

**GASIC 6 – Seguridad en Redes**

**Preguntas de Auditoría**

**Configuración y Seguridad de los Activos**

**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 configuración y seguridad de los activos se centra en definir, gestionar y monitorear los elementos configurables de la infraestructura tecnológica, tales como servidores, dispositivos de red, aplicaciones y bases de datos, para garantizar su correcto funcionamiento y protegerlos frente a riesgos de ciberseguridad. Esto incluye mantener inventarios actualizados, establecer configuraciones base alineadas con los principios de seguridad, como la funcionalidad mínima, y aplicar controles rigurosos sobre los cambios realizados en estos activos. Este enfoque permite minimizar vulnerabilidades, asegurar la continuidad operativa y facilitar la trazabilidad de las modificaciones en los sistemas.

**1.1 Gestión de la Configuración y Componentes del Sistema**

La gestión de configuración comienza con la identificación y clasificación de los componentes configurables (CIs), tales como hardware, software, servicios y redes, que serán inventariados en un repositorio centralizado. Este inventario debe reflejar con precisión el estado actual del sistema, evitando duplicidades y asegurando un nivel de granularidad suficiente para facilitar el monitoreo y generación de reportes. Las configuraciones base deben incorporar principios de seguridad como la funcionalidad mínima, reduciendo las capacidades de los sistemas únicamente a lo necesario para sus operaciones.

Los procesos de control de cambios aseguran que cualquier modificación en los CIs sea documentada, aprobada y registrada adecuadamente. Esto incluye relacionar cada cambio con una solicitud formal aprobada, revisando regularmente las configuraciones actuales contra las líneas de referencia establecidas. Los cambios no autorizados deben ser detectados y reportados a los gestores responsables para su corrección inmediata.

**1.2 Seguridad de las Configuraciones y Monitoreo**

Las configuraciones de seguridad deben aplicar medidas restrictivas, como la gestión limitada de identidades privilegiadas, la desactivación de servicios innecesarios y el control estricto del acceso a configuraciones críticas. Asimismo, el uso de software antimalware es esencial, configurando escaneos automáticos y funciones anti-explotación para proteger los activos empresariales. Las configuraciones de referencia actualizadas deben mantenerse bajo control de configuración, permitiendo reversiones rápidas en caso de errores o incidentes.

El monitoreo continuo es clave para identificar cambios no autorizados, evaluar el cumplimiento de las configuraciones y mantener la integridad de los activos. Los informes deben incluir métricas relevantes que permitan tomar decisiones basadas en datos, garantizando la alineación con los objetivos de seguridad y operación.

