 2

**CASIG 5 – Operaciones de Ciberseguridad**

**Preguntas de Auditoría**

**Gestionar las Liberaciones de 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

La liberación de cambios es el proceso mediante el cual se introducen nuevas funcionalidades, sistemas o actualizaciones en un entorno operativo, garantizando que estas modificaciones sean implementadas de forma controlada y segura. Este proceso asegura que los cambios sean entregados con el mínimo impacto en las operaciones, cumpliendo con los objetivos técnicos y de negocio, y que se mantenga la estabilidad del entorno tras la implementación.

**1.1 Transferencia y Control de Cambios**

La gestión de las liberaciones comienza con la preparación para la transferencia de servicios y aplicaciones desde pruebas a producción. Este proceso debe alinearse con los estándares de gestión de cambios organizativos e incluir la validación de las implementaciones piloto o paralelas para garantizar que estén en línea con los planes establecidos. Además, los procedimientos deben asegurar que las promociones a producción de sistemas y software estén bajo el control de configuración, mientras que toda la documentación asociada, como información de configuración y planes de contingencia, se actualiza rápidamente. Cuando los componentes de la solución se distribuyen electrónicamente, es fundamental que el sistema controle la distribución automática para garantizar que solo llegue a usuarios autorizados, notificando oportunamente sobre la liberación.

**1.2 Auditoría y Monitoreo de Liberaciones**

Desde el punto de vista de auditoría, se debe revisar que los procedimientos de control de cambios cubran aspectos críticos como la planificación del impacto, pruebas previas a la liberación, y la autorización formal de cambios. El mantenimiento de registros detallados permite rastrear todas las etapas de la liberación, desde la planificación inicial hasta la implementación final. Adicionalmente, la auditoría debe verificar la existencia de copias de seguridad que respalden los cambios y de procedimientos de rollback documentados para casos de contingencia. El monitoreo continuo tras la liberación debe evaluar la estabilidad del entorno operativo, garantizando la confidencialidad, integridad y disponibilidad de los sistemas y la información, además de confirmar que los recursos adicionales asignados se gestionen adecuadamente hasta que el entorno estabilizado cumpla con los estándares requeridos.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Prepararse para la transferencia de procedimientos del negocio y servicios de soporte, aplicaciones e infraestructura desde el entorno de pruebas al entorno de producción conforme a los estándares de gestión de cambios organizativos.  2. Determinar hasta qué punto la implementación del piloto o el procesamiento paralelo de los sistemas nuevos y viejos está en línea con el plan de implementación.  3. Asegurar que la promoción a producción de sistemas, software de aplicaciones e infraestructura esté bajo el control de configuración.  4. Actualizar rápidamente la documentación del proceso de negocio y del sistema, la información de configuración y los documentos de planes de contingencia relevantes, conforme corresponda.  5. Garantizar que todas las bibliotecas de medios se actualizan rápidamente con la versión del componente de la solución transferido del entorno de pruebas al entorno de producción. Archivar la versión actual y su documentación soporte.  6. Si la distribución de componentes de soluciones se lleva a cabo de forma electrónica, controlar la distribución automática para garantizar que se notifica a los usuarios y que la distribución solo se realiza a destinatarios autorizados correctamente identificados.  7. Proporcionar recursos adicionales, cuando se requiera, a los usuarios finales y personal de soporte hasta que se estabilice la liberación.  8. Proporcionar recursos de sistemas de seguridad de la información adicionales, conforme se requiera, hasta que el lanzamiento esté en un entorno operativo estable.  9. La introducción de nuevos sistemas y de cambios importantes en los sistemas existentes debería seguir reglas acordadas y un proceso formal de documentación, especificación, prueba, control de calidad e implementación gestionado. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Incluir procedimientos de copia de seguridad en el proceso de liberación (release) para permitir que la distribución de los cambios se revise en caso de falla o error.  2. Si la distribución se hace de forma física, mantener un registro formal de qué elementos se han distribuido, a quién y dónde se han implementado y cuándo se ha actualizado cada uno de ellos.  3. Para garantizar un control satisfactorio de todos los cambios, deberían existir responsabilidades y procedimientos de gestión.  4. Los procedimientos de control de cambios deberían documentarse y aplicarse para garantizar la  confidencialidad, integridad y disponibilidad de la información en las instalaciones de tratamiento de la información y en los sistemas de información, desde las primeras etapas de diseño, durante todo el ciclo de vida del desarrollo del sistema, y durante todos los esfuerzos de mantenimiento posteriores.  5. Siempre que sea factible, deberían integrarse los procedimientos de control de cambios para la  infraestructura TIC y para el software.  6. Los procedimientos de control de cambios deberían incluir:  6.1 la planificación y evaluación del impacto potencial de los cambios considerando todas las  dependencias.  6.2 la autorización de cambios.  6.3 la comunicación de los cambios a las partes interesadas pertinentes.  6.4 las pruebas y la aceptación de pruebas previa a los cambios.  6.5 la implementación de cambios, incluidos los planes de implementación.  6.6 las consideraciones de emergencia y contingencia, incluidos los procedimientos de vuelta atrás.  6.7 el mantenimiento de registros de cambios que incluyan todo lo anterior.  6.8 la garantía de cambio de la documentación operativa y de los procedimientos del usuario cuando sea necesaria para que continúen siendo adecuados.  6.9 la garantía de modificación de los planes de continuidad de las TIC y de los procedimientos de  respuesta y recuperación cuando sea necesario, para continúen siendo adecuados. |
| 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 |  |
| 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 la Gestión de las Liberaciones de Cambios**

