

**GASIC 6 – Seguridad en Redes**

**Preguntas de Auditoría**

**Infraestructura de Red**

**Competencias Básicas del Auditor**

1. **Conocimiento en seguridad de la información:** El auditor debe tener un profundo conocimiento de los principios y conceptos fundamentales de seguridad de la información, incluyendo la confidencialidad, integridad y disponibilidad de los datos.
2. **Conocimientos de redes:** Es esencial tener un conocimiento sólido de las redes de computadoras, incluyendo protocolos, topologías, componentes de red y arquitecturas.
3. **Comprensión de estándares y normativas:** Familiaridad con estándares de seguridad de la información como ISO 27001, NIST, CIS Controls y otras normativas aplicables. Debe comprender los requisitos de cumplimiento y saber cómo evaluar el cumplimiento de la organización.
4. **Herramientas de auditoría:** Ser capaz de utilizar herramientas de auditoría y análisis de seguridad, como escáneres de vulnerabilidades, herramientas de prueba de penetración, y sistemas de detección de intrusiones (IDS/IPS).
5. **Habilidades de análisis:** Ser capaz de analizar la configuración de dispositivos de red, registros de eventos y otros datos para identificar vulnerabilidades y problemas de seguridad.
6. **Gestión de riesgos:** Comprender cómo evaluar y gestionar los riesgos de seguridad en una infraestructura de red, incluyendo la identificación, análisis y mitigación de riesgos.

# Visión General

La infraestructura de red está compuesta por recursos físicos, como routers, switches, servidores y cables, y recursos lógicos, como direcciones IP, firewalls, protocolos de comunicación y sistemas de enrutamiento. Estos elementos trabajan juntos para soportar la comunicación y transferencia de datos entre usuarios, aplicaciones y dispositivos dentro de una organización. Una gestión efectiva de esta infraestructura implica diseñar y mantener una arquitectura de red que asegure disponibilidad, seguridad y resiliencia, considerando la criticidad de los servicios y los riesgos asociados. Además, esta infraestructura debe garantizar que los flujos de datos sean consistentes, confiables y seguros, incluso en escenarios de alta demanda o condiciones adversas.

**1.1 Diseño y Mantenimiento de la Arquitectura de Red**

El diseño de la arquitectura de red debe basarse en los requisitos de disponibilidad y seguridad de los servicios empresariales. Esto incluye implementar segmentación para minimizar el acceso no autorizado, aplicar el principio de menor funcionalidad para reducir la exposición de los sistemas, y utilizar protocolos seguros para la comunicación y gestión de la red. La infraestructura debe incorporar redundancia, como redes paralelas, centros de datos geográficamente separados y componentes duplicados, garantizando la continuidad operativa incluso en situaciones adversas. Los recursos administrativos deben estar segregados físicamente o lógicamente, evitando accesos no autorizados a través de la red principal o Internet.

