

**GASIC 6 – Seguridad en Redes**

**Preguntas de Auditoría**

**Comunicaciones 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

Las comunicaciones de red se refieren a la infraestructura y procesos que permiten la transferencia de datos y la conectividad entre dispositivos dentro y fuera de una organización. Esto se realiza mediante la implementación de tecnologías como redes **LAN, WAN, VPN** y protocolos de enrutamiento. Estas comunicaciones son esenciales para que la organización pueda compartir información, recursos y aplicaciones de manera eficiente y segura, facilitando la colaboración entre equipos y la toma de decisiones informadas. Además, las comunicaciones de red son fundamentales para respaldar las operaciones comerciales, la prestación de servicios a clientes y la adaptación a un entorno empresarial en constante evolución, lo que las convierte en un componente estratégico clave para el éxito y la competitividad de la organización.

**1.1 Vulnerabilidades que se pueden presentar**

La falta de una comunicación de red adecuadamente planificada y gestionada puede dar lugar a una serie de vulnerabilidades y desafíos significativos en una organización. Sin una estructura de red bien definida, se corre el riesgo de exposición a ataques cibernéticos y brechas de seguridad, ya que las conexiones no gestionadas pueden proporcionar puntos de entrada no autorizados a intrusos. Además, la falta de segmentación de red puede permitir que un malware se propague fácilmente a través de toda la infraestructura. La ineficiencia en la comunicación de datos también puede dar lugar a cuellos de botella, perdida de datos y problemas de rendimiento, lo que afecta directamente a la productividad y la calidad del servicio.

**1.2 Aplicación de las comunicaciones de red**

implica la planificación, configuración y gestión de infraestructuras que permiten la conectividad y transferencia de datos en una organización. Esto se logra mediante la instalación de dispositivos de red, definición de protocolos y políticas de seguridad. Se aplica desde la planificación inicial de la red y continúa a medida que la organización crece y se adapta. Es esencial para mejorar la eficiencia operativa, facilitar el acceso a recursos compartidos, garantizar la seguridad de los datos, cumplir con regulaciones y mantener la competitividad en un entorno empresarial en constante cambio.

**1.3 Como funciona**

Las comunicaciones de red se basan en el principio de asegurar que la información que fluye a través de la red ya sea dentro o fuera de la organización, esté protegida contra amenazas cibernéticas. Esto se logra mediante la implementación de tecnologías y políticas de seguridad que incluyen cifrado de datos, autenticación de usuarios y dispositivos, segmentación de red, detección de intrusiones y monitoreo constante del tráfico para identificar y mitigar posibles amenazas. Las comunicaciones de red seguras son esenciales para salvaguardar la integridad, la confidencialidad y la disponibilidad de la información crítica y para garantizar que la organización esté protegida contra ataques cibernéticos que puedan comprometer sus operaciones y datos sensibles.

**1.4 Datos críticos para la organización**

Las comunicaciones de red abarcan una amplia variedad de datos críticos, incluyendo información confidencial de la empresa, como secretos comerciales, propiedad intelectual, datos financieros y estratégicos, así como datos de clientes y empleados, que pueden incluir información personal, contraseñas, datos de tarjetas de crédito y registros de transacciones. Además, abarcan datos operativos esenciales para la continuidad del negocio, como la gestión de tráfico, registros de eventos de seguridad y métricas de rendimiento de la red. Proteger estos datos críticos es fundamental para evitar fugas de información, pérdida de confidencialidad y posibles daños a la reputación de la organización y ejecuten programas maliciosos que pueden dañar sistemas, robar datos o comprometer la seguridad de la empresa. No solo afectara negativamente a la empresa si este software tiene un virus, sino que también este podría no estar actualizado con los últimos parches de seguridad. Además, la instalación de software no necesario para el trabajo puede distraer a los empleados y afectar la productividad.

**1.5 Políticas de Conectividad**

Una política de conectividad es esencial para establecer un marco solido de seguridad informática en una organización. Ayuda a proteger la red, los datos y los sistemas contra amenazas cibernéticas y a garantizar que el acceso a la red sea seguro y controlado. Estas políticas ayudan a controlar el acceso, a prevenir intrusiones, a proteger la privacidad de los datos. Además, contribuyen a la resiliencia y la disponibilidad de la red, lo que es esencial para la continuidad del negocio.

