

**CASIG 5 – Operaciones de Ciberseguridad**

**Preguntas de Auditoría**

**Verificar y revisar la integridad del repositorio 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

Un repositorio de configuración completo y preciso permite a la organización gestionar eficazmente sus elementos de configuración (CIs), identificando y resolviendo discrepancias antes de que puedan afectar las operaciones. Esta actividad incluye el uso de herramientas de descubrimiento para comparar configuraciones físicas y lógicas y la implementación de procesos de verificación regulares, lo que garantiza una alineación continua con las necesidades del negocio.

**1.1 Verificación y Comunicación de Desviaciones en el Repositorio de Configuración**  
La verificación periódica de los elementos de configuración frente al repositorio es esencial para identificar cualquier desajuste entre la configuración real y la documentada. Para ello, se emplean herramientas de descubrimiento adecuadas que facilitan la comparación de las configuraciones físicas y lógicas. En caso de identificar elementos no autorizados o desviaciones significativas, es importante que estas se comuniquen y se tomen las acciones correctivas necesarias, como la eliminación de activos no autorizados. La revisión constante asegura que todos los elementos físicos definidos en el repositorio existan realmente y se encuentren en conformidad con las configuraciones aprobadas.

**1.2 Auditoría de la Integridad y Precisión del Repositorio de Configuración**  
Desde la perspectiva de auditoría, es fundamental verificar la integridad y precisión del repositorio de configuración mediante una revisión continua de los objetivos de gestión de los CIs. Esta auditoría evalúa el cumplimiento del repositorio frente a las necesidades del negocio, asegurando que exista un proceso formal para la verificación, con roles, responsabilidades y actividades bien definidas. La comparación periódica de la integridad y precisión del repositorio se realiza mediante indicadores cuantitativos, como el número de desviaciones detectadas entre la configuración documentada y la real, y el número de discrepancias de información incompleta o faltante. Estas mediciones permiten que se implementen acciones correctivas de manera oportuna, mejorando la calidad y confiabilidad del repositorio y asegurando un entorno de TI bien controlado y alineado con los objetivos organizacionales.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Comprobar periódicamente los elementos de configuración reales con respecto al repositorio de configuración, mediante comparación de las configuraciones físicas y lógicas y el uso de 2. herramientas de descubrimiento adecuadas, conforme sea necesario. 3. Comunicar y revisar todas las desviaciones de las correcciones o acciones aprobadas para remover cualquier activo no autorizado. 4. Comprobar regularmente que todos los elementos de configuración físicos, conforme a lo definido en el repositorio, existen físicamente. 5. Informar de cualquier desviación a la dirección |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Establecer y revisar periódicamente el objetivo de la gestión de CI para completar el repositorio de configuración conforme con las necesidades del negocio. 2. Establecer formalmente un proceso de verificación de la integridad del repositorio de configuración con sus roles, responsabilidades y actividades para documentar las actividades |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. |  |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Comparar periódicamente el grado de integridad y precisión contra los objetivos y llevar a cabo acciones correctivas, conforme sea necesario, para mejorar la calidad de los datos del repositorio. 2. Establecer indicadores cuantitativos específicos para la medición del desempeño y rendimiento de esta actividad, tales como: 3. Número de desviaciones entre el repositorio de configuración y la configuración real. 4. Número de discrepancias en relación con la información de configuración incompleta o faltante. |
| 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. **Preguntas de Auditoría para Verificar y revisar la integridad del repositorio de configuración**

|  |
| --- |
| * 1. **Temática: Procesos de verificación y revisión de la integridad del repositorio** |
| Los procesos de verificación y revisión de la integridad del repositorio garantizan que la información almacenada sea precisa, consistente y segura. Estos procesos implican realizar auditorías regulares y evaluaciones sistemáticas para detectar cualquier incoherencia, corrupción de datos o accesos no autorizados.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Con qué frecuencia se realiza la comprobación de los elementos de configuración con respecto al repositorio?   + ¿Con qué frecuencia se verifica la existencia física de los elementos de configuración listados en el repositorio?   + Revisar la política o protocolo de revisión de configuración y comparar con registros históricos para validar la periodicidad. * ¿Qué herramientas de descubrimiento se utilizan para comparar configuraciones físicas y lógicas? * ¿Cómo se gestionan y resuelven las discrepancias identificadas entre los elementos de configuración reales y el repositorio? ¿Existen protocolos o procesos definidos?   + ¿Se siguen estos procesos para evitar situaciones de riesgo?   + ¿Qué protocolo se sigue para actualizar el repositorio de configuración en caso de identificar elementos desactualizados o faltantes?   + ¿Qué protocolo se sigue en caso de identificar elementos de configuración que no existen físicamente, pero están listados en el repositorio?   + Revisar la documentación o protocolos relacionados con la actualización del repositorio de configuración. * ¿Se mantiene un registro de todas las comprobaciones realizadas y las discrepancias identificadas?   + ¿Se mantiene un registro de todas las comprobaciones físicas realizadas y las discrepancias identificadas?   + Solicitar registros o informes de comprobaciones anteriores y analizar las acciones tomadas en caso de discrepancias. |

