

**GASIC 6 – Seguridad en Redes**

**Preguntas de Auditoría**

**Reglas y Controles**

**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 seguridad en redes requiere un enfoque integral que combine reglas y controles específicos para proteger los activos empresariales de amenazas potenciales. Estas medidas incluyen desde la implementación de herramientas de filtrado hasta procesos de monitoreo continuo y capacitación de los usuarios, garantizando una protección robusta frente a riesgos como el malware, accesos no autorizados o el uso de software malicioso. La correcta aplicación de estas prácticas no solo resguarda la integridad de los datos y sistemas, sino que también permite cumplir con normativas de seguridad y mantener la continuidad operativa.

**1.1 Implementación de Controles Técnicos para la Protección de Redes**

Para mitigar riesgos, se deben establecer controles que limiten o bloqueen actividades sospechosas. Esto incluye el uso de servicios de filtrado DNS para bloquear dominios maliciosos conocidos, la instalación de herramientas antimalware actualizadas en todas las estaciones de trabajo y servidores, así como el escaneo periódico de datos y archivos adjuntos antes de su uso. Estas prácticas fortalecen la primera línea de defensa contra ataques externos y garantizan que los activos críticos estén protegidos.

**1.2 Medidas Preventivas y Correctivas en la Seguridad de Redes**

La prevención se complementa con procesos correctivos que detecten y mitiguen vulnerabilidades antes de que puedan ser explotadas. La gestión de correos electrónicos, mediante políticas como DMARC, y la implementación de filtros de URL basados en la red son esenciales para reducir la exposición a contenidos maliciosos. Además, el monitoreo de amenazas emergentes y la capacitación periódica de los usuarios en el reconocimiento de correos y sitios sospechosos fortalecen la postura de seguridad organizacional.