**1.3 Auditoría y Actualización de las Configuraciones**

La auditoría de configuraciones debe enfocarse en validar la integridad y precisión del inventario de CIs, asegurando que refleje cambios autorizados y detecte desviaciones. La documentación de los procesos de configuración segura debe revisarse y actualizarse regularmente, especialmente tras eventos que afecten la infraestructura tecnológica. Además, las auditorías deben garantizar que los procesos de configuración reflejen un enfoque proactivo en la protección de los activos, fortaleciendo la resiliencia operativa y alineándose con las mejores prácticas de seguridad.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Definir y acordar el alcance y nivel de detalle sobre la gestión de la configuración, es decir, qué elementos configurables de servicios, activos e infraestructura incluir.  1.1 Se debe mantener una configuración de base de los sistemas de control industrial y de tecnología de la información con incorporación de los principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).  2. Identificar y clasificar CIs y poblar el repositorio o inventario centralizado de los componentes del sistema que:  2.1 Refleja con precisión el sistema.  2.2 Incluye todos los componentes dentro del sistema.  2.3 No incluye contabilidad duplicada de componentes o componentes asignados a cualquier otro sistema.  2.4 Tiene el nivel de granularidad que se considera necesario para el seguimiento y la generación de informes.  2.5 Revisa y acuerda formalmente las líneas de referencia de la configuración de un servicio, aplicación o infraestructura  3. Se deben encontrar establecidos procesos de control de cambio de la configuración.  4. Se deben Identificar los requisitos de reporte de todas las partes interesadas, incluyendo el contenido, la frecuencia y el medio.  4.1 Se deben producir informes conforme a los requisitos identificados. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Establecer y mantener un modelo lógico para la gestión de la configuración, incluida la información de los tipos de CI, atributos, tipos de relaciones, atributos de relaciones y códigos de estado.  2. Establecer, documentar y aplicar las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes que reflejen el modo más restrictivo consistente con los requisitos operativos. Para la configuración de seguridad de redes se debe incluir:  2.1 minimizar número de identidades con derechos de acceso de nivel privilegiado o de administrador.  2.2 desactivar identidades innecesarias, no usadas o inseguras;  2.3 desactivar o restringir funciones y servicios innecesarios.  2.4 restringir acceso a potentes programas de utilidad y a configuración de parámetros del servidor.  2.5 sincronizar relojes.  3. Implementar y mantener software antimalware en todos los activos empresariales. Esto incluye medidas como:  3.1 Deshabilitar la funcionalidad de ejecución y reproducción automáticas para medios extraíbles  3.1 Configurar el software antimalware para escanear automáticamente los medios extraíbles  3.1 Habilitar funciones anti-explotación en activos y software empresariales, cuando sea posible.  3.1 Utilizar software antimalware basado en el comportamiento  4. Desarrollar, documentar y mantener bajo control de configuración, una configuración de referencia actual del sistema |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Revisar y actualizar el inventario de componentes del sistema e Identificar regularmente todos los cambios a los CIs.  1.1 El mantenimiento remoto de los activos de la organización se debe aprobar, registrar y realizar de manera que evite el acceso no autorizado.  2. Revise y actualice la configuración de referencia del sistema frecuentemente o cuando se instalan o actualizan los componentes del sistema.  2.1 Retener versiones anteriores de configuraciones de referencia del sistema para admitir la reversión.  3. Se debe revisar y actualizar la documentación de los procesos de configuración seguros anualmente o cuando se produzcan cambios empresariales importantes que puedan afectar a los dispositivos de red |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Identificar los cambios de estado de los CIs y compararlos con las líneas de referencia |
| 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 deben actualizar los detalles de configuración para los cambios de CI aprobados.  1.1 Se deben relacionar todos los cambios de configuración con las solicitudes de cambio aprobadas para identificar los cambios no autorizados.  1.1.1 Informar sobre cambios no autorizados a los gestores de cambios.  1.2 Para asegurar la integridad y precisión, se deben revisar los cambios propuestos a los CIs comparándolos con las líneas de referencia. |

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

|  |
| --- |
| Temática: Identificación y Clasificación de Configuración de Items (CIs) |
| La identificación y clasificación de Configuraciones de Items (CIs) son esenciales en la gestión de la seguridad de activos, ya que permiten un rastreo preciso y una gestión efectiva de los recursos de una organización. Esto facilita la protección de activos críticos, la respuesta rápida a incidentes y el cumplimiento de requisitos de seguridad, contribuyendo en última instancia a mantener la integridad y disponibilidad de la infraestructura tecnológica de la organización.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización tiene políticas y procedimientos definidos para la identificación y clasificación de Configuraciones de Items (CIs)?   + ¿Cómo se determina qué elementos se consideran CIs en la organización?   + ¿Existe un proceso documentado para la identificación y clasificación de Configuraciones de Items (CIs)?   + ¿Se ha designado un equipo o individuo responsable de la identificación y clasificación de CIs?   + ¿El proceso de identificación y clasificación de CIs incluye criterios claros y definidos?   + ¿Cómo se asegura la precisión y actualización de la información de los CIs en el inventario centralizado? * ¿Se han implementado medidas de seguridad para proteger la información y los activos relacionados con las CIs?   + ¿Se ha realizado una evaluación de riesgos específica para identificar las amenazas y vulnerabilidades que podrían afectar a las CIs?   + ¿Existen procedimientos documentados para la implementación de medidas de seguridad específicas para las CIs?   + ¿Se han implementado controles de acceso adecuados para proteger la información y los activos relacionados con las CIs? * ¿La organización mantiene un inventario centralizado de todos los activos y CIs?   + ¿El inventario centralizado incluye todos los tipos de activos y CIs relevantes para la organización, como hardware, software, dispositivos de red, licencias y otros elementos críticos?   + ¿Se ha designado un equipo o un individuo responsable de mantener y actualizar el inventario centralizado de activos y CIs?   + ¿Cómo se garantiza que no haya contabilidad duplicada de componentes o componentes asignados a otros sistemas?   + ¿El inventario centralizado se actualiza de manera regular y precisa para reflejar los cambios en el entorno de activos y CIs de la organización?     - Evalúe la frecuencia de actualización del inventario centralizado y verificar si se realizan actualizaciones en tiempo real o periódicas. * ¿Cuáles son los procedimientos para gestionar y aprobar cambios en la configuración de los CIs?   + ¿Los procedimientos establecen claramente quién tiene la autoridad para aprobar cambios en la configuración de los CIs?   + ¿Se mantienen registros detallados de los cambios realizados en la configuración?   + ¿Se registran las razones y justificaciones de los cambios en la configuración?   + ¿Cómo se garantiza que los cambios sean reflejados de manera precisa en el inventario centralizado? |

