

**GASIC 7 – Seguridad en Redes**

**Preguntas de Auditoría**

**Protección de Datos 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

La computación en la nube presenta riesgos específicos que deben gestionarse mediante controles bien definidos. La correcta administración de claves criptográficas, la mitigación de vulnerabilidades técnicas y la implementación de medidas de seguridad adaptadas al entorno cloud son pasos necesarios para minimizar exposiciones y proteger los activos digitales. Estas acciones permiten a las organizaciones garantizar la confidencialidad, integridad y disponibilidad de los datos en un entorno compartido y dinámico.

**1.1 Gestión de Claves Criptográficas y Configuración Segura**

La identificación de las claves asociadas a cada servicio en la nube y la implementación de procedimientos para su gestión son imprescindibles para proteger las operaciones. Esto incluye solicitar al proveedor información detallada sobre el ciclo de vida de las claves, desde su generación hasta su destrucción. Durante la configuración de máquinas virtuales, es necesario habilitar únicamente los puertos, protocolos y servicios esenciales, asegurando además que los sistemas estén equipados con herramientas de seguridad como antimalware y monitoreo de registros.

**1.2 Evaluación y Monitoreo de Vulnerabilidades**

La relación con el proveedor del servicio debe incluir una comprensión detallada de las capacidades de monitoreo disponibles. Gestionar vulnerabilidades requiere establecer procesos claros para identificar riesgos, implementar controles de aislamiento del sistema operativo y emplear cifrado según el resultado de los análisis. Estos controles deben aplicarse tanto a datos en reposo como en tránsito, asegurando una protección completa frente a amenazas internas y externas.

**1.3 Políticas de Gestión y Controles Criptográficos**

El cliente del servicio en la nube debe mantener el control directo sobre las claves de cifrado, evitando que el proveedor almacene o administre dichas claves. Esta medida garantiza que las operaciones críticas permanezcan bajo control interno, incluso ante cambios en los servicios del proveedor. Las capacidades criptográficas ofrecidas por el proveedor deben cumplir con las políticas organizacionales, ser compatibles con las protecciones internas y documentarse adecuadamente para prevenir interrupciones o pérdidas.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1.Identificar las claves criptográficas para cada servicio en la nube e implementar procedimientos para la gestión de claves.  1.1 Asegurar que se refuercen los aspectos apropiados (p. ej., solo aquellos puertos, protocolos y servicios que sean necesarios) y de que existan las medidas técnicas apropiadas (p. ej., antimalware, logging) para cada máquina virtual utilizada al momento de configurar máquinas virtuales.  2. Solicitar la siguiente información sobre los procedimientos utilizados cuando el servicio en la nube proporciona funcionalidad de gestión de claves para uso del cliente del servicio en la nube para gestionar las claves relacionadas con el servicio en la nube:  2.1 Tipo de claves.  2.2 Especificaciones del sistema de gestión de claves, incluidos procedimientos para cada etapa del ciclo de vida de las claves, es decir, generar, cambiar o actualizar, almacenar, retirar, recuperar, retener y destruir.  2.3 Procedimientos de gestión de claves recomendados para su uso por parte del cliente del servicio en la nube.  3. Solicitar información al proveedor de servicios en la nube sobre la gestión de aspectos técnicos y vulnerabilidades que pueden afectar los servicios en la nube prestados.  4. Identificar los aspectos técnicos y vulnerabilidades que se gestionaran.  4.1 Definir un proceso para gestionarlos.  5. Solicitar información al proveedor de servicios en la nube sobre las capacidades de monitoreo de servicios disponibles para cada servicio en la nube. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Proporcionar una evaluación exhaustiva del riesgo para el negocio mediante la implementación del modelo de procesamiento en la nube y está alineado con la gestión de riesgos empresariales (ERM), por el proceso de gestión de riesgos.  1.1 Implementar controles de seguridad y aislamiento del sistema operativo proporcionados por el proveedor de servicios para evitar ataques y accesos no autorizados.  1.1 Implementar controles criptográficos para su uso de los servicios en la nube si el análisis de riesgos lo justifica.  1.1.1 Los controles deben ser lo suficientemente sólidos para mitigar los riesgos identificados, ya sea que esos controles sean proporcionados por el cliente del servicio en la nube o por el proveedor del servicio en la nube.  1.1.2 Documentar los procedimientos para operaciones críticas donde una falla puede causar daños irrecuperables a los activos en el entorno de computación en la nube.  2. Revisar cualquier información proporcionada por el proveedor de servicios en la nube cuando el proveedor de servicios en la nube ofrece criptografía para confirmar si las capacidades criptográficas:  2.1 Cumplen con los requisitos de política del cliente del servicio en la nube.  2.2 Son compatibles con cualquier otra protección criptográfica utilizada por el cliente del servicio en la nube.  2.3 Se aplican a los datos en reposo y en tránsito hacia, desde y dentro del servicio en la nube.  3. Prohibir que el proveedor del servicio en la nube almacene y administre las claves de cifrado para operaciones criptográficas cuando el cliente del servicio en la nube emplea su propia administración de claves o un servicio de administración de claves separado y distinto.  3.1 Considerar el impacto de cualquier cambio realizado por el proveedor del servicio en la nube dentro del proceso de gestión de cambios del cliente del servicio |
| 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 Riesgos en la Nube**

