 2

**CASIG 5 – Operaciones de Ciberseguridad**

**Preguntas de Auditoría**

**Cierre y Post Implementación de los Cambios**

**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

El cierre de un cambio requiere formalizar la documentación asociada y evaluar el impacto real de las modificaciones realizadas en los procesos operativos. Este proceso asegura que las expectativas de negocio y las métricas de éxito definidas previamente sean verificadas, y que cualquier problema surgido tras la implementación sea gestionado adecuadamente. Además, se debe integrar la experiencia obtenida en los procedimientos para futuras solicitudes de cambio, garantizando una mejora continua.

**1.1 Gestión Documental y Evaluación Post-Implementación**

En el proceso de cierre, es fundamental definir períodos de retención adecuados para toda la documentación del cambio, asegurando que esta pase por un nivel de revisión similar al del cambio implementado. La documentación debe incluir procedimientos de negocio y TI, planes de continuidad y recuperación ante desastres, y materiales de capacitación. Adicionalmente, las revisiones post-implementación deben evaluar si los objetivos del negocio se han cumplido, los beneficios esperados se han alcanzado, y si los riesgos identificados se mitigaron con éxito. Este proceso involucra tanto a los dueños del negocio como a partes externas relevantes, garantizando una evaluación integral del impacto del cambio en la operación diaria.

**1.2 Auditoría, Seguimiento y Métricas de Desempeño**

Desde la perspectiva de auditoría, se debe verificar que las revisiones post-implementación estén alineadas con los procedimientos de gestión de cambios, asegurando que los informes de estado permitan rastrear cada cambio desde su solicitud inicial hasta su cierre final. El monitoreo continuo debe enfocarse en garantizar que los cambios aprobados se cierren oportunamente y que los pendientes sean gestionados según su prioridad. Adicionalmente, es crucial implementar métricas de rendimiento para medir el éxito de los cambios, como análisis de antigüedad de solicitudes y evaluación de beneficios logrados. Las pistas de auditoría y los sistemas de seguimiento permiten a la organización identificar y solucionar problemas detectados en esta etapa, con planes de acción claros y medibles.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Definir un período de retención adecuado para la documentación de los cambios y la documentación del sistema y del usuario antes y después del cambio.  2. Someter la documentación al mismo nivel de revisión que el cambio en sí mismo.  3. Llevar a cabo la revisión post-implementación conforme al proceso de gestión de cambios de la organización.  4. Categorizar las solicitudes de cambio en el proceso de seguimiento (p. ej., rechazado; aprobado, pero no iniciado; aprobado y en proceso; y cerrado). |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Incluir los cambios en la documentación en el procedimiento de gestión. Algunos ejemplos de documentación son: procedimientos operativos de negocio y de TI, documentación de continuidad del negocio y recuperación ante desastres, información de configuración, documentación de aplicaciones, pantallas de ayuda y materiales de capacitación.  2. Establecer procedimientos para garantizar que las revisiones post-implementación identifiquen, evalúen e informen sobre en qué medida han ocurrido los eventos siguientes: los requisitos de la empresa se han cumplido; los beneficios esperados se han logrado; el sistema se considera utilizable; las expectativas de las partes interesadas se han cumplido; han ocurrido impactos inesperados en la empresa; los riesgos clave se han mitigado; y los procesos de gestión de cambios, instalación y acreditación se han realizado de forma eficaz y eficiente.  3. Involucrar a los dueños del proceso de negocio y las terceras partes, como corresponda.  4. Implementar informes de estado de los cambios. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Considerar los requisitos para la revisión post-implementación que surjan de fuera del negocio y de TI (p. ej. auditoría interna, ERM, cumplimiento).  2. Asegurarse de que los informes de estado formen una pista de auditoría para que los cambios puedan rastrearse posteriormente, desde su inicio hasta su eventual disposición. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Consultar a los dueños del proceso de negocio y los directivos técnicos de TI sobre la elección de métricas para la medición del éxito y consecución de requisitos y beneficios.  2. Mantener un sistema de seguimiento e informes para todas las solicitudes de cambio  3. Establecer métricas de rendimiento para permitir la gestión de la revisión y la monitorización, tanto del estado detallado de los cambios como del estado general (p. ej., análisis de la antigüedad de las solicitudes de cambio).  4. Monitorizar los cambios abiertos para asegurarse de que todos los cambios aprobados se cierren de manera oportuna, según su prioridad. |
| 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. Acordar e implementar un plan de acción para solucionar los problemas identificados en la revisión post-implementación. Involucrar a los dueños del proceso de negocio y los directivos técnicos de TI en el desarrollo del plan de acción. |

