

**CASIG 5 – Operaciones de Ciberseguridad**

**Preguntas de Auditoría**

**Planificar, Evaluar y Priorizar las solicitudes del cambio**

**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 gestión estructurada de las solicitudes de cambio permite garantizar que los ajustes en procesos, sistemas e infraestructura sean coherentes con las necesidades del negocio y se realicen con un impacto mínimo en el entorno operativo. Este enfoque prioriza la alineación con los objetivos organizacionales y regula cada etapa del proceso, desde la recepción de solicitudes hasta la implementación final.

**1.1 Gestión Estructurada y Priorización de Solicitudes de Cambio**

Todas las solicitudes de cambio deben originarse y gestionarse exclusivamente a través de un proceso formal, utilizando herramientas y procedimientos que aseguren su trazabilidad. Estas solicitudes deben ser categorizadas en función de su impacto potencial en los procesos de negocio, infraestructura, aplicaciones y sistemas, considerando requisitos técnicos, legales y regulatorios. La evaluación incluye análisis detallados de impacto, interdependencias y riesgos operativos, priorizando las solicitudes en función de su urgencia y valor estratégico para la organización. Es esencial involucrar a los dueños de procesos de negocio y partes interesadas técnicas en la evaluación para garantizar que los cambios estén alineados con las metas operativas y regulatorias.

**1.2 Auditoría y Monitoreo de la Implementación de Cambios**

Desde la auditoría, se debe verificar que todas las solicitudes hayan sido aprobadas formalmente y documentadas, asegurando que cada cambio cuenta con un análisis previo de impacto. Las auditorías revisan las pruebas realizadas en entornos controlados, confirmando que los riesgos han sido mitigados antes de la implementación en vivo. Adicionalmente, es crítico mantener un registro de las conversiones de datos y los procesos asociados, incluyendo copias de seguridad y validaciones de integridad de datos. El monitoreo continuo debe confirmar que los planes de recuperación, rollback y fallback están activos y preparados, minimizando las interrupciones ante posibles fallos en la transición. Las auditorías de cambios estándar permiten verificar la eficiencia de procesos recurrentes y la pre-aprobación de cambios de bajo riesgo.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Asegurarse de que todos estos cambios surjan solo a través del proceso de gestión de solicitudes de cambio.  2. Priorizar todos los cambios solicitados basándose en los requisitos de negocio y técnicos, recursos requeridos y las razones legales, regulatorias y contractuales para el cambio solicitado.  3. Planificar y programar todos los cambios aprobados.  4. Planificar, evaluar y categorizar todas las solicitudes de una manera estructurada (p. ej., procesos de negocio, infraestructura, sistemas operativos, redes, sistemas de aplicación, software de aplicación comprado/empaquetado, planes de continuidad del negocio (BCP)) . Incluir un análisis de impacto para asegurarse de que se hayan identificado todos los componentes afectados.  5. Evaluar la probabilidad de afectar negativamente el entorno operativo y el riesgo de implementar el cambio. Considerar las implicaciones de seguridad, privacidad, legales, contractuales y de cumplimiento del cambio solicitado. Considerar también las interdependencias entre los cambios.  6. Involucrar a los propietarios de los procesos de negocio en el proceso de evaluación, cuando sea conveniente.  7. Considerar el impacto de los proveedores de servicios contratados (p. ej., de procesamiento de negocio , infraestructura, desarrollo de aplicaciones y servicios compartidos externalizados) en el proceso de gestión de cambios.  8. Incluir la integración de los procesos de gestión de cambios organizativos con los procesos de gestión de cambios de los proveedores de servicios y el impacto en términos contractuales y SLA.  9. Confirmar que el plan de conversión de datos no requiere cambios en los valores de los datos, a menos que sea absolutamente necesario por razones de negocio.  10. Ensayar y probar la conversión antes de intentar una conversión en vivo.  11. Coordinar y verificar los tiempos e integridad de la transición de la conversión rápida para que se produzca una transición continua y uniforme sin que se pierdan datos en la transición. Cuando sea necesario, si no existe otra alternativa, congelar las operaciones en vivo.  12. Planificar una copia de seguridad de todos los sistemas y datos recopilados en el momento previo a la conversión.  13. Componer un consejo de asesores, p.e. el consejo asesor de cambios (CAB) y el CAB de emergencia (ECAB), para el apoyo en la evaluación y priorización de cambios. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Usar solicitudes de cambio formales para permitir a los propietarios de los procesos de negocio y a TI solicitar cambios a procesos de negocio, infraestructura, sistemas o aplicaciones.  2. Aprobar formalmente cada cambio por parte de los dueños de los procesos de negocio, gestores de servicios y partes interesadas técnicas de TI, según corresponda.  3. Documentar los cambios realizados en los valores de los datos.  4. Los cambios que son de bajo riesgo y relativamente frecuentes deben pre-aprobarse como cambios estándar.  5. Definir un plan de migración del proceso de negocio, de los datos de servicios y de la infraestructura. En el desarrollo del plan, considerar, por ejemplo, el hardware, las redes, los sistemas operativos, el software, los datos de transacción, los archivos maestros, las copias de seguridad y archivos, las interfaces con otros sistemas (internos y externos), los posibles requisitos de cumplimiento, los procedimientos de negocio y la documentación del sistema.  5.1 Incorporar en el plan de conversión de datos métodos para recopilar, convertir y verificar los datos a convertir, e identificar y resolver cualquier error encontrado durante la conversión. Incluir la comparativa de los datos originales con los convertido para comprobar su integridad y que están completos.  6. En el plan de conversión del proceso de negocio, considerar todos los ajustes necesarios de los procedimientos, incluyendo la revisión de roles y responsabilidades y procedimientos de control.  7. Planificar la retención de los datos de copias de seguridad y archivados de acuerdo con las necesidades del negocio y los requisitos de cumplimiento o regulatorios. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Garantizar que haya un plan de recuperación que cubra el rollback de la migración y el fallback al procesamiento anterior si la migración falla.  2. Considerar el riesgo de los problemas de conversión, planificación de la continuidad del negocio y procedimientos de fallback en el proceso de negocio, plan de migración de datos e infraestructura en los que haya gestión de riesgo, necesidades del negocio o requisitos de cumplimiento/regulatorios.  3. Mantener pistas de auditoría para poder tener un registro de los pasos de la conversión. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles |  |
| 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 Evaluar, priorizar y autorizar solicitudes de cambio**