**1.3 Auditoría y Mejora Continua de Reglas y Controles**

La auditoría de reglas y controles debe enfocarse en validar su cumplimiento y efectividad dentro del entorno de red. Esto incluye revisar la correcta implementación de filtros de tráfico, verificando que bloqueen accesos a sitios web no aprobados o maliciosos, y auditar las políticas de control de software, asegurándose de que los sistemas detecten y restrinjan el uso de aplicaciones no autorizadas. Adicionalmente, es necesario monitorear los logs generados por los sistemas de seguridad para identificar patrones de acceso que puedan revelar intentos de violación de reglas establecidas. Con base en los hallazgos, se deben actualizar las configuraciones, implementar ajustes según los riesgos detectados y documentar las mejoras realizadas.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Implementar reglas y controles que impidan o detecten el uso de "software" no autorizado:  1.1 aplicar controles que impidan o detecten el uso de sitios Web conocidos o sospechosos de ser maliciosos.  1.2 realizar una validación periódica y automatizada de contenido de "software" y de datos de sistemas, especialmente en el caso de sistemas que soportan procesos empresariales críticos e investigar la presencia de cualquier archivo no aprobado o de modificaciones no autorizadas.  1.3 establecer medidas de protección contra riesgos asociados a obtención de archivos y programas informáticos desde o a través de redes externas o en cualquier otro soporte.  1.4 instalar y actualizar periódicamente "malware" de detección, reparación para escanear computadores y medios de almacenamiento electrónico.  1.5 escanear cualquier dato recibido a través de redes o mediante cualquier forma de medio de almacenamiento electrónico, en busca de "malware" antes de su uso.  1.6.escanear archivos adjuntos y descargas de correo electrónico y mensajería instantánea en busca de "malware" antes de usarlos. Realizar este escaneo en diferentes lugares y al entrar en red de la organización.  1.7 escanear páginas Web en busca de "malware" cuando se accede a ellas.  1.8 determinar ubicación y configuración de herramientas de detección y reparación de "malware" en función de resultados de evaluación de riesgos.  1. Se debe filtrar el tráfico de entrada, como el correo electrónico y las descargas, para protegerlo de información no solicitada (p.ej. spyware, correos electrónicos de phishing). |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Gestionar el acceso a sitios web externos para reducir la exposición a contenidos maliciosos.  1.1 Se deben utilizar servicios de filtrado DNS en todos los activos empresariales para bloquear el acceso a dominios maliciosos conocidos.  1.2 Se deben aplicar y actualizar filtros de URL basados en la red para limitar la conexión de un activo empresarial a sitios web potencialmente maliciosos o no aprobados.  1.3 Bloquear el acceso a los siguientes tipos de sitios Web:  1.3.1 sitios Web que tienen una función de carga de información, a menos que se permita por razones comerciales válidas.  1.3.2 sitios Web conocidos o sospechosos de ser maliciosos.  1.3.3 servidores de mando y control.  1.3.4 sitio Web malicioso adquirido de la inteligencia de amenazas.  1.3.5 sitios Web que comparten contenidos ilegales.  2. Gestionar el correo electrónico para reducir la exposición a contenidos maliciosos.  2.1 Se debe implementar la política y verificación DMARC, comenzando por implementar los estándares Sender Policy Framework (SPF) y DomainKeys Identified Mail (DKIM) para reducir la posibilidad de correos electrónicos falsificados o modificados de dominios válidos.  2.2 Se deben bloquear tipos de archivos innecesarios que intenten ingresar al portal de correo electrónico de la empresa.  2.3 Se deben implementar y mantener protecciones antimalware del servidor de correo electrónico, como escaneo de archivos adjuntos y/o zona de pruebas.  3. Instalar y activar herramientas de protección contra software malicioso en todas las instalaciones de procesamiento, con archivos de definición de software malicioso que se actualizan según sea necesario (automática o semiautomáticamente)  4. Implementar y respaldar la protección contra el malware mediante una adecuada concienciación del usuario. Se debe comunicar acerca de concienciación sobre software malicioso y hacer cumplir los procedimientos y responsabilidades de prevención.  5.Distribuir todo el software de protección centralmente (versión y parches) usando una configuración centralizada y la gestión de cambios de TI. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Incluir componentes del sistema que proactivamente busquen identificar código malicioso basado en la red o sitios web maliciosos.  2. Impartir formación periódica sobre malware en el uso de correo electrónico e Internet. Formar a los usuarios para que no abran e informen sobre correos electrónicos sospechosos y no instalen software compartido o no aprobado.  3. Revisar y evaluar la información sobre nuevas amenazas potenciales (p. ej., revisión de los consejos de seguridad de productos y servicios de proveedores) de forma regular. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Establecer objetivos e indicadores para la revisión y el cumplimiento de reglas y controles asociados. |
| 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. Se debe establecer un proceso de mejora continua según el análisis de desviaciones respecto a las metas y objetivos establecidos.  2. Documentar hallazgos y mejoras realizadas. |

