraestructura PKI. Por esta razón, las políticas de seguridad recomiendan que la revocación de certificados sea una de las primeras acciones aplicadas cuando un dispositivo autorizado se pierde o es sustraído.

Además de las medidas técnicas orientadas a bloquear el acceso del dispositivo, también resulta importante registrar el incidente dentro de los sistemas de gestión de seguridad de la organización. Documentar cuándo se reportó la pérdida del dispositivo, qué credenciales estaban asociadas al equipo y qué acciones se realizaron para mitigar el riesgo permite mantener un historial claro del incidente. Esta información puede resultar útil para analizar patrones de seguridad y mejorar los procedimientos de respuesta ante incidentes similares en el futuro.

En algunos casos, el análisis posterior del incidente puede revelar la necesidad de fortalecer las políticas de seguridad relacionadas con la administración de dispositivos. Por ejemplo, las organizaciones pueden decidir reducir el período de validez de los certificados instalados en los dispositivos, mejorar los procesos de monitoreo de autenticación o implementar controles adicionales que verifiquen el estado de seguridad del equipo antes de permitir su conexión a la red.

La gestión adecuada de incidentes relacionados con dispositivos extraviados o robados también contribuye a preservar la integridad de la cadena de confianza utilizada en el proceso de autenticación de la red. Al revocar rápidamente las credenciales asociadas a los dispositivos comprometidos, la organización garantiza que únicamente los equipos autorizados y bajo control continúen formando parte de la infraestructura de autenticación.

En conjunto, la pérdida o robo de un dispositivo autorizado representa un escenario que requiere acciones coordinadas entre los sistemas de gestión de identidades, la infraestructura PKI y los mecanismos de administración de dispositivos. La capacidad de revocar rápidamente las credenciales asociadas al equipo, proteger la información almacenada en el dispositivo y documentar adecuadamente el incidente constituye un elemento fundamental para mantener la seguridad de redes inalámbricas basadas en autenticación por certificados.

Tabla 1: Acciones rápidas ante incidentes de autenticación

Escenario	Acción inmediata	Acción complementaria
Compromiso de credenciales	Revocar certificado o credencial	Analizar logs de autenticación
Dispositivo extraviado	Revocar certificado del dispositivo	Borrado remoto y bloqueo de identidad
Sesión comprometida	Cierre de sesión forzado	Renovación de tokens
Acceso sospechoso	Revisar registros RADIUS	Ajustar políticas de monitoreo

Fuente: elaboración propia.

Cierre de sesión forzado/tokens

En las infraestructuras de autenticación modernas, el control del acceso a los recursos no se limita al momento en que el usuario se autentica en el sistema. Una vez completado el proceso de autenticación, los sistemas suelen **generar sesiones activas o tokens de acceso** que permiten al usuario interactuar con aplicaciones, servicios de red o recursos corporativos sin repetir el proceso de autenticación en cada solicitud. Estos mecanismos mejoran la experiencia de uso y reducen la carga sobre los sistemas de autenticación, pero también introducen la necesidad de gestionar adecuadamente la validez de estas sesiones cuando se detecta un incidente de seguridad.

Los **tokens de autenticación** representan credenciales temporales que confirman que un usuario o dispositivo ya ha sido autenticado por el sistema. Estos tokens pueden adoptar distintas formas según el tipo de servicio utilizado. En aplicaciones web, por ejemplo, es común utilizar tokens de sesión o tokens firmados digitalmente que permiten verificar la identidad del usuario durante la interacción con el sistema. En otros entornos, los tokens pueden formar parte de sistemas de autenticación federada o de mecanismos de autorización utilizados por diferentes servicios dentro de la infraestructura.

Cuando ocurre un incidente de seguridad —como el compromiso de credenciales o la pérdida de un dispositivo— puede resultar necesario **invalidar las sesiones activas asociadas a una identidad**. Si una sesión permanece activa después de que se ha detectado un problema de seguridad, el sistema podría seguir permitiendo el acceso a recursos incluso después de que se hayan tomado medidas como la revocación de credenciales o el bloqueo de la cuenta. Por esta razón, los sistemas de autenticación deben incorporar mecanismos que permitan finalizar las sesiones activas de manera controlada.

El **cierre de sesión forzado** consiste en invalidar las sesiones activas asociadas a un usuario o dispositivo antes de que finalice su período normal de validez. Esta acción puede realizarse desde los sistemas de gestión de identidad, desde las aplicaciones que gestionan las sesiones o desde herramientas de administración de seguridad que controlan el acceso a los recursos de la organización. Cuando una sesión se invalida, el sistema exige que el usuario vuelva a autenticarse antes de permitir nuevas interacciones con los servicios protegidos.