|  |
| --- |
| Temática: Promoción a producción y gestión de las liberaciones |
| Este proceso implica examinar cómo la organización planifica, prueba, aprueba y finalmente promueve los cambios al entorno de producción. El auditor debe enfocarse en la rigurosidad del proceso de pruebas para garantizar que los cambios no introduzcan vulnerabilidades o errores en los sistemas operativos. Además, es importante evaluar cómo se documentan y comunican las liberaciones, asegurándose de que todas las partes interesadas estén informadas y preparadas para los cambios.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se siguen estándares organizativos para la transferencia de procedimientos del negocio y servicios de soporte, aplicaciones e infraestructura desde el entorno de pruebas al entorno de producción? * ¿Se realiza una evaluación adecuada del piloto o procesamiento paralelo de los sistemas nuevos y viejos en línea con el plan de implementación? * ¿Existe un control de configuración efectivo para la promoción a producción de sistemas, software de aplicaciones e infraestructura? * ¿Se actualiza la documentación del proceso de negocio y del sistema, así como la información de configuración y los documentos de planes de contingencia de manera oportuna? * ¿Se asegura que todas las bibliotecas de medios se actualicen correctamente con la versión del componente transferido al entorno de producción y se archive la versión anterior con su documentación de soporte? * ¿Se proporcionan recursos adicionales a los usuarios finales y al personal de soporte hasta que la liberación esté estabilizada? * ¿Existen responsabilidades y procedimientos de gestión claramente definidos para garantizar un control efectivo de todos los cambios? * ¿Los procedimientos de control de cambios están documentados y se aplican para garantizar la confidencialidad, integridad y disponibilidad de la información? * ¿Se integran los procedimientos de control de cambios para la infraestructura TIC y el software? * ¿Los procedimientos de control de cambios incluyen todas las etapas, desde la planificación hasta la modificación de planes de continuidad y procedimientos de respuesta y recuperación cuando sea necesario? |

|  |
| --- |
| Temática: Control de Distribución de Cambios |
| Este proceso involucra la supervisión y regulación de cómo los cambios son distribuidos y aplicados a través de diferentes sistemas y plataformas para mantener la coherencia y minimizar los riesgos operacionales y de seguridad. En este contexto, el auditor debe evaluar la eficacia con la que la organización maneja la distribución de cambios, incluyendo la verificación de que todos los cambios se realicen de acuerdo con los procedimientos establecidos y que se sigan las políticas de seguridad adecuadas.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se controla la distribución automática de componentes de soluciones electrónicamente, notificando a los usuarios autorizados y garantizando que la distribución solo se realice a destinatarios debidamente identificados? * ¿Se proporcionan recursos adicionales a usuarios finales y personal de soporte hasta que la liberación de cambios esté estabilizada? * ¿Se asignan recursos de sistemas de seguridad de la información adicionales según sea necesario hasta que la liberación esté operativa de manera estable? * ¿Los procedimientos formales se siguen rigurosamente para la introducción de nuevos sistemas y cambios importantes en sistemas existentes, incluyendo documentación, especificación, prueba, control de calidad e implementación gestionada? * ¿Se incluyen procedimientos de copia de seguridad en el proceso de liberación para permitir la revisión de cambios en caso de falla o error? * Si la distribución se realiza físicamente, ¿se mantiene un registro formal de elementos distribuidos, destinatarios, ubicaciones de implementación y fechas de actualización? |

|  |
| --- |
| Temática: Soporte Oportuno en Producción |
| Este aspecto de la gestión de cambios se centra en asegurar que haya asistencia disponible rápidamente para abordar cualquier problema que surja tras la implementación de cambios en el entorno de producción. El auditor debe evaluar cómo la organización proporciona soporte continuo y eficaz, revisando los protocolos de respuesta a incidentes y los niveles de servicio acordados para asegurar que se cumplen las expectativas y necesidades del negocio.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se garantiza el soporte oportuno en producción para resolver problemas y mantener la estabilidad del entorno de producción? * ¿Existe un punto focal único para coordinar y proporcionar soporte en producción? * ¿Se siguen reglas y procedimientos documentados para la resolución de problemas y la gestión de incidentes en el entorno de producción? * ¿Se realizan evaluaciones de riesgo y se toman medidas de contingencia en caso de problemas críticos en producción? * ¿Se registra y documenta adecuadamente la resolución de problemas y la atención de incidentes en producción? |

|  |
| --- |
| Temática: Preservación de la Seguridad de la Información al Ejecutar Cambios |
| Esta evaluación se centra en asegurar que todos los cambios realizados en los sistemas no comprometan la integridad, confidencialidad y disponibilidad de la información. Al revisar esta área, el auditor debe verificar que existan procedimientos para revisar y ajustar las medidas de seguridad en respuesta a los cambios, asegurando que se mantengan alineados con las políticas de seguridad de la organización y las regulaciones pertinentes.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se siguen procedimientos específicos para garantizar la preservación de la seguridad de la información al ejecutar cambios? * ¿Se evalúa y documenta el impacto de los cambios en la seguridad de la información? * ¿Se toman medidas para garantizar la confidencialidad, integridad y disponibilidad de la información durante la implementación de cambios? * ¿Se documentan y mantienen registros de cambios relacionados con la seguridad de la información, incluyendo las evaluaciones de impacto y las medidas de seguridad implementadas? |