**1.6 Auditoría y Mejora Continua**

Desde la auditoría, es crítico verificar regularmente la necesidad y relevancia de cada conexión interna, garantizando que cumplan con los objetivos de seguridad y control definidos por la organización. Los indicadores de cumplimiento deben mantenerse actualizados y ser monitoreados para identificar desviaciones respecto a las metas establecidas. Un proceso de mejora continua permitirá evaluar y optimizar las conexiones de red según estas desviaciones, asegurando que las políticas sigan siendo efectivas y adaptándose a los cambios en el entorno tecnológico y empresarial.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Denegar el tráfico de comunicaciones de red de forma predeterminada y permitir el tráfico de comunicaciones de red por excepción  2. Identificar y definir conexiones externas e internas autorizadas en el sistema o sus componentes.  3. Documentar, para cada conexión interna, las características de la interfaz, los requisitos de seguridad y privacidad, y la naturaleza de la información comunicada.  3.1 Realizar verificaciones de cumplimiento de seguridad y privacidad en los componentes del sistema antes del establecimiento de la conexión interna.  4. Terminar las conexiones internas del sistema después de un tiempo definido por la organización.  5. Segregar a los grupos de servicios de información, usuarios y sistemas de información en las redes de la organización.  5.1 Realizar la partición de funciones privilegiadas en dominios físicos separados. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1 dividir red en límites de seguridad y controlar el tráfico entre ellos en función de las necesidades de la empresa.  1.1 Considerar gestión de la seguridad de grandes redes dividiéndolas en dominios de red separados y segregándolas de la red pública.  1.2. Considerar el ajuste de la cobertura radioeléctrica para la segregación de redes inalámbricas.  1.3 En el caso de entornos sensibles, se debería considerar la posibilidad de tratar todos los accesos inalámbricos como conexiones externas y segregar este acceso de redes internas hasta que se apruebe el acceso.  1.4 La red de acceso inalámbrico para invitados debería estar segregada de la del personal si este solo usa dispositivos terminales de usuario controlados que cumplan con políticas específicas de la organización.  1.4.1 El WiFi para invitados debería tener al menos las mismas restricciones que el WiFi para el personal, con el fin de desalentar el uso de WiFi para invitados por parte del personal.  1.5 Se debe permitir que solo los dispositivos autorizados tengan acceso a la información corporativa y a la red de la empresa.  1.5.1 Se deben configurar estos dispositivos para forzar la introducción de contraseña.  1.6 Limitar el número de conexiones de red externas al sistema.  2. Verificar que las conexiones a redes o sistemas externos sea solo a través de interfaces administradas por dispositivos de protección de límites dispuestos de acuerdo con una arquitectura de seguridad y privacidad organizacional  2.1 Prohibir la conexión directa de sistemas de seguridad nacional clasificados y no clasificados definidos por la organización a una red externa sin el uso de protección de límites. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Revisar frecuentemente la necesidad continua de cada conexión interna.  2. Supervisar y controlar las comunicaciones en las interfaces administradas externas al sistema y en las interfaces administradas internas clave dentro del sistema  3. Detectar y denegar el tráfico de comunicaciones salientes que suponga una amenaza para los sistemas externos.  3.1 Auditar la identidad de los usuarios internos asociados con las comunicaciones denegadas |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Establecer objetivos y metas para la identificación, control de comunicaciones y de seguridad.  1.1 Se deben mantener indicadores para su medición. |
| 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. Mantener un proceso de mejora continua para establecer mejoras en las conexiones de red según desviaciones identificadas según objetivos establecidos. |