|  |
| --- |
| Temática: Evaluación, Priorización y Autorización de solicitudes de cambio |
| El auditor debe asegurarse que la organización sigue un proceso estructurado y transparente para gestionar las solicitudes de cambio, para verificar que las modificaciones en procesos, sistemas y tecnologías se realicen de manera controlada y alineada con los objetivos del negocio.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización cuenta con un consejo asesor de cambios (CAB) y un consejo asesor de cambios emergencia (ECAB) para apoyar el proceso de evaluación y priorización de los cambios?   + ¿Quiénes componen el CAB y el ECAB?   + ¿Participan otras partes interesadas en este proceso? * ¿Se utiliza un proceso formal de gestión de solicitudes de cambio para registrar todas las solicitudes de cambio en la organización? * ¿Se evalúan de manera estructurada todas las solicitudes de cambio según su tipo (por ejemplo, procesos de negocio, infraestructura, sistemas operativos, redes, sistemas de aplicación, entre otros)?   + ¿Cómo se aseguran de que se hayan identificado todos los componentes afectados? * ¿La organización evalúa la probabilidad de afectar negativamente el entorno operativo y el riesgo de implementar el cambio?   + ¿Se evalúa el impacto hacia los proveedores externos? * ¿Se priorizan las solicitudes de cambio de acuerdo con criterios claros, como requisitos de negocio, recursos requeridos y razones legales, regulatorias y contractuales? * ¿Están documentados los criterios utilizados para determinar qué cambios son considerados de bajo riesgo? |

|  |
| --- |
| Temática: Planificación de la conversión de procesos de negocio, sistemas y datos |
| Para garantizar que la organización esté preparada para realizar cambios críticos de manera controlada y eficiente, el auditor debe revisar que se contemple un plan de conversión adecuado asegurando que los procesos se migren sin interrupciones significativas, que los datos se conserven con precisión y que cualquier cambio en los valores de los datos esté justificado. Además, esta revisión de la planificación de la conversión permite al auditor identificar riesgos relacionados con la pérdida de datos, la interrupción de servicios críticos y el incumplimiento de requisitos legales y regulatorios.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización cuenta con un plan formal gestión de los cambios aprobados?   + ¿El plan garantiza que no se cambien los valores de los datos a menos que sea necesario por razones de negocio?   + ¿El plan solicita una justificación en los valores de los datos modificados?   + ¿Los cambios aprobados son programados?   + ¿La organización lleva un registro de los cambios efectuados? * ¿Se realizan ensayos y pruebas de la conversión antes de intentar una conversión en vivo? * ¿Se coordina y verifica el tiempo y la integridad de la transición de la conversión rápida para evitar la pérdida de datos?   + ¿Se contempla algún procedimiento en caso de que se pierdan datos en la transición? * ¿Se planea una copia de seguridad de todos los sistemas y datos antes de la conversión? * ¿Se documentan los cambios realizados en los valores de los datos y se obtiene la aprobación del dueño de los datos del proceso de negocio, gestores de servicio y partes interesadas técnicas de TI? * ¿Se revisan y actualizan los roles y responsabilidades durante el proceso de conversión? * ¿Se documentan los procedimientos de control implementados durante la conversión? * ¿Se mantienen registros de pistas de auditoría que permitan un seguimiento detallado de los pasos de la conversión?   **3.2.1 Revisar Plan de Migración**   * ¿Existe un plan de migración integral que cubra el proceso de negocio, los datos de servicios y la infraestructura? * ¿Se documentan todos los componentes considerados en el plan de migración, como hardware, redes, sistemas operativos, software, datos de transacción, archivos maestros y otros? * ¿Se incluyen en el plan de conversión de datos métodos específicos para recopilar, convertir y verificar los datos, así como la resolución de errores? * ¿Se realiza una comparativa entre los datos originales y los convertidos para verificar su integridad y completitud? * ¿Se consideran los requisitos de cumplimiento y regulatorios en el plan de migración? * ¿La organización cuenta con un plan de recuperación que incluya el rollback de la migración y el fallback al procesamiento anterior en caso de falla en la migración? |