|  |
| --- |
| Temática: Claves Criptográficas |
| La auditoría de claves criptográficas es crucial para garantizar la seguridad de la información en entornos digitales. Estas claves desempeñan un papel fundamental en la protección de la confidencialidad e integridad de los datos, y su auditoría se vuelve esencial para prevenir accesos no autorizados, ataques criptoanalíticos y para cumplir con normativas de seguridad.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se han identificado todas las claves criptográficas asociadas con cada servicio en la nube?   + Revise la documentación de gestión de claves y los registros de configuración de servicios en la nube para asegurarse de que se haya identificado y documentado cada clave criptográfica utilizada.   + ¿Existen especificaciones detalladas del sistema de gestión de claves, incluyendo procedimientos para cada etapa del ciclo de vida de las claves?     - Verifique la existencia de registros de auditoría relacionados con cambios en el ciclo de vida de las claves, como generación, cambio o actualización, almacenamiento, retirada, recuperación, retención y destrucción. * ¿La organización tiene documentados los procedimientos utilizados cuando el servicio en la nube proporciona funcionalidad de gestión de claves para uso del cliente?   + ¿Se especifica claramente el tipo de claves utilizadas en el servicio en la nube?     - Realice una revisión de las configuraciones de seguridad del servicio en la nube para corroborar la información sobre el tipo de claves utilizadas.   + ¿La organización cuenta con procedimientos de gestión de claves recomendados para su uso por parte del cliente del servicio en la nube? * ¿Cómo se asegura la seguridad durante la transmisión de claves entre usuarios y sistemas?   + Revise la documentación de políticas de seguridad para la transmisión de claves y validar que se utilicen protocolos seguros, como HTTPS o TLS, durante las transferencias de claves. * ¿Existen recomendaciones específicas para que los clientes gestionen sus propias claves criptográficas?   + Revise la documentación de las políticas de gestión de claves para asegurarse de que se proporcionen recomendaciones claras a los clientes sobre cómo gestionar sus propias claves de forma segura. * ¿Cuál es el plan de respuesta a incidentes en caso de compromiso de claves?   + ¿Se notifica a las partes interesadas en caso de incidentes relacionados con claves?     - Revise los registros de incidentes pasados para confirmar que se ha notificado a las partes interesadas relevantes en caso de compromiso de claves, según lo establecido en el plan de respuesta a incidentes.   + Entreviste al equipo de respuesta a incidentes para asegurarse de que están al tanto de los procedimientos de notificación y han seguido estos procedimientos en el pasado. * ¿Hay procedimientos claros para la recuperación de claves comprometidas?   + Verifique la eficacia de los procedimientos de recuperación de claves a través de simulacros o revisiones de incidentes pasados para confirmar que se aplicaron correctamente. |

|  |
| --- |
| Temática: Configuración de Máquinas Virtuales |
| La auditoría de la configuración de máquinas virtuales es crucial para garantizar la seguridad y estabilidad de las operaciones digitales. A través de este proceso, se verifica que las máquinas virtuales estén correctamente configuradas, reduciendo así el riesgo de vulnerabilidades y accesos no autorizados. La revisión de políticas y estándares de seguridad, así como la gestión efectiva de claves criptográficas, aseguran el cumplimiento normativo y la confidencialidad de la información.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se ha implementado una política de seguridad para restringir solo los puertos, protocolos y servicios necesarios en las máquinas virtuales? * ¿Se han reforzado los aspectos apropiados de las máquinas virtuales utilizadas en la nube?   + Verifique que se hayan implementado medidas técnicas apropiadas, como soluciones antimalware y logging, en cada máquina virtual según lo establecido en los procedimientos de configuración.   + ¿Existe documentación clara que describa las medidas técnicas implementadas en cada máquina virtual? * ¿Existe un análisis de los riesgos asociados a los puertos y protocolos abiertos?   + Analice los registros de configuración de máquinas virtuales para identificar puertos y protocolos abiertos y compararlos con los resultados de los análisis de riesgos. * ¿Se han desactivado servicios no esenciales para reducir la superficie de ataque?   + Verifique la documentación de procedimientos de configuración para asegurarse de que se establezca la desactivación de servicios no esenciales como una práctica estándar. * ¿Hay procesos automáticos para la detección y respuesta a posibles amenazas? * ¿Se han aplicado parches y actualizaciones de seguridad de manera regular en las máquinas virtuales?   + Revise los registros de parches y actualizaciones aplicadas para confirmar la regularidad y puntualidad de las actualizaciones de seguridad. * ¿El proveedor de servicios en la nube ofrece capacidades de monitoreo detalladas para las máquinas virtuales utilizadas?   + Consulte la documentación del proveedor de servicios en la nube para verificar la disponibilidad y alcance de las capacidades de monitoreo ofrecidas.   + Realice pruebas de monitoreo en tiempo real para evaluar la efectividad y la profundidad del monitoreo proporcionado por el proveedor. * ¿Existen alertas configuradas para eventos críticos relacionados con la seguridad en las máquinas virtuales?   + Verifique la efectividad de las alertas realizando pruebas de eventos críticos y si se generan notificaciones y se siguen los procedimientos establecidos. |