|  |
| --- |
| * 1. **Temática: Comunicación de las desviaciones** |
| La comunicación eficaz de las desviaciones en la configuración implica notificar a las partes interesadas pertinentes sobre cualquier diferencia encontrada entre las configuraciones actuales de los sistemas y las líneas base de configuración establecidas. Una comunicación oportuna y precisa permite a los equipos de seguridad, operaciones y gestión tomar decisiones informadas y actuar rápidamente para rectificar las desviaciones, mitigar posibles riesgos de seguridad y mantener la continuidad del negocio.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización utiliza mecanismos y canales formales y documentados para comunicar las desviaciones a las partes relevantes?   + Evaluar los canales de comunicación utilizados y solicitar ejemplos de comunicaciones recientes.   + ¿Qué mecanismo o proceso se utiliza para informar a la dirección sobre desviaciones identificadas?     - Evaluar los canales de comunicación utilizados para informar a la dirección y solicitar ejemplos de comunicaciones recientes. * ¿Con qué frecuencia se informa a la dirección sobre estas desviaciones? * ¿Se realiza un seguimiento de las desviaciones informadas a la dirección hasta su resolución? * ¿Se mantiene un registro histórico de todas las desviaciones informadas a la dirección y las acciones tomadas al respecto?   + Solicitar y revisar registros históricos para validar la comunicación y gestión adecuada de desviaciones con la dirección.   + Solicitar registros o informes que muestren el seguimiento y estado actual de las desviaciones comunicadas a la dirección. * ¿Cómo se verifica que la dirección ha tomado medidas adecuadas en respuesta a las desviaciones informadas?   + Entrevistar a miembros de la dirección para entender las acciones tomadas en respuesta a desviaciones informadas. * ¿Qué protocolo se sigue para remover activos no autorizados identificados a través de estas desviaciones?   + Revisar la política o protocolo relacionado con la gestión de activos no autorizados. |

|  |
| --- |
| 3.3 Temática: Formalización del proceso de verificación y revisión de integridad del repositorio de configuración |
| La formalización del proceso de verificación y revisión de la integridad del repositorio de configuración implica establecer procedimientos estandarizados y documentados para regularmente evaluar y asegurar que los datos dentro del repositorio de configuración permanezcan precisos, consistentes y libres de corrupción o alteraciones no autorizadas. La formalización ayuda a garantizar que todas las revisiones y verificaciones se realicen de manera sistemática, utilizando métodos validados y que cualquier hallazgo o desviación sea adecuadamente registrado y tratado.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existe un proceso documentado para la verificación de la integridad del repositorio de configuración?   + Solicitar y revisar la documentación o protocolo que describe el proceso de verificación de la integridad. Asegurarse de que esté formalmente establecido y aprobado por la dirección o las partes relevantes.   + ¿Cómo se definen y asignan los roles y responsabilidades dentro de este proceso de verificación?     - Dentro de la documentación del proceso, identificar las secciones que detallan los roles y responsabilidades. * ¿Cómo se establecen los objetivos, en el proceso, para la verificación del repositorio de configuración en función de las necesidades del negocio? * ¿Estos se encuentran en línea con los objetivos de la organización y la política general de seguridad?   + ¿Con qué frecuencia se revisan y actualizan estos objetivos?     - Revisar registros o actas de reuniones donde se discutan o revisen los objetivos del repositorio. Comparar con la política o protocolo establecido para validar la periodicidad de revisión.     - Revisar la documentación o estrategia donde se definen los objetivos del repositorio de configuración.     - ¿Qué mecanismos se utilizan para medir el progreso hacia el logro de estos objetivos?     - Solicitar informes o dashboards que muestren métricas relacionadas con el avance hacia los objetivos establecidos.     - Entrevistar al equipo encargado de la gestión de configuraciones para entender cómo monitorean y evalúan el progreso. * ¿Existen mecanismos de retroalimentación y mejora continua para el proceso de verificación de la integridad del repositorio? |