

**GASIC 7 – Seguridad en Redes**

**Preguntas de Auditoría**

**Operaciones en la Nube**

**Competencias Básicas del Auditor**

1. **Conocimiento de la Nube:** Un auditor eficaz en operaciones de ciberseguridad en la nube debe tener un profundo entendimiento de las tecnologías en la nube, los modelos de servicio (IaaS, PaaS, SaaS), y las principales plataformas de nube, como AWS, Azure o Google Cloud.
2. **Seguridad en la Nube:** Se requiere un conocimiento sólido de los principios de seguridad en la nube, incluyendo la configuración segura de servicios en la nube, la gestión de identidades y accesos, y las mejores prácticas para proteger datos y aplicaciones.
3. **Evaluación de Riesgos en la Nube:** Competencias en la identificación y evaluación de riesgos específicos de la nube, incluyendo amenazas y vulnerabilidades únicas asociadas con entornos basados en la nube.
4. **Cumplimiento Normativo:** Entender los requisitos legales y regulatorios aplicables a la nube, y la capacidad de evaluar el cumplimiento con estándares como GDPR, HIPAA, o normativas específicas de la industria.
5. **Herramientas de Seguridad en la Nube:** Conocimiento y experiencia en el uso de herramientas de seguridad específicas para la nube, como soluciones de monitoreo, gestión de eventos, y herramientas de análisis de vulnerabilidades en entornos en la nube.
6. **Auditoría Técnica:** Competencias en la realización de auditorías técnicas específicas para entornos en la nube, incluyendo la revisión de configuraciones, la evaluación de controles de acceso, y la identificación de anomalías.
7. **Comunicación Efectiva:** Habilidades para comunicar hallazgos de auditoría y recomendaciones de manera clara y efectiva tanto a audiencias técnicas como no técnicas. La capacidad de traducir aspectos técnicos en términos comprensibles para stakeholders diversos es esencial.
8. **Gestión de Incidentes en la Nube:** Competencias en la respuesta a incidentes específicos de la nube, incluyendo la capacidad de coordinar respuestas efectivas ante amenazas y eventos de seguridad.
9. **Actualización Continua:** Reconocimiento de la importancia de mantenerse actualizado con las tendencias y evoluciones en la ciberseguridad en la nube, participando en formación continua y manteniendo certificaciones relevantes.

# Visión General

Las operaciones en la nube requieren una planificación y gestión rigurosa para garantizar la seguridad, la continuidad del servicio y el cumplimiento de los requisitos organizacionales. La colaboración efectiva con los proveedores de servicios, el monitoreo constante del entorno y la preparación para interrupciones o cambios son aspectos clave para mantener un entorno seguro y confiable. Implementar controles robustos y procedimientos de mejora continua asegura que las operaciones en la nube estén alineadas con los objetivos de seguridad y resiliencia de la organización.

**1.1 Roles, Responsabilidades y Gestión de Soporte**

El primer paso para garantizar operaciones seguras en la nube es acordar roles y responsabilidades claras con el proveedor de servicios, documentándolas en un contrato. Esto incluye definir quién es responsable de cada aspecto de la seguridad de la información y verificar que el proveedor pueda cumplir con estas obligaciones. Adicionalmente, es crucial identificar los puntos de contacto del soporte al cliente del proveedor, asegurando que existan canales eficaces para gestionar incidentes y solicitudes de manera ágil.

**1.2 Continuidad Operativa y Recuperación**

La planificación de la continuidad es esencial para mitigar el impacto de interrupciones en las operaciones de la nube. Esto implica mantener múltiples copias de los datos en ubicaciones diversas para respaldos y recuperación, identificar productos y servicios críticos, y establecer tiempos máximos tolerables de interrupción y objetivos de recuperación. Estos pasos permiten priorizar la restauración de servicios en caso de fallos y garantizar que la organización pueda operar con el menor impacto posible.

