

**13 – Uso de los Servicios de Red**

**CASIG 4 – Control de Acceso e Identidades**

**Preguntas de Auditoría**

**Uso de Servicios de Red**

|  |
| --- |
| **Competencias Básicas del Auditor**   1. **Conocimiento de Normativas y Estándares**: Familiaridad con marcos de referencia y estándares de la industria como NIST, ISO 27001, CIS, entre otros. 2. **Habilidades Analíticas**: Capacidad para analizar registros, logs y datos para identificar patrones anómalos o actividades sospechosas. 3. **Comprensión de Sistemas de Autenticación**: Entender diferentes mecanismos de autenticación, como autenticación de dos factores, tokens, certificados digitales, entre otros. 4. **Conocimiento de Tecnologías de Red**: Entender cómo funcionan las redes, protocolos y cómo se pueden explotar las vulnerabilidades relacionadas con el acceso. 5. **Habilidades de Comunicación**: Capacidad para comunicar hallazgos, riesgos y recomendaciones de manera clara a diferentes audiencias, desde técnicos hasta ejecutivos. 6. **Conocimiento de Herramientas de Auditoría**: Familiaridad con herramientas y software específicos utilizados para auditar sistemas y redes. 7. **Comprensión de la Gestión de Riesgos**: Capacidad para identificar, evaluar y priorizar riesgos asociados con la administración de cuentas y credenciales. 8. **Habilidades de Investigación**: Capacidad para investigar incidentes de seguridad, identificar la causa raíz y recomendar medidas correctivas. 9. **Conocimiento de Procesos de Negocio**: Entender cómo funcionan los procesos de negocio y cómo la administración de cuentas y credenciales se integra en ellos. 10. **Habilidades Interpersonales**: Capacidad para trabajar en equipo, gestionar conflictos y colaborar con diferentes departamentos y partes interesadas. 11. **Conocimiento de Legislación y Cumplimiento**: Estar al tanto de las leyes y regulaciones pertinentes que afectan la administración de cuentas y credenciales en la jurisdicción relevante. |

# Visión General

La gestión de acceso e identidades (IAM) en el contexto de servicios de red se centra en regular y controlar el acceso a las redes y servicios de red para usuarios autorizados y en asegurar que los proveedores cumplan con los niveles de seguridad acordados. Estos controles establecen una estructura sólida para garantizar el uso seguro de los servicios de red, desde la autenticación y la encriptación hasta la supervisión de la actividad de red.

**1.1 Directrices para la Seguridad en el Uso de Servicios de Red**

La organización debe evaluar la capacidad de sus proveedores para gestionar los servicios de red de forma segura y conforme a los estándares de seguridad. Los aspectos clave incluyen:

* **Evaluación de los Proveedores de Servicios de Red:** Determinar la capacidad del proveedor para gestionar servicios de red con las certificaciones de terceros que demuestren medidas de seguridad adecuadas.
* **Características de Seguridad de los Servicios de Red:** Asegurar la implementación de tecnologías de autenticación, encriptación y control de conexiones que garanticen una conectividad segura.

Las conexiones seguras requieren la correcta aplicación de parámetros técnicos, como los procedimientos de almacenamiento en caché y las configuraciones de acceso a servicios de red, que ajusten la seguridad según las necesidades de rendimiento y confidencialidad.

**1.2 Directrices Específicas para el Control de los Servicios de Red**

Para gestionar los servicios de red de manera efectiva, la organización debe implementar normas y procedimientos específicos que cubran:

* **Requisitos de Autenticación y Procedimientos de Autorización:** Definir quién puede acceder a qué servicios y redes, y con qué medios (por ejemplo, VPN o red inalámbrica).
* **Gestión de Acceso y Monitoreo:** Establecer controles tecnológicos, procedimientos de administración de red y atributos de usuario (hora, ubicación) que limiten el acceso y monitoreen la actividad.

Las normas sobre el uso de servicios de red deben ser formuladas y adoptadas para limitar el acceso a las redes permitidas y supervisar el uso de estos servicios, así como para acordar derechos de auditoría con los proveedores.

