

**CASIG 5 – Operaciones de Ciberseguridad**

**Preguntas de Auditoría**

**Establecer una línea base de configuración**

**Competencias Básicas del Auditor**

**1. Conocimiento en Sistemas de Información y Arquitecturas de TI:** Un auditor debe comprender cómo funcionan los sistemas de información, incluyendo hardware, software, redes y bases de datos. Debe estar familiarizado con las arquitecturas de TI más comunes y cómo se interconectan sus componentes.

**2.Entendimiento de Estándares y Marcos de Ciberseguridad:** Es esencial que el auditor conozca y comprenda los estándares y marcos de referencia en ciberseguridad, como ISO 27001, NIST SP 800-53 y CIS Controls. Estos proporcionan las mejores prácticas y directrices para la gestión de la configuración y otros aspectos de la ciberseguridad.

**3.Habilidades en Herramientas de Auditoría y Análisis:** El auditor debe ser competente en el uso de herramientas específicas de auditoría que permitan evaluar y analizar configuraciones, detectar vulnerabilidades y validar la conformidad con las políticas y estándares establecidos.

**4.Conocimiento en Gestión de Cambios y Control de Versiones:** Dado que la gestión de la configuración implica cambios constantes, el auditor debe entender cómo se gestionan, aprueban y documentan estos cambios. Además, debe conocer sistemas de control de versiones para rastrear y validar las modificaciones en los CIs.

**5.Competencia en Evaluación de Riesgos y Análisis de Impacto:** El auditor debe ser capaz de identificar y evaluar riesgos asociados con configuraciones inadecuadas o no autorizadas. Además, debe poder determinar el impacto potencial de cualquier desviación o vulnerabilidad en la seguridad y operatividad del sistema.

# Visión General

Una línea base de configuración actúa como un modelo de referencia que define el estado aceptado y seguro de los sistemas, facilitando tanto la administración de cambios como la recuperación en caso de incidentes. Mantener esta línea base permite a la organización responder eficazmente ante necesidades de rollback y gestionar de forma separada los ambientes de desarrollo, prueba y producción, asegurando que los sistemas críticos operen siempre bajo configuraciones autorizadas. Además, esta línea base permite ajustar configuraciones especiales para los activos que están expuestos a mayores riesgos, como los empleados que viajan a ubicaciones de mayor vulnerabilidad.

**1.1 Control de la Línea Base de Configuración**

La gestión de la línea base de configuración exige un control riguroso y un proceso de revisión continuo. Es fundamental mantener un repositorio que permita identificar y clasificar los elementos de configuración (CIs), lo que facilita la supervisión de cualquier cambio y su comparación con el estado de referencia. Cada cambio propuesto debe ser revisado minuciosamente para asegurar que se mantenga la precisión y consistencia con la configuración aprobada. Una vez que los cambios son autorizados, la línea base debe actualizarse para reflejar con precisión las configuraciones actuales y autorizadas del sistema.

**1.2 Auditoría de la Línea Base de Configuración**

Desde la perspectiva de auditoría, mantener la integridad y precisión de la línea base es clave para el cumplimiento de las políticas de la organización y el control eficiente de la infraestructura de TI. La auditoría se enfoca en revisar la vigencia de la configuración, la precisión de las relaciones entre los elementos de configuración y el cumplimiento de los indicadores de rendimiento establecidos, tales como la frecuencia de actualizaciones y la integridad del repositorio. A través de esta supervisión, la organización refuerza la seguridad de sus sistemas, asegurando que todos los cambios en la configuración sigan los procedimientos establecidos y mantengan la infraestructura bajo un control operativo seguro y eficiente.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Establecer y mantener un modelo lógico (línea base) 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. Mantener un numero definido de versiones anteriores de líneas base de configuración, para apoyar en caso de necesidad de rollback de los sistemas. 3. Mantener una línea base de configuración específica para los ambientes de desarrollo y prueba, que sea gestionada separada de la línea base de configuraciones para el ambiente de operaciones. 4. Asignar configuraciones especiales para los activos que sean usando por individuos que viajan a lugares que expongan a los activos de la organización a un mayor riesgo. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Identificar y clasificar CIs. Definir y poblar un repositorio de Cis. 2. 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) 3. Crear, revisar y acordar formalmente las líneas de referencia de la configuración de un servicio, aplicación o infraestructura |
| 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 la línea base de configuración de los sistemas periódicamente y cada vez que un nuevo sistema es instalado o actualizado. 2. Identificar regularmente todos los cambios a los Cis. 3. Revisar los cambios propuestos a los CIs comparándolos con las líneas de referencia, para asegurar la integridad y precisión. 4. Actualizar los detalles de configuración para los cambios de CI aprobados |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Monitorear y controlar los cambios de acuerdo con las políticas y procedimientos establecidos. 2. Establecer indicadores cuantitativos específicos para la medición del desempeño y rendimiento de esta actividad, tales como: 3. Número de partes interesadas que aprueban el modelo de configuración. 4. Porcentaje de precisión de las relaciones entre los elementos de configuración. 5. Número de elementos de configuración CIs listados en el repositorio. 6. Porcentaje de precisión sobre las líneas de referencia de la configuración de un servicio, 7. aplicación o infraestructura. 8. Frecuencia de cambios/actualizaciones al repositorio. 9. Porcentaje de precisión e integridad del repositorio de CIs. |
| 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 la vigencia, integridad, precisión y disponibilidad de la línea base de configuración de los sistemas utilizando mecanismos automatizados. |