**1.3 Monitoreo, Riesgos y Mejora Continua**

El monitoreo constante del uso de servicios y la evaluación de riesgos son fundamentales para mantener la seguridad y el rendimiento de las operaciones en la nube. Herramientas de análisis de registros y monitoreo permiten detectar amenazas o intrusiones rápidamente y tomar medidas correctivas. Asimismo, es importante fomentar una cultura organizacional enfocada en la mejora continua, realizando evaluaciones periódicas para identificar vulnerabilidades y ajustar los controles en respuesta a nuevas amenazas. Este enfoque dinámico asegura que las operaciones en la nube se mantengan resilientes y adaptativas frente a un entorno de amenazas en constante evolución.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Acordar con el proveedor del servicio en la nube una asignación adecuada de roles y responsabilidades de seguridad de la información, y confirmar que puede cumplir con los roles y responsabilidades asignados.  1.1 Deben establecerse en un acuerdo las funciones y responsabilidades de seguridad de la información de ambas partes.  2. Identificar y gestionar la relación con la función de atención y soporte al cliente del proveedor del servicio en la nube  3. Identificar los programas de utilidad que se utilizarán en su entorno de computación en la nube y asegurarse de que no interfieran con los controles del servicio en la nube cuando se permita el uso de programas de utilidad. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Crear o mantener múltiples copias de datos en ubicaciones física y/o lógicamente diversas (que pueden estar dentro del propio sistema de procesamiento de información) con fines de copia de seguridad y/o recuperación.  2. Deben existir un método definido y documentado para determinar el impacto de cualquier interrupción en la organización, que debe incorporar lo siguiente:  2.1 Identificar los productos y servicios críticos  2.2 Identificar todas las dependencias, incluidos los procesos, las aplicaciones, los socios comerciales y los proveedores de servicios externos.  2.3 Comprender las amenazas a los productos y servicios críticos  2.4 Determinar los impactos resultantes de las interrupciones planificadas o no planificadas y cómo varían con el tiempo.  2.5 Establecer el periodo máximo tolerable de interrupción  2.6 Establecer prioridades para la recuperación  2.7 Establecer objetivos de tiempo de recuperación para la reanudación de productos y servicios críticos dentro de su período máximo tolerable de interrupción.  2.8 Estimar los recursos necesarios para la reanudación.  3. Planificar, preparar y medir la disponibilidad, la calidad y la capacidad y los recursos adecuados para ofrecer el rendimiento requerido del sistema de acuerdo con los requisitos normativos, contractuales y empresariales.  3.1 Realizar proyecciones de las necesidades futuras de capacidad para mitigar el riesgo de sobrecarga del sistema. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Monitorear el uso de los servicios en la nube y pronosticar sus necesidades de capacidad para garantizar el desempeño de los servicios en la nube a lo largo del tiempo.  2. Establecer un estado de preparación para transferir las operaciones de computación en la nube a un proveedor de servicios alternativo en caso de que el proveedor de servicios seleccionado no pueda cumplir con los requisitos contractuales o cese sus operaciones. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Realizar evaluaciones de riesgos de forma regular para identificar posibles vulnerabilidades en la infraestructura de la nube y tomar medidas correctivas.  1.1 Utilizar herramientas de monitoreo y análisis de registros para detectar y responder rápidamente a posibles amenazas o intrusiones en la nube. |
| 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. Fomentar una cultura de seguridad cibernética en la organización, donde la mejora continua sea parte integral de las operaciones en la nube.  1.1 Realizar evaluaciones periódicas de la seguridad en la nube para identificar áreas de mejora y ajustar los controles de acuerdo a las nuevas amenazas y vulnerabilidades. |

