 2

**CASIG 5 – Operaciones de Ciberseguridad**

**Preguntas de Auditoría**

**Establecer el Proceso de Gestión 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

El proceso de gestión de cambios regula cómo se introducen modificaciones en los sistemas, procesos y políticas de una organización, garantizando que estas sean planificadas, evaluadas y ejecutadas de manera controlada. Esto incluye la coordinación entre las partes interesadas, la mitigación de riesgos técnicos y de negocio, y el cumplimiento de normativas de seguridad y operativas. Además, establece los procedimientos necesarios para asegurar la continuidad de las operaciones frente a cualquier alteración planificada o emergente.

**1.1 Diseño y Estructura del Proceso de Gestión de Cambios**

El diseño del proceso debe centrarse en mitigar cualquier efecto adverso de los cambios, controlando específicamente aquellos que afectan la seguridad de la información o la estabilidad operativa. Esto incluye la asignación de roles y responsabilidades claras para cada actor involucrado, así como la creación de consejos asesores, como el CAB y el ECAB, que supervisan y autorizan las modificaciones según su urgencia. Un plan de implementación detallado es esencial, considerando la estrategia global, los pasos específicos de implementación, los recursos necesarios, los criterios de aceptación y los procesos de recuperación. Adicionalmente, se debe garantizar la existencia de planes de fallback y remediación que permitan la continuidad operativa en caso de fallos durante la implementación.

**1.2 Auditoría y Seguimiento del Proceso de Gestión de Cambios**

Desde la auditoría, es imprescindible revisar que cada cambio esté respaldado por un registro claro, desde su solicitud inicial hasta su cierre. El procedimiento debe incluir pasos como la creación de solicitudes de cambio (RFC), la evaluación de riesgos técnicos y de negocio, y la autorización formal. La auditoría interna puede ser requerida para validar los planes de implementación y mitigar riesgos asociados. Además, es fundamental involucrar a proveedores externos para garantizar que sus responsabilidades estén documentadas y sean cumplidas en cada etapa del proceso. El monitoreo continuo permite identificar desviaciones y asegurar que los objetivos del cambio sean alcanzados con un impacto mínimo en la operación.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Este proceso debe mitigar cualquier efecto adverso de los cambios según sea necesario.  2. Los cambios relevantes como cambios en la organización, procesos de negocio, instalaciones de procesamiento de información y sistemas que afectan la seguridad de la información deben ser controlado desde la perspectiva de la seguridad de la información.  3. Cumplir con la pertinente legislación, códigos de práctica de la industria, estándares y prácticas organizativas.  4. Establecer roles y responsabilidades de todas las partes interesadas.  5. Composición de consejos asesores, p.e. el consejo asesor de cambios (CAB) y el CAB de emergencia (ECAB).  6. Crear un plan de implementación que refleje la estrategia global de implementación, secuencia de los pasos de implementación, requisitos de recursos, interdependencias, criterios de la dirección para la aceptación de la implementación a producción, establecimiento de requisitos de verificación, estrategia de transición para el soporte en producción y actualización de los planes de continuidad del negocio.  7. Identificar y documentar los procesos de fallback y recuperación.  8. Garantizar que existan planes de remediación, puede incluir retrocesos, planes de continuidad del servicio u otras acciones diseñadas para permitir que el proceso comercial continúe. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Establecer un proceso formal de gestión de cambios de seguridad de la información que incluya las siguientes actividades:  1.1 Identificar y registrar los cambios necesarios de controles, procesos del SGSI, documentación del SGSI, alcance, política y procedimientos estándar del SGSI.  1.2 Cambios en el plan, incluidos procedimientos alternativos.  1.3 Obtener una evaluación de riesgos de los cambios propuestos a partir del proceso de evaluación de riesgos (evaluación de impactos potenciales).  1.4 Aprobar o rechazar cambios.  1.5 Iniciar cambios a través del proceso de gestión de implementación de seguridad y el proceso de gestión de políticas de seguridad.  1.6 Obtener y registrar los resultados de los cambios.  1.7 Comunicar los resultados de los cambios en el proceso de evaluación de riesgos, así como en el proceso de gestión de incidentes de seguridad de la información a todas las partes interesadas.  2. Confirmar que todos los planes de implementación cuentan con la aprobación de las partes interesadas técnicas y de negocio y que están revisados por auditoría interna, cuando sea necesario.  3. Definir un procedimiento de cambios que incluya las siguientes actividades:  3.1 Crear y registrar una solicitud de cambio (RFC)  3.2 Revisar RFC  3.3 Valorar y evaluar el cambio  3.4 Autorizar el cambio, compilación y prueba  3.5 Coordinar la creación y prueba de cambios  3.6 Autorizar la implementación de cambios  3.7 Coordinar la implementación del cambio  3.8 Revisar y cerrar el registro de cambios. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Revisar formalmente el riesgo técnico y de negocio asociado con la implementación.  2. Asegurar que considere el riesgo y se aborde en el proceso de planificación.  3. Obtener de los proveedores externos de soluciones el compromiso de su participación en cada paso de la implementación. |
| 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 Establecer el Proceso de Gestión de Cambios**