|  |
| --- |
| Temática: Configuraciones de Seguridad |
| La práctica implica revisar y evaluar las medidas implementadas por una organización para garantizar que los activos estén configurados de manera segura y consistente con los requisitos operativos. El objetivo principal es verificar que se sigan prácticas adecuadas para minimizar riesgos y proteger los recursos de información.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización ha establecido, documentado y aplicado configuraciones de hardware, software, servicios y redes que reflejen el modo más restrictivo consistente con los requisitos operativos?   + Evalúe una muestra de activos, como servidores y estaciones de trabajo, para verificar que estén configurados de acuerdo con las políticas y procedimientos establecidos. * ¿Se han minimizado el número de identidades con derechos de acceso de nivel privilegiado o de administrador en la configuración de seguridad?   + ¿Se han desactivado las identidades innecesarias, no utilizadas o inseguras en la configuración de seguridad?   + Evalúe la configuración de seguridad para verificar que las cuentas inseguras o innecesarias estén desactivadas o eliminadas. * ¿Se han desactivado o restringido funciones y servicios innecesarios en la configuración de seguridad? * ¿Se ha restringido el acceso a potentes programas de utilidad y a la configuración de parámetros del servidor? * ¿Se ha sincronizado el reloj de los sistemas para garantizar la consistencia en los registros de eventos y las transacciones? |

|  |
| --- |
| 3.3 Temática: Configuración de Software Antimalware |
| Los software antimalware ayudan a proteger los activos de información, ya que estos programas identifican y eliminan malware, como virus, ransomware y troyanos, que pueden comprometer la integridad y la confidencialidad de la información. Los software antimalware desempeñan un papel fundamental al detectar y prevenir incidentes de seguridad. Ayudan a garantizar que los activos estén configurados de manera adecuada y protegidos contra amenazas externas e internas. Al mantener estos activos libres de malware, se promueve la confiabilidad, integridad y disponibilidad de la información.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización tiene software antimalware instalado en todos los activos empresariales?   + ¿Existe una política o procedimiento documentado para la configuración del software antimalware en todos los sistemas y activos empresariales?   + ¿Se deshabilita de manera efectiva la funcionalidad de ejecución y reproducción automáticas para medios extraíbles en todos los activos? * ¿Se han habilitado funciones anti-explotación en los activos y software empresariales donde sea posible?   + ¿Qué medidas se han tomado para garantizar que las funciones anti-explotación estén configuradas de manera efectiva y se actualicen regularmente?   + ¿La organización utiliza software antimalware basado en el comportamiento para detectar amenazas desconocidas y comportamientos maliciosos?   + ¿Cómo se monitorea y se asegura que el software antimalware basado en el comportamiento esté actualizado con las últimas definiciones de amenazas? * ¿El software antimalware genera informes y registros de actividad?   + ¿Se revisan regularmente los registros para identificar posibles incidentes de malware o configuraciones incorrectas?   + ¿Se lleva a cabo un inventario regular de activos empresariales para identificar los dispositivos en uso? * ¿La organización lleva a cabo evaluaciones periódicas de la efectividad de las medidas de seguridad antimalware?   + Revise la documentación organizacional, como políticas de seguridad, procedimientos y manuales, para verificar la existencia de un proceso documentado para evaluar la efectividad de las medidas antimalware.   + ¿Se realizan pruebas de penetración o simulacros de incidentes que involucran posibles amenazas de malware para evaluar la respuesta y la protección?   + ¿Las evaluaciones incluyen la revisión de la detección y respuesta a amenazas de malware?   + ¿Se toman medidas correctivas en función de las conclusiones de las evaluaciones de seguridad antimalware? |