**1.3 Perspectiva de Auditoría en el Uso de Servicios de Red**

La auditoría del uso de servicios de red verifica el cumplimiento de las políticas de seguridad, autenticación y autorización. Los auditores revisan los niveles de servicio, la implementación de controles de acceso, y el monitoreo de la integridad de la red, asegurando que los proveedores cumplan con los requisitos de seguridad y que los usuarios sigan las normas de uso establecidas. Además, la auditoría asegura que los acuerdos de derecho a la auditoría con los proveedores se respeten, y que los mecanismos de seguridad, como la segmentación de la red, estén activos y alineados con los objetivos de protección de la organización.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Determinar la capacidad del proveedor de servicios de red para gestionar los servicios acordados de forma segura.  1.1 La organización también debe considerar las certificaciones de terceros proporcionadas por los proveedores de servicios para demostrar que mantienen las medidas de seguridad adecuadas.  2. Considerar y mantener las siguientes características de seguridad de los servicios de red:  2.1 Tecnología aplicada para la seguridad de los servicios de red, como autenticación, encriptación y controles de conexión a la red.  2.2 Parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las normas de seguridad y conexión a la red.  2.3 Almacenamiento en caché (por ejemplo, en una red de distribución de contenido) y sus parámetros que permiten a los usuarios elegir el uso del almacenamiento en caché de acuerdo con los requisitos de rendimiento, disponibilidad y confidencialidad.  2.4 Procedimientos para el uso de servicios de red para restringir el acceso a servicios o aplicaciones de red, cuando sea necesario.  3. Los servicios de red incluyen la provisión de conexiones, servicios de red privada y soluciones de seguridad de red administrada, como firewalls y sistemas de detección de intrusos.   4. Proteger y monitorear la integridad de la red (p. ej., segregación de la red, segmentación de la red) |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Implementar y monitorear los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red. La organización debe asegurarse de que los proveedores de servicios de red implementen estas medidas.   1.1 El derecho a la auditoría debe acordarse entre la organización y el proveedor.   2. Las normas sobre el uso de redes y servicios de red deben formularse e implementarse para cubrir:  2.1 Las redes y los servicios de red a los que se permite acceder.  2.2 Requisitos de autenticación para acceder a diversos servicios de red  2.3 Procedimientos de autorización para determinar quién puede acceder a qué redes y servicios en red.  2.4 Administración de redes y controles tecnológicos y procedimientos para proteger el acceso a conexiones de red y servicios de red;  2.5 Los medios utilizados para acceder a redes y servicios de red [por ejemplo, uso de red privada virtual (VPN) o red inalámbrica];  2.6 Hora, ubicación y otros atributos del usuario al momento del acceso;  2.7 Seguimiento del uso de los servicios de red. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. |  |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles |  |
| NIVEL 5 [Optimizado]: La organización se centra en la mejora continua y está diseñada para girar y responder a las oportunidades y los cambios. |  |

# Preguntas de Auditoría para los Usos de los Servicios de Red

|  |
| --- |
| 3.1 Temática: Identificación y documentación de los requisitos de Uso de Red |
| Durante este proceso de auditoría, se analiza si la organización ha establecido de manera completa y precisa los requisitos de uso de red. Esto incluye aspectos como quiénes tienen autorización para acceder a qué recursos, cómo deben autenticarse los usuarios, qué aplicaciones y servicios pueden utilizar y bajo qué circunstancias. El auditor verifica si estos requisitos están documentados de manera adecuada en políticas, normativas o procedimientos de uso de red y si estos documentos son accesibles y comprensibles para los usuarios.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización ha documentado políticas y normas claras que establecen cómo los usuarios deben acceder y utilizar las redes y servicios de red? * ¿Las normas definen las expectativas y restricciones para el uso de recursos de red, incluyendo aspectos de seguridad y cumplimiento? * ¿La organización ha identificado y documentado los mecanismos de seguridad, los niveles de servicio y los requisitos específicos de servicio para sus servicios de red? ¿Se dispone de documentación, políticas y acuerdos de nivel de servicio (SLA) que establecen claramente estos mecanismos y requisitos? * ¿Las normas sobre el uso de redes y servicios de red están fácilmente disponibles para todos los usuarios de manera electrónica o en formatos impresos? * ¿Los usuarios son conscientes de dónde pueden acceder a estas normas y cómo obtener una copia si es necesario? * ¿Los procedimientos incluyen detalles sobre autenticación, autorización, acceso a recursos y comportamiento aceptable en la red? * ¿Los usuarios deben leer y aceptar oficialmente las normas sobre el uso de redes y servicios de red antes de obtener acceso? * ¿Se mantiene un registro de aceptación de normas para cada usuario y se actualiza regularmente? * ¿Se mantienen registros de monitoreo, alertas y revisiones regulares para evaluar la conformidad con los mecanismos y niveles de servicio? |