**1.2 Auditoría y Monitoreo de la Infraestructura**

Desde el punto de vista de auditoría, es esencial mantener diagramas actualizados de la arquitectura de red y realizar revisiones periódicas para garantizar que las configuraciones y los dispositivos cumplan con los objetivos de seguridad definidos. Los registros de eventos deben producirse y conservarse durante un tiempo adecuado, asegurando que incluyan información relevante para identificar y mitigar desviaciones en el comportamiento de la red. Adicionalmente, se deben monitorear los indicadores clave relacionados con la seguridad y el mantenimiento de la infraestructura, documentando hallazgos y estableciendo mejoras según sea necesario. Revisar las versiones de software y protocolos regularmente permite garantizar la compatibilidad y minimizar vulnerabilidades en la infraestructura.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Identificar los requisitos de disponibilidad de los servicios empresariales y de los sistemas de información.  2. Establecer y mantener una arquitectura de red segura. Para esto se debe incluir:      2.1 Abordar la segmentación, los privilegios mínimos y la disponibilidad, como mínimo.      2.2 Incorporar el principio de menor funcionalidad mediante la configuración de los sistemas para proporcionar solo las capacidades esenciales.      2.3 Utilizar protocolos de comunicación y administración de red seguros.  3. Diseñar e implementar una arquitectura de sistemas con la redundancia adecuada para cumplir con estos requisitos. La organización debería tener en cuenta lo siguiente a la hora de implantar sistemas redundantes:      3.1 contratar a dos o más proveedores de instalaciones de red y de procesamiento de información crítica, como proveedores de servicios de Internet.      3.2 usar redes redundantes.      3.3 usar dos centros de datos separados geográficamente con sistemas duplicados.      3.4 usar fuentes de alimentación físicamente redundantes.      3.5 usar múltiples instancias paralelas de componentes de software, con un equilibrio de carga automático entre ellas.      3.6 tener componentes duplicados en los sistemas en las redes.  4. Establecer y mantener recursos informáticos dedicados, ya sea física o lógicamente separados, para todas las tareas administrativas o tareas que requieran acceso administrativo.          4.1 Los recursos informáticos deben estar segmentados de la red principal de la empresa y no se les debe permitir el acceso a Internet.  5. Implementar mecanismos para lograr los requisitos de resiliencia en situaciones normales y adversas (por ejemplo, a prueba de fallas, equilibrio de carga, cambio en caliente o “hot swap”).  6. Priorizar los recursos (por ejemplo, hardware, dispositivos, datos, tiempo, personal y software) en función de su clasificación, criticidad y valor comercial  7. Asegurar que la comunicación organizacional y los flujos de datos están mapeados. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Establecer y mantener diagramas de arquitectura y/u otra documentación del sistema de red.  2. Considerar, al momento de gestionar la infraestructura de red:      2.1 Asegurar que la infraestructura de la red esté actualizada      2.2 Establecer y mantener una arquitectura de red segura      2.3 Administrar de forma segura la infraestructura de red      2.4 Establecer y mantener diagramas de arquitectura      2.5 Centralizar la autenticación, autorización y auditoría de la red (AAA)      2.6 Uso de protocolos de comunicación y gestión de red segura      2.7 Asegurar que los dispositivos remotos utilicen una VPN y se conecten a la infraestructura AAA de una empresa      2.8 Establecer y mantener recursos informáticos dedicados para todo el trabajo administrativo  3. Identificar y mantener una lista de activos de infraestructura que deben monitorizarse conforme a la criticidad del servicio y la relación entre los elementos de configuración y servicios que dependen de ellos.  4. Exigir a los usuarios que se autentiquen en servicios de autenticación y VPN administrados por la empresa antes de acceder a los recursos empresariales en los dispositivos del usuario final.  5. Definir e implementar reglas que identifiquen y registren incumplimientos de umbrales y los estados de eventos.      5.1 Se debe encontrar un equilibrio entre la generación de eventos menores insignificantes y eventos significativos para que los registros de eventos no estén sobrecargados de información innecesaria.      5.1 Se debe identificar el nivel de información que debe registrarse, conforme a una consideración de riesgo y rendimiento. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Asegurar que la infraestructura de red se mantenga actualizada      1.1 Se deben revisar las versiones de software mensualmente o con mayor frecuencia para verificar la compatibilidad del software.  2. Revisar y actualizar la documentación anualmente o cuando se produzcan cambios empresariales importantes que puedan afectar al sistema de red.  3. Establecer procedimientos para monitorizar los registros de eventos.      3.1 Se deben llevar a cabo revisiones regulares |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Producir registros de eventos y conservarlos durante un periodo de tiempo adecuado para que ayuden en futuras investigaciones.  2. Establecer objetivos de seguridad para la infraestructura de red.  3. Mantener y revisar indicadores para la mantención y seguridad de la infraestructura de red. |
| NIVEL 5 [Optimizado]: La organización se centra en la mejora continua y está diseñada para girar y responder a las oportunidades y los cambios. | 1. Revisar desviaciones en la medición de indicadores y lecciones de aprendidas en comparación con los objetivos de la organización.  2. Documentar hallazgos y establecer mejoras según las desviaciones observadas. |