1. **Preguntas de Auditoría para las Comunicaciones de Red**

|  |
| --- |
| Temática: División de las Redes y Control del Tráfico |
| Implica evaluar y fortalecer las medidas de seguridad implementadas en la infraestructura de red. Esto se hace para garantizar que solo el tráfico autorizado y necesario pueda fluir entre las distintas divisiones de la red, reduciendo así los riesgos de acceso no autorizado o ataques cibernéticos. Este proceso incluye la revisión de configuraciones de cortafuegos, segmentación de red y la implementación de controles de acceso. Controlar el tráfico de acuerdo con las necesidades de la empresa garantiza un uso eficiente de los recursos de red y una protección adecuada de los datos y sistemas críticos.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se han implementado controles de acceso para garantizar que solo usuarios autorizados tengan acceso a segmentos específicos de la red?   + Evalúe la configuración de los sistemas de control de acceso, como listas de control de acceso (ACL) o políticas de seguridad de red, para verificar que se restrinja el acceso a segmentos específicos.   + ¿La organización tiene registros de la configuración de dispositivos de red, como routers y switches, para confirmar que se han establecido reglas de acceso adecuadas? * ¿Se realiza una revisión regular de los registros de seguridad de red para identificar eventos o actividades sospechosas?   + Revise los registros de seguridad de red y los informes de revisión de registros para verificar si se están realizando revisiones periódicas.   + Verifique la documentación que indique las acciones tomadas en respuesta a eventos o actividades sospechosas identificadas en los registros.   + ¿Existen procedimientos que describan la frecuencia y el proceso de revisión de los registros de seguridad de red?   + ¿Se realiza un monitoreo constante de la red para detectar y responder a actividades inusuales o potenciales amenazas? * ¿Existen cortafuegos o dispositivos de seguridad configurados para limitar el tráfico no autorizado o malicioso?   + Revise las configuraciones de los dispositivos de seguridad de red, para asegurarse de que estén implementados y configurados para bloquear el tráfico no autorizado o malicioso.   + ¿Existen informes, manuales y procedimientos de seguridad de red en la organización que describan la configuración y el mantenimiento de dispositivos de seguridad?   + ¿La red tiene medidas de control de tráfico en su lugar para mitigar ataques de denegación de servicio (DDoS) u otras amenazas similares? * ¿Se ha implementado la segmentación de red para aislar sistemas críticos de otros segmentos de la red?   + Examine la topología de red y los diagramas de segmentación para confirmar que los sistemas críticos están aislados de manera efectiva.   + ¿La red está adecuadamente segmentada y dividida para garantizar la separación lógica de recursos y la seguridad de datos sensibles?   + Realice un análisis de la red para verificar la efectividad de la segmentación y la separación de tráfico mediante herramientas de escaneo de red. * ¿Existe un proceso de gestión de incidentes de seguridad de red para abordar eventos de seguridad de manera efectiva?   + Evalúe la respuesta a incidentes de seguridad de red pasados para determinar si se siguieron los procedimientos establecidos. * ¿Existen procedimientos establecidos para el control del tráfico de red, incluyendo reglas de firewall y sistemas de detección de intrusiones? |