|  |
| --- |
| Temática: Control de los proveedores de servicios en la nube |
| Este punto tiene como objetivo verificar la efectividad de los controles de seguridad aplicados por los proveedores para proteger la información y los sistemas alojados en la nube. Se examinan aspectos como la gestión de accesos, la protección de datos, la resiliencia ante amenazas, las políticas de cumplimiento y otros elementos críticos que influyen en la seguridad de la información en el entorno de la nube, se busca garantizar la transparencia y cumplimiento de los proveedores.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se ha solicitado información al proveedor de servicios en la nube sobre la gestión de aspectos técnicos y vulnerabilidades que pueden afectar los servicios en la nube prestados?   + Verifique que la organización tenga un proceso documentado para la solicitud de información a proveedores de servicios y que este proceso haya sido seguido.   + ¿Se han identificado los aspectos técnicos y vulnerabilidades que afectan los servicios en la nube?     - Revisar informes de evaluación de riesgos o auditorías internas que muestren la identificación de aspectos técnicos y vulnerabilidades * ¿Se ha solicitado información al proveedor de servicios en la nube sobre las capacidades de monitoreo para cada servicio utilizado?   + Verifique la existencia de documentación que respalde la solicitud de información al proveedor, como correos electrónicos, cartas o formularios de solicitud.   + ¿La solicitud de información incluye detalles específicos sobre los servicios en la nube y sus respectivas capacidades? ¿Se han recibido respuestas detalladas y completas?   + ¿Se ha evaluado la satisfacción con las respuestas proporcionadas por el proveedor de servicios en la nube?     - Realice entrevistas con los responsables de la solicitud de información para obtener retroalimentación sobre la calidad y utilidad de las respuestas recibidas. * ¿La evaluación exhaustiva del riesgo para el negocio ha sido realizada y está alineada con la gestión de riesgos empresariales (ERM)?   + Verifique que la evaluación de riesgos esté alineada con la gestión de riesgos empresariales, examinando documentos de políticas y procedimientos relacionados con ERM.   + ¿Se han implementado controles de seguridad y aislamiento del sistema operativo proporcionados por el proveedor de servicios en la nube para evitar ataques y accesos no autorizados?   + ¿Se han implementado controles criptográficos cuando el análisis de riesgos lo justifica?   + ¿Los controles implementados son lo suficientemente sólidos para mitigar los riesgos identificados, ya sea proporcionados por el cliente o el proveedor del servicio en la nube?   + ¿Se han documentado los procedimientos para operaciones críticas en el entorno de computación en la nube donde una falla puede causar daños irrecuperables? * ¿Se revisa cualquier información proporcionada por el proveedor de servicios en la nube para confirmar si las capacidades criptográficas cumplen con los requisitos de política del cliente del servicio en la nube?   + ¿Las capacidades criptográficas son compatibles con cualquier otra protección criptográfica utilizada por el cliente del servicio?   + Verifique si las capacidades criptográficas se aplican adecuadamente a los datos en reposo y en tránsito hacia, desde y dentro del servicio en la nube. * ¿La prohibición de que el proveedor del servicio en la nube almacene y administre las claves de cifrado está claramente establecida en la política de seguridad de la organización?   + Analice los acuerdos contractuales con proveedores para confirmar que contengan cláusulas explícitas que prohíban almacenar y administrar las claves cuando el cliente tiene su propio sistema de gestión de claves.   + ¿El cliente utiliza su propia administración de claves o un servicio de administración de claves separado y distinto?   + ¿El cliente del servicio en la nube considera el impacto de cualquier cambio realizado por el proveedor del servicio en la nube en su proceso de gestión de cambios? |