1. **Preguntas de Auditoría para la Infraestructura de Red**

|  |
| --- |
| Temática: Registros de Eventos |
| Se requiere dar revisión a los registros de eventos cómo parte esencial de la gestión de la seguridad y el rendimiento de la infraestructura de red para así lograr tener una infraestructura que pueda lograr la resiliencia, más segura y mejor monitoreada. Para esto es necesario revisar los registros previos de la red, estos registros ayudarán a entender hacía donde va el flujo de la red, cómo opera, posibles vulnerabilidades que solucionar y cómo gestionar de mejor manera la red. Es por esto que la combinación de herramientas adecuadas, procesos bien definidos y personal capacitado puede ayudar a mantener una red segura y eficiente.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se están registrando eventos de red de manera adecuada y consistente?   + ¿Los registros de eventos están siendo almacenados de acuerdo con las políticas de retención de datos establecidas?   + ¿Se han implementado medidas para proteger los registros de eventos contra modificaciones no autorizadas?   + ¿Los registros de eventos son revisados y monitoreados regularmente por personal autorizado?   + ¿Existen procedimientos documentados para la notificación y respuesta a eventos de seguridad identificados en los registros?   + ¿Se lleva a cabo un análisis periódico de los registros de eventos para identificar patrones o tendencias de seguridad? * ¿Existe un procedimiento documentado que indique dónde se almacenan los registros de eventos de la infraestructura de red?   + Revise la documentación de políticas y procedimientos de seguridad de la infraestructura de red para identificar si existe un procedimiento que especifique claramente dónde se almacenan los registros de eventos.   + ¿Se establecen períodos de retención de registros de eventos para la infraestructura de red?   + ¿Los registros de eventos de la infraestructura de red están protegidos contra alteraciones no autorizadas o eliminación no autorizada?¿Se realizan copias de seguridad periódicas de los registros de eventos?   + ¿Dónde se almacenan físicamente los registros de eventos de la infraestructura de red?     - Revise los registros de inventario de la organización para identificar cualquier equipo de almacenamiento específico designado para registros de eventos en la infraestructura de red. * ¿Existe una política de retención de registros para la infraestructura de red?   + Evalúe si la política de retención de registros se encuentra publicada y disponible para todos los empleados que necesitan acceder a ella.   + ¿La política especifica los tipos de registros que deben ser retenidos y su período de retención?   + ¿Se define claramente las responsabilidades de las partes involucradas en la retención y gestión de registros de infraestructura de red?   + ¿La organización tiene un proceso establecido para la producción de registros de eventos?   + ¿Existe un período de retención de registros definido y documentado para los registros de eventos?   + ¿Se ha designado a un responsable o equipo encargado de la gestión y supervisión de los registros de eventos? * ¿Están claramente definidos los roles y responsabilidades de las personas que tienen acceso a los registros de la infraestructura de red?   + ¿Se mantienen registros de acceso que documenten quién ha accedido a los registros de la infraestructura de red y cuándo lo hizo?   + ¿Se aplican medidas de seguridad, como autenticación y autorización, para controlar el acceso a los registros de la infraestructura de red?   + ¿Se realizan revisiones periódicas de acceso a los registros para garantizar que solo las personas autorizadas tengan acceso? * ¿Existe un proceso documentado para realizar un seguimiento de cambios en la configuración de dispositivos de red?   + ¿Se designa a una persona o equipo responsable de llevar a cabo el seguimiento de cambios en la configuración de dispositivos de red?   + ¿Se utilizan herramientas o sistemas automatizados para registrar y rastrear cambios en la configuración de dispositivos de red? ¿Se realizan revisiones periódicas de los registros?   + ¿Se documentan los motivos y justificaciones de los cambios en la configuración de dispositivos de red? |