1. **Preguntas de Auditoría para Operaciones en la Nube**

|  |
| --- |
| Temática: Monitoreo del Uso de los Servicios en la Nube |
| Esta evaluación implica llevar a cabo una revisión exhaustiva de las prácticas y sistemas implementados para supervisar la utilización de recursos en entornos *cloud*. Esto incluye revisar las políticas y procesos establecidos para el monitoreo continuo de actividades en la nube, tales como el acceso a servicios, la gestión de identidades, la utilización de recursos computacionales y el tráfico de datos. La auditoría busca asegurar que los controles de monitoreo estén configurados de manera efectiva, proporcionando visibilidad integral sobre las operaciones en la nube.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se ha acordado con el proveedor del servicio en la nube una asignación adecuada de roles y responsabilidades de seguridad de la información?   + Revise la documentación contractual y acuerdos de nivel de servicio (SLA) para identificar la asignación específica de roles y responsabilidades de seguridad entre la organización y el proveedor de servicios en la nube.   + ¿Se han establecido en un acuerdo las funciones y responsabilidades de seguridad de la información de ambas partes?     - Verifique si hay evidencia de que ambas partes han revisado y aceptado los términos relacionados con las funciones y responsabilidades de seguridad en el acuerdo.   + ¿Se ha identificado y gestionado adecuadamente la relación con la función de atención y soporte al cliente del proveedor del servicio en la nube?   + ¿Se han identificado los programas de utilidad que se utilizarán en el entorno de computación en la nube y se ha asegurado de que no interfieran con los controles del servicio en la nube? * ¿Existe procedimientos claros que establezcan la necesidad de crear y mantener múltiples copias de datos para fines de copia de seguridad y recuperación?   + ¿Se realizan copias de seguridad regularmente de los datos críticos?   + Verifique la existencia de procedimientos automáticos o programados para la realización de copias de seguridad y confirmar su funcionamiento.   + ¿Las copias de seguridad se almacenan en ubicaciones física y/o lógicamente diversas?   + ¿Se realizan pruebas periódicas de recuperación para garantizar la efectividad del proceso de recuperación de datos? * ¿Existe un método definido y documentado para determinar el impacto de cualquier interrupción en la organización?   + ¿Se han identificado claramente los productos y servicios críticos de la organización?   + ¿Se han identificado todas las dependencias, incluidos procesos, aplicaciones, socios comerciales y proveedores de servicios externos?   + ¿Existe un entendimiento claro de las amenazas que podrían afectar a los productos y servicios críticos? * ¿La organización tiene un plan formal para la planificación, preparación y medición de la disponibilidad, calidad y capacidad del sistema de acuerdo con los requisitos normativos, contractuales y empresariales?   + ¿La organización cuenta con recursos adecuados para ofrecer el rendimiento requerido del sistema según los requisitos establecidos?   + ¿Se realizan mediciones periódicas de la disponibilidad, calidad y capacidad del sistema?   + ¿La organización realiza proyecciones de las necesidades futuras de capacidad para mitigar el riesgo de sobrecarga del sistema? * ¿La organización monitorea de manera efectiva el uso de los servicios en la nube y pronostica sus necesidades de capacidad?   + ¿Existe un proceso formal para establecer un estado de preparación para transferir las operaciones de computación en la nube a un proveedor de servicios alternativo?   + ¿La organización cuenta con un plan de contingencia específico en caso de que el proveedor de servicios en la nube seleccionado no pueda cumplir con los requisitos contractuales o cese sus operaciones? * ¿Cómo se configuran las herramientas de monitoreo para capturar eventos relevantes en los servicios en la nube?   + Evaluar la configuración de las herramientas de monitoreo para garantizar que estén correctamente ajustadas para capturar eventos críticos, incluyendo accesos no autorizados, cambios en la configuración y actividades anómalas.   + ¿Cuál es el proceso para garantizar que las herramientas de monitoreo estén configuradas según las mejores prácticas de seguridad y se actualicen en respuesta a cambios en la infraestructura de la nube? * ¿Está el personal capacitado para utilizar y comprender las herramientas de monitoreo en la nube?   + Evalúe la capacitación del personal en el manejo de las herramientas de monitoreo, asegurando que puedan interpretar y responder efectivamente a los eventos registrados.   + ¿Cómo se mide la efectividad de la capacitación del personal en el uso de herramientas de monitoreo en la nube, y cuáles son los mecanismos para actualizar las habilidades del personal en respuesta a cambios tecnológicos y de seguridad?   + ¿La organización fomenta una cultura de seguridad cibernética? * ¿La mejora continua es parte integral de las operaciones en la nube?   + ¿Se realizan evaluaciones periódicas de seguridad en la nube?   + ¿Se identifican áreas de mejora durante las evaluaciones de seguridad en la nube?   + ¿Los controles se ajustan según las nuevas amenazas y vulnerabilidades identificadas? * ¿Se realizan evaluaciones de riesgos de forma regular en la infraestructura de la nube?   + Verifique la existencia de registros de evaluaciones de riesgos anteriores y compararlos con un calendario establecido para confirmar la regularidad de las evaluaciones.   + ¿Se identifican y documentan adecuadamente las posibles vulnerabilidades descubiertas durante las evaluaciones de riesgos?   + ¿Se toman medidas correctivas en respuesta a las vulnerabilidades identificadas durante las evaluaciones de riesgos?   + ¿Se utilizan herramientas de monitoreo y análisis de registros para detectar y responder rápidamente a posibles amenazas o intrusiones en la nube? |