En infraestructuras que utilizan autenticación basada en certificados y control de acceso mediante servidores RADIUS, el cierre de sesión forzado puede aplicarse junto con otras medidas de seguridad. Por ejemplo, cuando se revoca el certificado de un dispositivo o se bloquea una identidad dentro del directorio corporativo, también puede ser necesario invalidar las sesiones activas que se hayan establecido previamente mediante esa identidad. Esta acción garantiza que los accesos previamente autorizados no continúen activos después de que la credencial haya dejado de ser confiable.

Las recomendaciones de seguridad relacionadas con la gestión de sesiones destacan la importancia de establecer **políticas claras sobre la duración y renovación de los tokens de autenticación.** Los tokens con períodos de validez excesivamente largos pueden aumentar el riesgo de que una sesión comprometida continúe siendo utilizada durante un período prolongado. Por esta razón, las buenas prácticas de seguridad recomiendan limitar la duración de las sesiones y exigir nuevas verificaciones de identidad cuando el usuario intenta acceder a recursos sensibles o cuando la sesión permanece activa durante un período prolongado (OWASP, 2023).

Otra práctica común consiste en utilizar **tokens de corta duración combinados con mecanismos de renovación controlada.** En este modelo, el sistema emite tokens válidos durante intervalos de tiempo limitados y exige que el usuario obtenga nuevos tokens mediante procesos de autenticación o verificación adicionales. Este enfoque reduce el impacto potencial de un token comprometido, ya que su período de validez se encuentra restringido.

Los sistemas de autenticación también pueden aplicar políticas que finalicen automáticamente las sesiones cuando se detectan cambios en el contexto del acceso. Por ejemplo, un cambio en la dirección IP del dispositivo, el uso de

un nuevo dispositivo o la detección de comportamientos inusuales pueden activar mecanismos que obliguen al usuario a autenticarse nuevamente. Estas medidas permiten reforzar el control de acceso cuando las condiciones de la sesión cambian de manera significativa.

Desde una perspectiva operativa, la capacidad de invalidar sesiones activas resulta especialmente importante durante la respuesta a incidentes de seguridad. Cuando se detecta una credencial comprometida o un dispositivo potencialmente comprometido, la organización debe asegurarse de que todas las sesiones activas asociadas a esa identidad se cierren de inmediato. Esta acción evita que un atacante pueda continuar utilizando el acceso previamente autorizado después de que se hayan aplicado otras medidas de protección.

En conjunto, la gestión de sesiones y tokens constituye un componente esencial dentro de los sistemas modernos de autenticación y control de acceso. La capacidad de limitar la duración de las sesiones, renovar los tokens de manera controlada e invalidar accesos activos cuando se detectan incidentes permite reforzar la seguridad de la infraestructura y reducir el impacto de credenciales comprometidas o dispositivos extraviados. Estos mecanismos forman parte de los procedimientos de respuesta a incidentes que permiten a las organizaciones mantener el control sobre el acceso a sus sistemas y recursos digitales.

Informe y plan de mejora.

En los procesos de respuesta a incidentes de seguridad, las acciones técnicas aplicadas durante la contención del problema representan sólo una parte del proceso de gestión del incidente. Una vez que el acceso no autorizado ha sido bloqueado o que las credenciales comprometidas han sido revocadas, resulta necesario realizar un análisis estructurado del incidente que permita comprender qué ocurrió, cómo se detectó el evento y qué medidas pueden adoptarse para reducir la probabilidad de que situaciones similares vuelvan a producirse. Este proceso se formaliza mediante la elaboración de un informe de incidente y la definición de un plan de mejora.

El informe de incidente constituye un documento que registra de manera detallada la información relevante sobre el evento de seguridad. En este documento se describen los sistemas afectados, el momento en que se detectó el incidente, las evidencias disponibles y las acciones realizadas por el equipo técnico para contener la situación. La elaboración de este informe permite conservar un registro claro de lo ocurrido y facilita la comunicación del incidente dentro de la organización.

En entornos donde la autenticación de red se basa en certificados y servidores de autenticación como RADIUS, el informe suele apoyarse en la información obtenida de los registros de autenticación y de los sistemas de monitoreo de seguridad. Estos registros permiten identificar qué dispositivo o identidad intentó conectarse a la red, desde qué punto de acceso se originó la conexión y qué tipo de evento se registró durante el proceso de autenticación. Analizar esta información permite reconstruir la secuencia de eventos que condujo al incidente.