1. **Preguntas de Auditoría para Reglas y Controles**

|  |
| --- |
| Temática: Uso de Software no Autorizado |
| Se busca tener bien definidas las reglas de instalación de software no validado por la empresa con fin de proteger a esta de posibles aplicaciones que puedan contener archivos malignos.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización realiza una validación periódica y automatizada del contenido de software y datos en sistemas que soportan procesos empresariales críticos?   + Solicite y revise informes o registros de validaciones automatizadas recientes en sistemas críticos para verificar la realización de estas validaciones.   + ¿Qué herramientas o soluciones se utilizan para llevar a cabo esta validación automatizada?   + ¿Cuál es la frecuencia y el alcance de estas validaciones automatizadas?   + ¿Cómo se determinan y mantienen las listas de software y datos aprobados que deben ser validados?     - Verifique la existencia de una lista actualizada de software y datos aprobados y compararla con la documentación de políticas y procedimientos.   + ¿Existen procedimientos de respuesta ante la detección de archivos no aprobados durante la validación?     - Revise la documentación de procedimientos de respuesta ante la detección de archivos no aprobados y verificar su existencia.   + ¿Cómo se comunican los resultados de las validaciones y las acciones tomadas en caso de detección de problemas?   + ¿Se lleva un registro de las actividades de validación automatizada, incluyendo los resultados y las acciones subsiguientes?     - Revise registros de actividades de validación automatizada que incluyan detalles sobre los resultados de las validaciones y las acciones tomadas en caso de problemas.     - Compare los registros de actividades con los informes de detección de problemas para verificar la consistencia y el seguimiento adecuado. * ¿La organización tiene un proceso establecido para instalar y actualizar periódicamente el software de detección y reparación de malware en todas las computadoras y medios de almacenamiento electrónico?   + Verifique si existe un calendario o programa establecido para las actualizaciones periódicas del software de detección de malware.   + ¿Se asigna responsabilidad clara para la instalación y actualización del software de detección y reparación de malware?   + ¿El software de detección y reparación de malware se actualiza de manera oportuna para abordar nuevas amenazas y vulnerabilidades?   + ¿Se lleva un registro de las actualizaciones y de la fecha en que se realizaron?   + ¿Se realizan pruebas de funcionamiento después de cada actualización del software de detección de malware? * ¿Cómo se distribuyen e implementan las actualizaciones en todas las computadoras y medios de almacenamiento electrónicos de la organización?   + Revise la documentación procedimientos relacionados con la distribución de actualizaciones para identificar el enfoque y el método utilizado (por ejemplo, parches, actualizaciones automáticas, etc.).   + Realice un muestreo de sistemas y medios de almacenamiento electrónicos para verificar si tienen instaladas las actualizaciones más recientes y si se ha seguido el proceso documentado.   + ¿Esto se realiza de manera automática?¿Se mantiene un registro de todas las actualizaciones distribuidas e implementadas?   + ¿Se realiza una evaluación de riesgos antes de distribuir e implementar actualizaciones?   + ¿Se espera a que los usuarios no estén trabajando para aplicar las actualizaciones?   + ¿Si existe un error a la hora de actualizar o instalar, existe un respaldo para volver al estado anterior de la actualización o instalación?   + ¿Se cuentan con planes de contingencia en caso de problemas o fallos durante la implementación de actualizaciones? * ¿Se realiza un escaneo completo y regular de todas las computadoras y dispositivos de almacenamiento electrónico en busca de malware?   + ¿Existe un proceso para gestionar y responder a las amenazas de malware detectadas durante los escaneos?   + ¿Se han definido intervalos de tiempo específicos para llevar a cabo los escaneos regulares en busca de malware en todas las computadoras y dispositivos de almacenamiento electrónicos?   + ¿Existe una documentación de cada escaneo realizado y si se encontraron amenazas de las acciones realizadas?     - ¿Los resultados de los escaneos en busca de malware se registran y almacenan de manera adecuada?   + ¿Se utiliza software de seguridad actualizado y adecuado para llevar a cabo los escaneos en busca de malware? * ¿La organización tiene una política o procedimiento formal que exige la instalación y activación de herramientas de protección contra software malicioso en todas las instalaciones de procesamiento?   + ¿La política o procedimiento establece claramente los tipos de herramientas de protección que deben ser instalados?   + ¿Cuál es el proceso de distribución e implementación de estas herramientas en todas las instalaciones de procesamiento?   + ¿Se establecen plazos claros para la instalación y activación de estas herramientas en nuevas instalaciones de procesamiento?   + ¿Existe un mecanismo de seguimiento o supervisión para garantizar el cumplimiento de esta política o procedimiento?   + ¿Existen procedimientos para verificar que todas las instalaciones de procesamiento tengan activadas y actualizadas las herramientas de protección contra software malicioso?   + ¿Los responsables de las instalaciones de procesamiento son conscientes de la política y procedimiento de protección contra software malicioso? |