|  |
| --- |
| Temática: Conexiones a Redes o Sistemas Externos |
| Implica revisar y evaluar la infraestructura de red y los dispositivos de seguridad utilizados para garantizar que todas las conexiones externas estén adecuadamente controladas y protegidas. Esto se hace para asegurarse de que ninguna conexión no autorizada pueda acceder a los sistemas internos y para mantener la privacidad y seguridad de los datos. El enfoque se basa en limitar el acceso solo a través de interfaces administradas y configuradas de manera segura, siguiendo las políticas y estándares de seguridad de la organización. Este proceso ayuda a prevenir amenazas externas y salvaguardar la integridad de los sistemas y datos de la empresa.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existe un inventario actualizado de todas las conexiones a redes o sistemas externos, y se revisa periódicamente?   + Revise la documentación de políticas y procedimientos relacionados con la gestión de conexiones externas.   + ¿Existe documentación actualizada y detallada de las políticas y procedimientos relacionados con la gestión de conexiones externas, incluyendo políticas de acceso, autorización y seguridad de la información? * ¿Se han implementado dispositivos de protección de límites, como **firewall y gateways**, para controlar el tráfico de red externo?   + Realice un análisis de riesgos para identificar posibles amenazas y vulnerabilidades en las conexiones externas.   + ¿Se ha llevado a cabo un análisis completo de riesgos que incluye la identificación y evaluación de las posibles amenazas y vulnerabilidades relacionadas con las conexiones externas de la organización, y se han implementado medidas de mitigación adecuadas para abordar estos riesgos identificados? * ¿Las interfaces administradas de estos dispositivos están configuradas de manera segura y cumplen con las políticas de seguridad?   + Evalúe la configuración de los dispositivos de protección de límites para garantizar que estén alineados con las políticas de seguridad.   + ¿Se ha verificado que la configuración de los dispositivos de protección de límites, como firewalls y sistemas de detección de intrusiones, esté alineada específicamente con las políticas de seguridad de la organización, y se han identificado posibles desviaciones o configuraciones no autorizadas que podrían representar riesgos para la seguridad de la red? * ¿Se aplican reglas de filtrado de paquetes para permitir el tráfico solo a servicios y protocolos autorizados?   + Realice un análisis exhaustivo de las reglas de filtrado de paquetes en los dispositivos de seguridad de red (firewalls, routers, etc.) para identificar y verificar la configuración de reglas específicas.   + ¿Se ha llevado a cabo una revisión detallada de las reglas de filtrado de paquetes en los dispositivos de seguridad de red para determinar si están configuradas de acuerdo con las políticas de seguridad de la organización, y se han identificado posibles desviaciones o configuraciones no autorizadas que puedan representar riesgos para la seguridad de la red? * ¿Existe una supervisión continua y registros de eventos de seguridad de las conexiones externas?   + Revisar los registros de eventos de seguridad para identificar actividades inusuales o incidentes previos.   + ¿Se han realizado revisiones periódicas de los registros de eventos de seguridad y se han documentado incidentes previos, y en caso afirmativo, se han tomado medidas adecuadas para abordar y mitigar los riesgos identificados a partir de estos registros? * ¿Se realizan pruebas regulares de penetración y evaluaciones de vulnerabilidades en los dispositivos de protección de límites?   + Realizar pruebas de penetración controladas para evaluar la resistencia de los dispositivos de protección de limites.   + ¿Se han llevado a cabo pruebas de penetración controladas en los dispositivos de protección de límites, y se han identificado y remediado de manera efectiva las vulnerabilidades o debilidades detectadas durante estas pruebas para fortalecer la resistencia de la red ante posibles ataques cibernéticos? * ¿Se mantienen actualizados los dispositivos de seguridad con parches y actualizaciones de firmware?   + Verifique que los dispositivos estén actualizados con los últimos parches de seguridad y que sigan un proceso de gestión de cambios.   + ¿Se ha establecido un proceso de gestión de cambios formal y se sigue regularmente para garantizar que los dispositivos de protección de límites estén actualizados con los últimos parches de seguridad y actualizaciones de firmware, y se ha verificado que estos dispositivos estén configurados de manera segura después de cada actualización para evitar posibles vulnerabilidades? * ¿Se ha implementado autenticación de dos factores o autenticación fuerte para acceder a conexiones externas críticas?   + Entreviste al personal técnico para asegurarse de que estén al tanto de las políticas y prácticas de seguridad.   + ¿Se ha realizado entrevistas con el personal técnico encargado de la administración y configuración de los dispositivos de protección de límites, y se ha confirmado que están plenamente informados y cumplen con las políticas y prácticas de seguridad establecidas para mantener un entorno de red seguro? * ¿Hay procedimientos documentados para gestionar incidentes de seguridad relacionados con conexiones externas?   + Evalúe los procedimientos de respuesta a incidentes y la capacidad de la organización para abordar problemas de seguridad relacionados con las conexiones externas.   + ¿La organización cuenta con procedimientos de respuesta a incidentes bien definidos y efectivos para abordar problemas de seguridad relacionados con las conexiones externas, y se han realizado pruebas o ejercicios de simulación para evaluar la eficacia y la capacidad de respuesta del equipo de seguridad en caso de incidentes de seguridad que afecten a estas conexiones externas? |