1. **Preguntas de Auditoría para Establecer Líneas Base de Configuración**

|  |
| --- |
| Temática: Establecimiento de un Modelo Lógico para la Gestión de la Configuración |
| El establecimiento de un modelo lógico para la gestión de la configuración proporciona un marco estructurado para identificar, organizar y controlar las configuraciones de los sistemas de TI. Este modelo actúa como una columna vertebral para la gestión de la configuración, permitiendo a las organizaciones comprender cómo sus componentes de TI se interrelacionan y dependen unos de otros, facilitando así la identificación de los impactos potenciales de los cambios en la configuración. Al definir claramente las jerarquías, dependencias y relaciones entre los diferentes elementos de configuración, el modelo lógico ayuda a los auditores y al personal de TI a garantizar la coherencia, rastrear cambios y resolver rápidamente problemas relacionados con la configuración  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización tiene documentado un modelo lógico para la gestión de la configuración que incluye información sobre los tipos de CI, atributos, tipos de relaciones, atributos de relaciones y códigos de estado? * ¿Se realiza una revisión periódica del modelo lógico para asegurar su relevancia y actualización? * ¿Se capacita al personal responsable en la gestión y mantenimiento del modelo lógico? * ¿Se realizan auditorías internas para verificar la correcta implementación y seguimiento del modelo lógico? * ¿La organización tiene definido un número específico de versiones anteriores de líneas base que deben ser conservadas?   + ¿Se realiza un seguimiento y registro de las versiones anteriores de las líneas base? * ¿Existen procedimientos claros para realizar un rollback utilizando una versión anterior en caso de necesidad?   + ¿Se han realizado pruebas de rollback en el pasado para asegurar la efectividad del proceso?   + ¿El personal encargado está capacitado para realizar rollbacks de manera efectiva y en el menor tiempo posible? * ¿La organización mantiene líneas base separadas para los ambientes de desarrollo, prueba y operaciones?   + ¿Se realizan revisiones periódicas para asegurar que no haya mezcla o traslape entre las configuraciones de los diferentes ambientes?   + ¿Existen controles para evitar que cambios no autorizados en el   + ambiente de desarrollo o prueba afecten el ambiente de operaciones?   + ¿El personal está capacitado para gestionar y mantener separadas las líneas base de cada ambiente?   + ¿Se realizan auditorías específicas para verificar la separación y correcta gestión de las líneas base de cada ambiente? * ¿La organización tiene identificados los activos que requieren configuraciones especiales debido a los riesgos asociados con viajes?   + ¿Se realiza una revisión periódica de las configuraciones especiales para asegurar su efectividad y relevancia?   + ¿El personal encargado está capacitado para implementar y gestionar estas configuraciones especiales?   + ¿Se realizan pruebas y simulaciones para verificar la efectividad de las configuraciones especiales en escenarios reales de viaje?   + ¿Existen políticas y procedimientos claros para la asignación y gestión de estas configuraciones especiales?   + ¿Tiene la organización un sistema de liberación de un solo punto adecuado para la documentación de configuración (dibujos técnicos, especificaciones de diseño, ICD, instrucciones de trabajo/tarjetas de operación, especificaciones de proceso, dibujos de herramientas, etc.? * ¿Existen controles de acceso y seguridad para garantizar la integridad y confidencialidad de la información en el repositorio de CIs? |