|  |
| --- |
| Temática: Uso de Sitios Web Sospechosos |
| Al implementar reglas y controles al ingreso de sitios web sospechosos se busca minimizar la exposición a contenido malicioso que pueda comprometer tanto la información como los sistemas de la organización. Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización cuenta con un procedimiento formal para evaluar y determinar qué sitios web se rechazarán para prevenir o detectar el uso de sitios web potencialmente maliciosos?   + ¿Los criterios para evaluar sitios web sospechosos están claramente definidos en el procedimiento?     - Solicite y revise el procedimiento formal o guía que establece cómo se evalúan los sitios web y qué criterios se utilizan para determinar si un sitio web es sospechoso o malicioso.   + ¿Cómo se mantiene actualizada la lista de sitios web conocidos o sospechosos de ser maliciosos?¿Existe un registro documentado de los sitios web que han sido rechazados debido a sospechas de ser maliciosos?   + ¿Se ha designado un equipo o una persona responsable de llevar a cabo la evaluación de los sitios web? * ¿Se ha implementado un sistema de filtrado web para bloquear el acceso a sitios web maliciosos conocidos?   + Realice una revisión técnica del sistema de seguridad de la red para identificar la presencia de un sistema de filtrado web y verificar si está configurado para bloquear sitios web maliciosos conocidos.   + ¿Se utilizan servicios de filtrado DNS en todos los activos empresariales para bloquear el acceso a dominios maliciosos conocidos?     - ¿Se lleva un registro de incidentes relacionados con el acceso a sitios web maliciosos y se toman medidas adecuadas en respuesta a estos incidentes?   + ¿Se proporciona capacitación y concienciación al personal sobre la importancia de evitar sitios web maliciosos y cómo reconocerlos?   + ¿La organización cuenta con sistemas de prevención de intrusiones (IPS) o sistemas de detección de malware en su infraestructura de red?     - Realice un escaneo de la red para identificar la presencia de dispositivos IPS o software de detección de malware en la infraestructura.     - Evalúe los registros de eventos generados por los sistemas IPS y de detección de malware para verificar si están operando y detectando amenazas de manera efectiva.   + ¿Se ha establecido una frecuencia específica para verificar el correcto funcionamiento de los sistemas de detección de sitios web sospechosos?   + ¿Se lleva a cabo regularmente una revisión y actualización de las reglas y controles de sitios web sospechosos para garantizar su relevancia y eficacia?   + ¿Se realiza una evaluación periódica de la seguridad de acceso a sitios web sospechosos?     - Verifique la implementación de protocolos de cifrado (por ejemplo, HTTPS) en los sitios web sospechosos mediante un análisis de la configuración de seguridad. * ¿La organización cuenta con un sistema o herramienta de monitoreo de tráfico de red para detectar patrones o comportamientos inusuales?   + ¿Se establecen reglas y controles específicos para el monitoreo de patrones inusuales en el tráfico de red?¿Se documentan y comunican las alertas o hallazgos?     - ¿Se realiza un seguimiento constante de las métricas de rendimiento de estas herramientas para asegurar su eficacia?   + ¿Existe un procedimiento documentado para notificar y manejar alertas o incidentes relacionados con el acceso a sitios web maliciosos?     - ¿Cómo se notifican las alertas o incidentes relacionados con el acceso a sitios web maliciosos?       * ¿ Existe un plan de reacción frente a cualquier amenaza o incidente?       * ¿Se realiza un análisis y evaluación adecuados de las alertas o incidentes relacionados con el acceso a sitios web maliciosos?     - ¿Se tienen procedimientos establecidos para tomar medidas correctivas y preventivas en respuesta a alertas o incidentes relacionados con sitios web maliciosos?     - ¿Estos datos se encuentra correctamente asegurados solo accesibles por personal autorizado? |