|  |
| --- |
| Temática: Proceso de Solicitudes de Cambio |
| La organización debe asegurar que las solicitudes de cambio se gestionen adecuadamente desde su creación hasta su implementación, que se evalúen en función de su impacto en la seguridad de la información y otros aspectos críticos, y que se documenten de manera completa y precisa. En este proceso el auditor puede verificar que se sigan los protocolos adecuados, que se tomen decisiones informadas sobre la autorización de cambios y que se mantenga un registro adecuado de todas las solicitudes y cambios implementados. Este proceso se debe encontrar documentado e incluir las siguientes actividades:   * Crear y registrar una solicitud de cambio (RFC) * Revisar RFC * Valorar y evaluar el cambio * Autorizar el cambio, compilación y prueba * Coordinar la creación y prueba de cambios * Autorizar la implementación de cambios * Coordinar la implementación del cambio * Revisar y cerrar el registro de cambios   Este levantamiento puede incluir análisis específicos tales como:  **3.1.1 Crear y registrar una solicitud de cambio (RFC):**   * ¿Se ha implementado un procedimiento efectivo para la creación y registro de solicitudes de cambio (RFC) que incluya la información necesaria, como descripción del cambio, justificación, impacto previsto y prioridad? * ¿Se verifica que todas las RFC sean registradas de manera oportuna y de acuerdo con el procedimiento establecido? * ¿Existe un mecanismo para rastrear y documentar el estado actual de todas las RFC, incluyendo su fecha de creación y las actualizaciones correspondientes? * ¿Se requiere la identificación de los responsables de la RFC, incluyendo aquellos que solicitan el cambio y aquellos que deben aprobarlo? * ¿Se asegura que las RFC contengan información suficiente para permitir una revisión adecuada y una evaluación inicial del cambio propuesto? * ¿Se realiza una revisión de calidad de las RFC para asegurar que cumplen con los estándares de documentación y contenido requeridos?   **3.1.2 Revisar RFC:**   * ¿Existe un proceso formal y documentado para revisar las RFC que incluye una evaluación inicial de su validez y coherencia? * ¿Se asegura que las RFC sean revisadas por un equipo o individuo competente que evalúe su factibilidad y su alineación con los objetivos y estrategias organizativas? * ¿Se verifica que las RFC sean revisadas en función de su prioridad y que se tomen medidas adecuadas para las RFC críticas y de alta prioridad? * ¿Las RFC revisadas incluyen una evaluación de riesgos preliminar y un análisis de impacto para ayudar en la toma de decisiones sobre la aprobación? * ¿Se documentan las revisiones realizadas a las RFC, incluyendo los resultados de la revisión y las acciones recomendadas? * ¿Se asegura que todas las RFC sean comunicadas de manera adecuada a los interesados relevantes y que se mantenga un registro de dicha comunicación?   **3.1.3 Valorar y evaluar el cambio:**   * ¿Se realiza una evaluación de riesgos de los cambios propuestos como parte del proceso de valoración y evaluación? * ¿Se asegura que la valoración de los cambios se base en criterios claros, como la seguridad de la información, la continuidad del negocio y los requisitos regulatorios? * ¿Las evaluaciones de cambios incluyen una revisión de sus posibles impactos en sistemas, procesos, recursos y personal? * ¿Se verifica que se establezcan evaluaciones de impacto adecuadas para los cambios de alta complejidad o riesgo? * ¿Se documenta la evaluación de cada cambio, incluyendo la identificación de riesgos y la justificación para la aprobación o rechazo? * ¿Se involucra a los expertos técnicos y a los responsables de la seguridad de la información en el proceso de valoración y evaluación de los cambios?   **3.1.4 Autorizar el cambio, compilación y prueba:**   * ¿Existe un proceso formal y documentado para autorizar cambios, que incluye la designación de personas autorizadas para aprobar cambios? * ¿Las autorizaciones de cambios se basan en la evaluación de impacto y riesgo previamente realizada? * ¿Se asegura que las aprobaciones sean registradas y documentadas, incluyendo las fechas de autorización? * ¿Se verifica que se hayan establecido criterios de compilación y pruebas para cada cambio y que estos sean adecuados para su naturaleza y complejidad? * ¿Existe un proceso de coordinación eficiente para la compilación y pruebas de cambios, que incluye la asignación de recursos y la programación de actividades? * ¿Se documentan los resultados de las pruebas de cambios, incluyendo cualquier problema o desviación identificada?   **3.1.5 Coordinar la creación y prueba de cambios:**   * ¿Se asegura que la creación y prueba de cambios se lleve a cabo de manera planificada y coordinada, minimizando conflictos y riesgos? * ¿Existe una comunicación efectiva entre los equipos responsables de la creación y prueba de cambios, así como con otras partes interesadas? * ¿Se verifica que se cumplan los plazos establecidos para la creación y prueba de cambios? * ¿Existe una revisión independiente de los cambios antes de su implementación para garantizar su calidad y conformidad? * ¿Se asegura que se resuelvan de manera adecuada y oportuna los problemas identificados durante la creación y prueba de cambios?   **3.1.6 Autorizar la implementación de cambios:**   * ¿Existe un proceso formal y documentado para autorizar la implementación de cambios, que incluye la revisión de los resultados de las pruebas y la evaluación final del cambio? * ¿Las autorizaciones de implementación se basan en la satisfacción de los criterios de aceptación previamente establecidos? * ¿Se asegura que las aprobaciones de implementación sean registradas y documentadas de manera adecuada? * ¿Existe una revisión final de la documentación y los resultados de las pruebas antes de la autorización de implementación? * ¿Se verifica que se comuniquen de manera efectiva las autorizaciones de implementación a los equipos responsables y otros interesados? * ¿Se documentan los planes de implementación, incluyendo los pasos específicos a seguir y las fechas programadas?   **3.1.7 Coordinar la implementación del cambio:**   * ¿Se garantiza que la implementación de cambios se coordine de manera efectiva, considerando las interdependencias y minimizando posibles conflictos? * ¿Se verifica que se asignen los recursos necesarios para la implementación y que estén disponibles según lo planificado? * ¿Se asegura que se siga el plan de implementación y que se registren los progresos y desviaciones? * ¿Se documentan los resultados de la implementación, incluyendo cualquier incidente o problema que surja durante este proceso?   **3.1.8 Revisar y cerrar el registro de cambios:**   * ¿Existe un proceso formal para revisar y cerrar los registros de cambios, que incluye la verificación de que los cambios se han implementado de acuerdo con los planes y aprobaciones? * ¿Se verifica que se hayan completado todos los pasos de implementación y que no haya elementos pendientes? * ¿Las revisiones incluyen la comparación de los resultados de implementación con los criterios de aceptación previamente definidos? * ¿Se documentan las revisiones realizadas y los resultados obtenidos? * ¿Se asegura que los registros de cambios sean cerrados de manera oportuna y de acuerdo con los procedimientos establecidos? * ¿Existe una comunicación efectiva de los resultados de la revisión y el cierre de los registros de cambios a todas las partes interesadas pertinentes? |

