 2

**CASIG 5 – Operaciones de Ciberseguridad**

**Preguntas de Auditoría**

**Cambios de Emergencia**

**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

Los cambios de emergencia son modificaciones críticas que deben implementarse rápidamente para resolver problemas urgentes que amenazan la operación normal de los sistemas o la continuidad del negocio. Debido a su naturaleza, estos cambios requieren procedimientos especializados que equilibren la rapidez en la ejecución con el control adecuado para minimizar riesgos y garantizar que las operaciones no se vean comprometidas tras su implementación.

**1.1 Procedimientos y Control de Cambios de Emergencia**

Definir qué constituye un cambio de emergencia es esencial para evitar abusos o malentendidos en su aplicación. El procedimiento para estos cambios debe estar documentado, incluyendo los pasos para declarar, evaluar, autorizar y registrar el cambio. A diferencia del procedimiento normal, la evaluación debe ser realizada por el Comité Asesor de Emergencia (ECAB), y las pruebas pueden ser limitadas o omitidas en situaciones críticas. Además, los registros de cambios y configuraciones pueden actualizarse posteriormente en horarios laborales regulares. Las decisiones y autorizaciones para estos cambios deben ser documentadas, incluyendo el tiempo estimado para su ejecución y los permisos de acceso temporal, los cuales deben revocarse inmediatamente después de la implementación.

**1.2 Auditoría y Revisión de Cambios de Emergencia**

Desde una perspectiva de auditoría, es fundamental monitorear todos los cambios de emergencia, verificando que hayan seguido el procedimiento establecido y que las autorizaciones estén documentadas correctamente. Las revisiones post-implementación deben involucrar a todas las partes interesadas y enfocarse en identificar las causas raíz del problema que originó el cambio. Estas revisiones deben considerar procesos de negocio, documentación técnica, integridad de datos y los entornos de desarrollo y pruebas. Las acciones correctivas derivadas de esta revisión no solo deben solucionar los problemas actuales, sino también prevenir futuros incidentes que requieran cambios de emergencia.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Las decisiones para la autorización de cambios de emergencia deben estar documentadas  2. Los cambios autorizados se asignan al grupo técnico correspondiente.  3. Definir lo que constituye un cambio de emergencia. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. El tiempo para completar estas actualizaciones debe ser documentado cuando se autoriza el cambio.  2. El procedimiento de cambio de emergencia seguirá el procedimiento de cambio normal excepto que:  2.1 La evaluación será otorgada por la ECAB en lugar de que esperar una reunión del CAB.  2.2 Las pruebas pueden reducirse o, en casos extremos, renunciarse por completo, si esto se considera un riesgo necesario para realizar el cambio de inmediato.  2.3 La actualización del registro de cambios y los datos de configuración puede diferirse, normalmente hasta el horario laboral normal.  3. Asegurar que existe un procedimiento documentado para declarar, evaluar, aprobar inicialmente, autorizar después del cambio y registrar un cambio de emergencia.  4. Verificar que todos los acuerdos de acceso de emergencia para los cambios se autoricen, documenten y revoquen adecuadamente después de que el cambio se haya aplicado. |
| 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. Monitorizar todos los cambios de emergencia y realizar las revisiones posteriores a la implementación con la participación de todas las partes interesadas. |
| 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. La revisión debe considerar e iniciar acciones correctivas basadas en las causas raíz, tales como problemas con los procesos de negocio, desarrollo y mantenimiento de sistemas de aplicación, entornos de desarrollo y pruebas, documentación y manuales, e integridad de datos. |

1. **Preguntas de Auditoría para Evaluar los Cambios de Emergencia**

|  |
| --- |
| Temática: Gestión y revisión de cambios de emergencia |
| El auditor debe verificar que esté definido claramente en la documentación lo que constituye un cambio de emergencia, proporcionando criterios específicos para su identificación, así mismo, evaluar las justificaciones y urgencia que dan pie a considerar un cambio como un cambio de emergencia.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización contempla un procedimiento de cambio de emergencia que siga un proceso documentado, distinto al procedimiento de cambio normal, especificando las diferencias, como la evaluación por parte de la ECAB, la posible reducción de pruebas y la programación diferida de actualizaciones del registro de cambios y datos de configuración?   + ¿Se lleva a cabo una evaluación de impacto antes de autorizar un cambio de emergencia para comprender sus posibles efectos en los sistemas, procesos y operaciones?   + ¿Se asignan los cambios autorizados al grupo técnico correspondiente para su implementación de manera eficaz?   + ¿Se contempla una revisión independiente de los cambios de emergencia para garantizar la integridad y calidad de la implementación? * ¿La organización se asegura que todos los acuerdos de acceso de emergencia para los cambios se autoricen, documenten y revoquen de manera adecuada después de la implementación del cambio? * ¿Están todas las decisiones relacionadas con la autorización de cambios de emergencia debidamente documentadas y disponibles para su revisión? * ¿Se establece un límite de tiempo para la autorización de cambios de emergencia, y se registra este tiempo desde la solicitud hasta la autorización? * ¿Existe un registro centralizado que documenta todos los cambios de emergencia, incluyendo su fecha de solicitud, autorización y finalización? * ¿Se notifica y comunica adecuadamente a todas las partes interesadas sobre la implementación de un cambio de emergencia y sus implicaciones? |

|  |
| --- |
| Temática: Monitoreo y acciones correctivas de los cambios de emergencia |
| Al revisar el monitoreo, el auditor se asegura de que los cambios de emergencia se implementen de manera adecuada y se identifiquen problemas de manera oportuna. Además, al evaluar las acciones correctivas, el auditor verifica que se aborden las causas raíz de cualquier problema surgido durante la implementación de cambios de emergencia.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se realiza una monitorización efectiva de todos los cambios de emergencia y se llevan a cabo revisiones posteriores a la implementación con la participación de todas las partes interesadas? * ¿Se asegura que las revisiones posteriores a la implementación consideren e inicien acciones correctivas basadas en las causas raíz de los problemas identificados, como problemas con los procesos de negocio, desarrollo y mantenimiento de sistemas de aplicación, entornos de desarrollo y pruebas, documentación y manuales, e integridad de datos? * ¿Se mantiene un registro completo de las acciones correctivas tomadas como resultado de las revisiones posteriores a la implementación de cambios de emergencia? * ¿Se considera y documenta la retroalimentación de las partes interesadas en la revisión posterior a la implementación de cambios de emergencia? * ¿Se revisan regularmente los procedimientos de cambio de emergencia para su mejora continua y se documentan las actualizaciones? |