|  |
| --- |
| **3.2 Integridad y disponibilidad de la red** |
| Mediante estas pruebas de auditoría, se examina si la organización ha establecido salvaguardias para prevenir ataques o eventos maliciosos que puedan afectar la integridad de la red, como ataques de denegación de servicio (DDoS) o intrusiones. También se evalúa si se han implementado sistemas de detección y respuesta ante incidentes de seguridad para identificar y mitigar posibles amenazas en tiempo real.  Además, se verifica si la organización tiene en marcha estrategias para garantizar la disponibilidad de la red, lo que implica asegurarse de que los sistemas estén operativos y accesibles cuando sea necesario.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización ha implementado medidas de segregación de red y segmentación para proteger la integridad de su red? ¿Se han definido y documentado las áreas de la red que deben estar segregadas o segmentadas para evitar accesos no autorizados? * ¿La organización controla el acceso a segmentos de red específicos según las necesidades de los usuarios y los roles? * ¿Se requiere autenticación y autorización adecuada para acceder a segmentos de red críticos o sensibles? * ¿La organización ha implementado medidas para proteger la integridad de su red y prevenir modificaciones no autorizadas? * ¿Se han establecido controles y mecanismos para detectar y evitar posibles alteraciones de datos o configuraciones en la red? * ¿La organización realiza un seguimiento continuo de los cambios y la actividad en la red para detectar cualquier intento de modificación no autorizada? * ¿La organización lleva a cabo pruebas de penetración y evaluaciones de riesgos periódicas para identificar posibles vulnerabilidades en la integridad de la red? ¿Se toman medidas en función de los resultados de estas pruebas para fortalecer la seguridad de la red? * ¿Existen registros de auditoría que demuestren el monitoreo y la revisión de cambios en la red? * ¿La organización tiene un proceso establecido para detectar y responder a incidentes que puedan comprometer la integridad de la red? * ¿Se han definido procedimientos de respuesta y se ha capacitado al personal para abordar posibles incidentes? |

|  |
| --- |
| **3.3 Capacidad y cumplimiento de los proveedores de Red** |
| Auditar la capacidad y cumplimiento de los proveedores de red implica revisar y evaluar cómo la organización asegura que los proveedores externos de servicios de red cumplan con los requisitos de seguridad y rendimiento acordados. En este sentido, se examina si la organización ha realizado una evaluación exhaustiva de los proveedores de servicios de red antes de establecer una asociación y se verifica si se han establecido acuerdos contractuales que definan claramente los niveles de servicio y los requisitos de seguridad que los proveedores deben cumplir.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización ha evaluado la capacidad y experiencia del proveedor de servicios de red para gestionar los servicios de manera segura y eficaz? * ¿Se han establecido criterios de selección para asegurarse de que el proveedor cumple con los estándares de seguridad requeridos? * ¿Se ha establecido un acuerdo formal entre la organización y el proveedor que otorga el derecho a realizar auditorías de seguridad? * ¿El acuerdo define los términos y condiciones bajo los cuales la organización puede llevar a cabo auditorías? * ¿La organización exige que el proveedor de servicios de red posea certificaciones de seguridad o cumplimiento relevantes para demostrar su compromiso con las mejores prácticas? * ¿Se considera la validez y relevancia de las certificaciones de terceros proporcionadas por el proveedor como evidencia de su mantenimiento de medidas de seguridad adecuadas? * ¿El proveedor de servicios de red informa a la organización sobre cambios en sus prácticas de seguridad o actualizaciones en la infraestructura? * ¿Existe un proceso para evaluar el impacto de estos cambios en la seguridad y tomar medidas si es necesario? * ¿El proveedor de servicios de red tiene un proceso establecido para la gestión de incidentes y respuestas a posibles brechas de seguridad? * ¿La organización entiende cómo el proveedor maneja incidentes de seguridad y cómo se coordinaría la respuesta en caso de un incidente? |