|  |
| --- |
| Temática: Actualización de la Red |
| Mantener una infraestructura de red actualizada es esencial para mantener un entorno de red seguro y eficiente, así como para garantizar que la infraestructura de red cumpla con los objetivos comerciales y las regulaciones aplicables. Además, deben ser revisadas y actualizadas periódicamente para adaptarse a los cambios en las tecnologías, las amenazas y las necesidades de la organización.Este levantamiento puede incluir análisis específicos tales como:¿Se han implementado políticas de gestión de contraseñas fuertes y se cambian regularmente las contraseñas en los dispositivos de red?¿Cuáles son los parámetros que deben cumplir las contraseñas?¿Cada cuánto tiempo expiran las contraseñas para que deban ser cambiadas?¿Se mantiene otro mecanismo que ayude con la seguridad de los inicio de sesión tal así como un MFA?¿Se cuenta con un proceso de gestión de cambios para garantizar que las actualizaciones y cambios en la red sean una mejora y realicen de manera controlada y documentada?¿Cómo se controlan los cambios en la red?¿Se han documentado todos los cambios realizados en la red?¿Cómo se garantiza que los cambios en la red sean una mejora?¿El proceso de gestión de cambios en la red, ha sido planificado correctamente?¿Se ha realizado una evaluación de vulnerabilidades reciente en la infraestructura de red y si es así, se han documentado todos los hallazgos?¿Cuál es el procedimiento para hallar vulnerabilidades en la red de la organización?¿Cómo se evalúan dichas vulnerabilidades, hay algún indicador a seguir?¿Según los hallazgos de las vulnerabilidades, cómo se ha procedido al manejo de estas?¿Se siguen los procedimientos de respaldo y restauración antes de aplicar actualizaciones críticas?¿Existe un procedimiento documentado para respaldar la infraestructura de red antes de aplicar actualizaciones críticas?¿En dónde se guardan dichos respaldos?¿Se realiza una copia de seguridad completa de la configuración de la infraestructura de red antes de aplicar actualizaciones críticas?¿Quién tiene acceso y cómo accede a los respaldos?¿Se mantiene un registro de las actualizaciones críticas aplicadas y los respaldos asociados?¿Se comprueba que los respaldos estén íntegros antes de una restauración? |

|  |
| --- |
| 3.3 Temática: Monitoreo de la Infraestructura |
| El objetivo principal de analizar la estructura organizacional es garantizar que la organización tenga una estructura bien definida y funcional que permita una gestión efectiva de recursos humanos y una toma de decisiones coherente, la cual esté en constante revisión ante cambios que surjan y que requiera cambiar la estructura organizacional para adaptarse a estos cambios.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se verificó la estructura organizativa en áreas funcionales de SIC para identificar áreas críticas para el cumplimiento de las necesidades organizacionales?   + Verifique que las necesidades organizacionales se basan en la apreciación al riesgo y al cumplimiento de los objetivos estratégicos.     - Verifique que el diseño de la estructura organizativa funcional ha sido validado por un comité estratégico de seguridad de la información o mecanismo similar.   + Compruebe si existe una revisión documental y entrevistas con los líderes de las áreas funcionales para determinar la criticidad de su operación.   + Verifique que las áreas críticas cuentan con la supervisión, independencia, autoridad y recursos necesarios para dar respuesta a su función. * ¿Se evalúa si la estructura actual permite adaptarse a cambios en necesidades?   + ¿Existen mecanismos para identificar y abordar rápidamente necesidades emergentes?     - ¿Se han examinado incidentes y casos previos de desviación de tiempos de finalización de tareas o necesidades emergentes especiales y su causa raíz?       * Verifique que para cada caso se ha identificado los mecanismos de detección, los mecanismos de comunicación con el liderazgo organizacional y las acciones tomadas para remediarlo.     - ¿La función SIC realiza ejercicios de planificación de escenarios para simular situaciones de emergencia y evaluar cómo se respondería a ellas?     - ¿Se han tomado medidas respecto al resultado de estas simulaciones?     - ¿Se han levantado alertas y propuestas a la alta dirección en base al resultado de estos ejercicios?   + ¿Se evalúa si se requiere personal adicional en función de cambios organizacionales?     - Examine registros de reuniones de planificación estratégica y decisiones de gestión que indiquen los cambios necesarios.     - Contraste los registros con los informes financieros y presupuestarios para identificar posibles restricciones que afecten la adaptabilidad de la estructura.     - Verifique que se ha notificado del riesgo de no adaptar la estructura organizacional de la función SIC.     - Verifique si la organización ha realizado un análisis comparativo con la estructura de personal en organizaciones de industrias y funciones similares.     - Verifique la organización ha comparado las tasas de crecimiento y tamaño de la fuerza laboral en función de los factores como: riesgo, tamaño y complejidad de las operaciones. Considere las recomendaciones de mejores prácticas como los informes sectoriales ENISA y NIST. * ¿Se evalúan acuerdos de servicio con terceros para soportar cambios organizacionales? * ¿Se verifica eficacia en el uso de contratistas externos para recursos adicionales? |