1. **Preguntas de Auditoría para Revisar el cierre y la post implementación de los cambios**

|  |
| --- |
| Temática: Documentación asociada a los cambios y su retención |
| La evaluación debe verificar que la organización cumple con las obligaciones legales y regulatorias, mantiene un historial rastreable de actividades, facilita revisiones internas y auditorías, gestiona eficazmente los riesgos asociados con la gestión de cambios, evalúa la efectividad de los procesos y puede demostrar la conformidad con estándares y mejores prácticas, de manera documentada. En este aspecto, la retención adecuada de la documentación es esencial para mantener la integridad, la responsabilidad y la transparencia en todo el ciclo de vida de los cambios en una organización.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se ha definido un período de retención adecuado para la documentación de los cambios y la documentación del sistema y del usuario antes y después del cambio?   + ¿Se somete la documentación al mismo nivel de revisión que el cambio en sí mismo? * ¿Cómo se documentan los cambios realizados, incluyendo detalles sobre la justificación, el proceso de aprobación y la implementación? * ¿Cuáles son los procedimientos para la retención de la documentación de cambios y cómo se garantiza el acceso a largo plazo a estos registros? * ¿Existen mecanismos de seguridad para proteger la documentación de cambios contra acceso no autorizado o pérdida de información? * ¿Cómo se realiza la revisión y actualización de la documentación de cambios para reflejar cualquier ajuste o modificación posterior a la implementación? |

|  |
| --- |
| Temática: Categorización y el proceso de post-Implementación de los cambios |
| Durante la evaluación, se debe revisar cómo los cambios son categorizados según su tipo, urgencia e impacto, y cómo esta categorización influye en las revisiones de eficacia posteriores. Además, se deben evaluar los métodos que la organización emplea para medir el éxito de los cambios, incluyendo la evaluación de cualquier repercusión no anticipada y la efectividad de las soluciones implementadas.  Este levantamiento puede incluir análisis específicos tales como:  **3.2.1 Revisar la categorización**   * ¿Se categorizan adecuadamente las solicitudes de cambio en el proceso de seguimiento? Por ejemplo: estados como rechazado, aprobado, pero no iniciado, aprobado y en proceso, y cerrado.   **3.2.2 Revisar conformidad con el proceso de gestión de cambios de la organización**   * ¿La organización lleva a cabo la revisión post-implementación conforme al proceso de gestión de cambios de la organización? * ¿Se incluyen los cambios en la documentación en el procedimiento de gestión abarcando áreas como procedimientos operativos, continuidad del negocio, información de configuración y documentación de aplicaciones?   **3.2.3 Revisar el proceso de post-implementación**   * ¿Se han establecido procedimientos para garantizar que las revisiones post-implementación evalúen el cumplimiento de requisitos empresariales, beneficios esperados, usabilidad del sistema y otras métricas relevantes? * ¿Se involucran adecuadamente a los dueños de procesos de negocio y terceras partes en las revisiones post-implementación, según corresponda? * ¿Se implementan informes de estado de los cambios para mantener a todas las partes interesadas informadas sobre el progreso de los cambios? * ¿Se consideran los requisitos de revisión post-implementación que puedan surgir de fuentes externas al negocio y a TI, como auditoría interna, gestión de riesgos empresariales (ERM) y cumplimiento? * ¿Se asegura de que los informes de estado generen una pista de auditoría sólida para rastrear los cambios desde su inicio hasta su disposición final?   **3.2.4 Revisar métricas y seguimiento de solicitudes de cambio**   * ¿Se involucra a los responsables de procesos de negocio y a líderes de TI en la definición de indicadores clave de rendimiento (KPI’s) para evaluar el éxito y el logro de requisitos y beneficios en relación con las solicitudes de cambio? * ¿Existe un sistema de seguimiento y generación de informes que proporcione información detallada sobre el estado, prioridad y antigüedad de todas las solicitudes de cambio? * ¿Se han implementado métricas de rendimiento que permitan la revisión y monitorización efectiva tanto a nivel de cambios individuales como en un contexto general?   **3.2.5 Monitorización y Resolución de Problemas Post-Implementación:**   * ¿Se lleva a cabo una supervisión regular de las solicitudes de cambio pendientes para asegurarse de que todas las aprobadas se cierren en tiempo y forma, conforme a su nivel de prioridad y requisitos? * ¿La organización cuenta con un procedimiento establecido y un plan de acción para abordar las deficiencias y problemas identificados durante las revisiones post-implementación de los cambios?   + ¿Se asegura la participación de los dueños de procesos de negocio y líderes de TI en la elaboración y ejecución de dicho plan? |