|  |
| --- |
| Temática: Tráfico de Entrada |
| Auditando el tráfico de entrada lo que se busca es que la empresa tenga bien definidos los controles y las reglas en cuanto a la protección de los datos que llegan a redes y sistemas dentro de la empresa ya sea mediante ejercicios de escaneo , por acciones y reglas que el personal debe de cumplir.   * ¿La organización tiene una política o procedimiento formal que establece la práctica de escanear cualquier dato recibido a través de redes o medios electrónicos en busca de malware antes de su uso?   + ¿La política o procedimiento establece claramente quién es responsable de llevar a cabo los escaneos de malware en los datos recibidos?   + ¿La organización cuenta con herramientas o software de escaneo de malware para llevar a cabo esta práctica?   + ¿Se escanean todos los tipos de datos, incluyendo archivos adjuntos de correos electrónicos, descargas desde internet y archivos compartidos internamente?   + ¿Cómo se manejan los datos que se identifican como maliciosos durante el escaneo? * ¿La organización tiene establecido un mecanismo formal para que los usuarios informen sobre posibles datos maliciosos o sospechosos?   + ¿Los usuarios están informados sobre la existencia y el funcionamiento del mecanismo de notificación de datos maliciosos o sospechosos?¿El mecanismo de notificación se encuentra fácilmente accesible?   + ¿Se tiene constancia de todos los datos maliciosos informados por los usuarios?   + ¿Se lleva un registro de los resultados de las acciones tomadas en respuesta a las detecciones?     - Revise los registros de datos maliciosos informados por los usuarios y registro de resultado de acciones tomadas para responder a incidentes * ¿La organización tiene una política o procedimiento documentado para filtrar el tráfico de entrada?¿El filtrado de tráfico de entrada abarca correo electrónico y descargas de archivos?   + ¿Se establecen criterios claros para el filtrado de tráfico de entrada, como reglas de bloqueo o permisos?   + ¿Qué herramientas o soluciones tiene la organización para llevar a cabo el filtrado de tráfico de entrada?   + ¿Cómo se configuran y actualizan las reglas de filtrado para identificar y bloquear spyware, correos electrónicos de phishing y otros tipos de amenazas?   + ¿Con qué frecuencia se actualizan las bases de datos y firmas de amenazas utilizadas en el filtrado?   + ¿Se mantiene un registro de los resultados del filtrado, incluyendo las amenazas detectadas y las acciones tomadas? * ¿Se han establecido políticas y procedimientos específicos para proteger los correos electrónicos entrantes y salientes de amenazas como malware y correos electrónicos de phishing?   + Evalúe la implementación y seguimiento de estas políticas a través de registros de revisión y aprobación de políticas de seguridad.   + ¿Se utiliza un software de seguridad de correo electrónico o una solución antispam para detectar y bloquear correos electrónicos no deseados o maliciosos?   + ¿Se realizan análisis de contenido y escaneo de archivos adjuntos en los correos electrónicos entrantes?   + ¿Qué tipos de archivos están bloqueados en el portal de correo electrónico de la empresa?¿Las reglas y archivos bloqueados están correctamente documentadas? * ¿Se realiza un monitoreo constante del tráfico de correo electrónico en busca de archivos adjuntos maliciosos o zonas de pruebas potenciales? * ¿La organización ofrece capacitación regular a los usuarios sobre la importancia de las protecciones anti-malware en el correo electrónico y cómo pueden contribuir a la seguridad cibernética?   + ¿Quiénes son los encargado de realizar capacitación y concientización de los usuarios?   + Evalúe los registros de asistencia de los empleados a las sesiones de capacitación sobre seguridad de correo electrónico.   + ¿Se proporciona información clara y accesible a los usuarios sobre las mejores prácticas y pautas de seguridad relacionadas con el correo electrónico y anti-malware?   + ¿Se realizan pruebas de conocimientos o evaluaciones periódicas para medir la comprensión de los usuarios sobre las protecciones anti-malware en el correo electrónico? |