La documentación del incidente también debe incluir una descripción de las medidas aplicadas para mitigar el riesgo. Estas medidas pueden abarcar la

revocación de certificados comprometidos, la invalidación de sesiones activas, el bloqueo de identidades dentro del sistema de directorio o la eliminación de dispositivos dentro de los sistemas de administración corporativos. Registrar estas acciones permite verificar que las medidas adoptadas fueron suficientes para restablecer la seguridad del sistema.

Una vez finalizada la etapa de documentación, las organizaciones suelen realizar un análisis posterior del incidente orientado a identificar oportunidades de mejora en la infraestructura de seguridad. Este análisis busca comprender qué factores permitieron que el incidente se produjera y qué cambios podrían implementarse para fortalecer los controles existentes. Los marcos de gestión de incidentes recomiendan que este análisis forme parte de un proceso continuo de mejora de la seguridad organizacional (ISO/IEC 27035-2, 2023).

El plan de mejora que surge de este análisis puede incluir distintas medidas según la naturaleza del incidente. En algunos casos, las organizaciones pueden decidir reforzar las políticas de autenticación o modificar la configuración de los sistemas de monitoreo para detectar eventos sospechosos con mayor rapidez. En otros casos, puede resultar necesario actualizar los procedimientos de administración de certificados o mejorar los mecanismos de registro de eventos dentro del servidor de autenticación.

En el contexto de redes inalámbricas empresariales, el análisis posterior de incidentes puede revelar la necesidad de mejorar la gestión del ciclo de vida de los certificados o de fortalecer los controles asociados a los dispositivos utilizados por los usuarios. Por ejemplo, un incidente relacionado con un dispositivo extraviado podría llevar a implementar políticas más estrictas de revocación automática de certificados o a mejorar los mecanismos de administración remota de dispositivos.

Los procesos de mejora también pueden incluir acciones orientadas a fortalecer la capacitación de los usuarios y del personal técnico. Informar a los usuarios sobre las buenas prácticas relacionadas con la protección de dispositivos y credenciales puede reducir significativamente la probabilidad de incidentes asociados a pérdidas de equipos o compromisos de credenciales. Del mismo modo, capacitar al personal técnico en el análisis de registros de autenticación y en la gestión de incidentes puede mejorar la capacidad de respuesta de la organización.

Otro aspecto relevante dentro del plan de mejora consiste en evaluar si los sistemas de monitoreo y registro de eventos están proporcionando la información necesaria para identificar incidentes de manera temprana. Si los registros de autenticación no contienen información suficiente sobre los eventos de acceso a la red, los equipos de seguridad pueden encontrar dificultades para investigar incidentes o detectar comportamientos anómalos. En estos casos, puede resultar necesario ajustar la configuración de los sistemas de registro para mejorar la visibilidad de la actividad de la red.

Finalmente, el informe de incidente y el plan de mejora constituyen herramientas fundamentales para fortalecer la gestión de seguridad de la organización. Documentar de manera sistemática los incidentes y analizar sus causas permite transformar cada evento de seguridad en una oportunidad para mejorar los controles existentes. Este enfoque contribuye a desarrollar infraestructuras de red más resilientes y a fortalecer los mecanismos de autenticación y control de acceso utilizados por la organización.

CONTINUAR

Referencias

Aruba Networks. (2023). *WPA3-Enterprise and EAP-TLS overview*. https://arubanetworking.hpe.com/techdocs/aos/wifi-design-deploy/security/modes/wpa3-enterprise/

Cisco Systems. (2016). *Troubleshooting RADIUS authentication*. https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html

FreeRADIUS Project. (2024). *FreeRADIUS server documentation (Version 3.2.9)*. https://www.freeradius.org/documentation/freeradius-server/3.2.9/

International Organization for Standardization. (2023). *ISO/IEC 27035-2:2023 – Information security incident management – Part 2: Guidelines to plan and prepare for incident response*. https://cdn.standards.iteh.ai/samples/78974/58e4871b153f4bb387a4c39d2d5ff4af/ISO-IEC-27035-2-2023.pdf

Internet Engineering Task Force. (2008). *Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile (RFC 5280)*. https://datatracker.ietf.org/doc/html/rfc5280

Keytos. (2023). *Cómo autenticar Wi-Fi con certificados*. https://www.keytos.io/blog/es/autoridad-de-certificacion/como-autenticar-a-wi-fi-con-

certificados.html

National Institute of Standards and Technology. (2023). *Guidelines for managing the security of mobile devices in the enterprise (NIST SP 800-124 Rev. 2).* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r2.pdf

OWASP Foundation. (2023). *Session management cheat sheet.* https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

Smallstep. (2023). *Using EAP-TLS certificates for secure Wi-Fi authentication.* https://smallstep.com/blog/eaptls-certificate-wifi/

CONTINUAR