|  |
| --- |
| Temática: Formalización de la Definición de la Línea Base de Configuración |
| La formalización de la definición de la línea base de configuración implica documentar de manera clara y detallada los estándares, configuraciones y parámetros aceptables para los sistemas y componentes de TI dentro de una organización. Este proceso establece un marco de referencia estandarizado que asegura que todos los sistemas estén configurados de manera segura y coherente, minimizando así las vulnerabilidades y los riesgos asociados.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existe un plan de dotación de personal para cumplir con requerimientos de * ¿La organización tiene un proceso formal y documentado para crear líneas de referencia de configuración? * ¿Existen procedimientos establecidos para la actualización y modificación del modelo lógico? * ¿La organización tiene documentado el alcance y nivel de detalle requerido para la gestión de la configuración?   + ¿Se han realizado reuniones o acuerdos formales con las partes interesadas para definir y acordar el alcance y nivel de detalle? * ¿Se revisa y actualiza periódicamente el alcance y nivel de detalle en función de las necesidades cambiantes de la organización? * ¿La organización tiene un proceso formal y documentado para identificar y clasificar CIs?   + Revisar la documentación que describe el proceso de identificación y clasificación de CIs. * ¿Existe un repositorio centralizado donde se almacenan y gestionan todos los CIs identificados?   + Solicitar acceso al repositorio y verificar su estructura y contenido. * ¿Se realiza una revisión periódica de los CIs en el repositorio para asegurar su actualización y relevancia?   + Solicitar registros de revisiones anteriores y fechas programadas para futuras revisiones. * ¿El personal encargado está capacitado en la identificación, clasificación y gestión de CIs en el repositorio? * ¿Existen criterios claros para determinar qué elementos configurables de servicios, activos e infraestructura se incluyen en la gestión de la configuración?  ¿Existen acuerdos formales con las partes interesadas para revisar y acordar las líneas de referencia de configuración? |

|  |
| --- |
| 3.3 Temática: Mejora Continua y Monitoreo de la línea Base de Configuración |
| La mejora continua y el monitoreo de la línea base de configuración no solo implica mantener una vigilancia constante sobre las configuraciones de los sistemas para asegurar su alineación con las líneas base establecidas, sino también adaptar y actualizar estas líneas base para reflejar las cambiantes condiciones de seguridad, tecnología y negocio.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se realiza una auditoría interna para verificar la correcta definición y acuerdo del alcance y nivel de detalle en la gestión de la configuración?   + ¿Qué metodología o herramienta se utiliza para identificar y registrar cambios en los CIs? ¿Se encuentra en línea con la política y prácticas de seguridad de la organización?   + ¿Con qué frecuencia se realiza la identificación de cambios en los CIs? * ¿Cómo se determina la frecuencia de revisión y actualización de la línea base de configuración de los sistemas? * ¿Existen registros que evidencien las revisiones y actualizaciones * realizadas a la línea base tras la instalación o actualización de un sistema? * ¿Se notifica a las partes interesadas pertinentes sobre las actualizaciones realizadas en la línea base de configuración, en los CI o en los detalles de configuración?   + Nota: Las notificaciones pueden ser esenciales para garantizar que todos los involucrados estén al tanto de los cambios y puedan actuar en consecuencia. * ¿Qué protocolo se sigue cuando se detectan discrepancias o inconsistencias durante la revisión de la línea base de configuración? * ¿Existen herramientas o software especializados que ayuden en la revisión y actualización automática de la línea base de configuración? * ¿Se mantiene un registro histórico de todos los cambios identificados en los CIs? * ¿Qué protocolo se sigue en caso de identificar cambios no autorizados o inesperados en los CIs? * ¿Cómo se lleva a cabo el proceso de revisión de los cambios propuestos en los CIs?   + ¿Existen criterios establecidos para aceptar o rechazar cambios propuestos en función de las líneas de referencia?   + ¿Se mantiene un registro de las revisiones realizadas y las decisiones tomadas respecto a los cambios propuestos?   + ¿Qué acciones se toman si se detecta que un cambio propuesto compromete la integridad o precisión de un CI?   + ¿Se realiza una validación posterior para asegurar que los cambios implementados en los CIs se alinean con las líneas de referencia? * ¿Qué proceso se sigue para actualizar los detalles de configuración tras la aprobación de cambios en los CIs?   + ¿Se verifica la correcta implementación de los cambios aprobados en los CIs? * ¿Cómo se asegura que los detalles de configuración actualizados reflejen fielmente los cambios aprobados?   + ¿Qué protocolo se sigue en caso de errores o inconsistencias * detectadas tras la actualización de los detalles de configuración? * ¿La organización utiliza métricas relevantes y específicas para la identificación de áreas de mejora? Algunos ejemplos de indicadores pueden ser:   + Número de partes interesadas que aprueban el modelo de configuración   + Porcentaje de precisión de las relaciones entre los elementos de configuración   + Número de elementos de configuración listados en el repositorio   + Porcentaje de precisión sobre las líneas de referencia de la configuración de un servicio, aplicación o infraestructura   + Frecuencia de cambios/actualizaciones al repositorio   + Porcentaje de precisión e integridad del repositorio de CIs |