|  |
| --- |
| Temática: Control de cambios relevantes y cumplimiento normativo |
| Esta evaluación se centra en cómo la organización integra consideraciones de cumplimiento dentro de su proceso de gestión de cambios, asegurando que cada cambio sea evaluado en términos de su impacto en el cumplimiento normativo. El auditor debe examinar la efectividad con la que la organización identifica, documenta y maneja los cambios que pueden afectar el cumplimiento normativo  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se garantiza que este proceso de control de cambios mitigue cualquier efecto adverso de los cambios, según sea necesario? * ¿Se controlan los cambios relevantes, como los relacionados con la organización, procesos de negocio, instalaciones de procesamiento de información y sistemas, desde la perspectiva de la seguridad de la información? * ¿Se asegura el cumplimiento de la legislación pertinente, códigos de práctica de la industria, estándares y prácticas organizativas en la gestión de cambios? * ¿Están claramente definidos y documentados los roles y responsabilidades de todas las partes interesadas involucradas en el proceso de cambio? * ¿Se ha establecido la composición de los consejos asesores relevantes, como el Consejo Asesor de Cambios (CAB) y el CAB de Emergencia (ECAB), y se han definido sus funciones y responsabilidades? |

|  |
| --- |
| Temática: Implementación del Cambio |
| Durante la auditoría de la implementación del cambio, es fundamental que el auditor evalúe cómo la organización lleva a cabo y gestiona esta fase crítica del proceso de gestión de cambios. El auditor debe concentrarse en la efectividad con la que se planifican, ejecutan y monitorean los cambios para asegurar que se implementen de acuerdo con las políticas establecidas y las mejores prácticas de seguridad.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se realiza una revisión formal del riesgo técnico y de negocio asociado con la implementación de cambios, considerando el riesgo en el proceso de planificación? * ¿Se crea un plan de implementación que refleja una estrategia global de implementación, secuencia de pasos, requisitos de recursos, interdependencias, criterios de aceptación y estrategias de transición para el soporte en producción? * ¿Se identifican y documentan los procesos de fallback y recuperación en caso de que la implementación tenga problemas? * ¿Existen planes de remediación, incluyendo retrocesos y planes de continuidad del servicio, diseñados para permitir que el proceso comercial continúe en caso de problemas durante la implementación? * ¿Se obtiene el compromiso de los proveedores externos de soluciones para su participación en cada fase de la implementación de cambios? |