

**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

Implementar políticas y controles robustos para gestionar la información sensible permite a las organizaciones minimizar riesgos asociados con el almacenamiento, transmisión y procesamiento de datos en la nube. Al integrar medidas como el cifrado, etiquetado y copia de seguridad, se refuerza la confianza en los servicios cloud, asegurando el cumplimiento de normativas y estándares internacionales.

**1.1 Etiquetado y Clasificación de Datos**

Este proceso debe seguir los procedimientos adoptados por la organización, aprovechando funcionalidades del proveedor que faciliten la clasificación automática de los datos. La segmentación de activos etiquetados ayuda a aplicar controles específicos según el nivel de sensibilidad de la información, fortaleciendo las políticas de acceso y uso de datos dentro del entorno cloud.

**1.2 Cifrado y Copias de Seguridad**

Las claves de cifrado deben estar exclusivamente bajo control del cliente para evitar accesos no autorizados. Asimismo, la creación de copias de seguridad en ubicaciones seguras y su verificación periódica aseguran la disponibilidad de datos en caso de pérdida o interrupciones del servicio. Cuando el proveedor del servicio en la nube no ofrece estas capacidades, la organización debe implementar sus propios mecanismos de respaldo y recuperación.

**1.3 Monitoreo, Integridad y Mejora Continua**

Es esencial establecer rutinas de integridad de datos para evitar errores en el procesamiento y garantizar la precisión de las operaciones en la nube. Estas rutinas deben incluir comprobaciones de entrada y salida en aplicaciones y bases de datos, así como el seguimiento de posibles discrepancias. Además, se deben realizar auditorías regulares para evaluar las capacidades de copia de seguridad y recuperación de claves, documentando hallazgos y aplicando mejoras basadas en los resultados. Este enfoque permite mantener la protección de datos actualizada frente a nuevas amenazas, garantizando la continuidad y seguridad de la información almacenada en la nube.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Etiquetar la información y los activos asociados mantenidos en el entorno de computación en la nube de acuerdo con los procedimientos de etiquetado adoptados por el cliente del servicio en la nube.  1.1 Cuando corresponda, se puede adoptar la funcionalidad proporcionada por el proveedor de servicios en la nube que admite el etiquetado.  2. Utilizar una fuente de tiempo externa y precisa, acordada externamente, para sincronizar los relojes del sistema de todos los sistemas de procesamiento de información relevantes dentro de la organización o dominio de seguridad definido explícitamente para facilitar el seguimiento y la reconstitución de las líneas de tiempo de las actividades.  2.1 Solicitar información sobre la sincronización del reloj utilizada para el proveedor de servicios en la nube sistemas.  3. Utilizar la identificación automática de equipos como método de autenticación de la conexión.  3.1 Utilizar tecnologías que tengan en cuenta la ubicación para validar la integridad de la autenticación de la conexión basándose en la ubicación conocida del equipo.  4. Definir requisitos para segregar redes para lograr el aislamiento de los inquilinos en el espacio compartido del servicio en la nube.  4.1 Verificar que el proveedor cumple con esos requisitos del servicio en la nube.  5. Solicitar una descripción documentada del proceso de terminación del servicio que cubra la devolución y eliminación de los activos del cliente del servicio en la nube seguida de la eliminación de todas las copias de esos activos de los sistemas del proveedor del servicio en la nube.  5.1 La descripción debe enumerar todos los activos y documentar el  cronograma para la terminación del servicio, que debe ocurrir de manera oportuna. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Implementar rutinas de integridad de entrada y salida de datos (es decir, comprobaciones de conciliación y edición) para interfaces de aplicaciones y bases de datos con el fin de evitar errores de procesamiento manuales o sistemáticos o la corrupción de datos.  2. Cifrar los datos en tránsito a través de redes con claves privadas que sólo el cliente conozca.  3. Cifrar los datos almacenados en bases de datos de producción en vivo en sistemas en la nube  3.1 Limitar solo al cliente el conocimiento de las claves de descifrado.  4. Prohibir utilizar copias que contengan datos de producción actual o históricos que contengan información sensible/confidencial en los datos de prueba.  5. Solicitar las especificaciones de la capacidad de copia de seguridad al proveedor de servicios en la nube cuando el proveedor de servicios en la nube proporcione capacidad de copia de seguridad como parte del servicio en la nube.  5.1 Verificar también que se cumplen los requisitos de respaldo.  6. Implementar capacidades de respaldo cuando el proveedor del servicio en la nube No las proporcione.  7. Proteger los almacenes de claves durante la transmisión, el almacenamiento y la copia de seguridad.  7.1 Limitar el acceso a los almacenes clave a los gerentes clave cuya función laboral requiere acceso a los almacenes.  8. Separar al proveedor de servicios de los procedimientos de aprovisionamiento y gestión de la configuración.  8.1 Limitar a una función de operaciones de seguridad dentro de la organización del cliente y proporcionar pistas de auditoría para documentar todas las actividades. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Establecer y probar la copia de seguridad y la capacidad de recuperación de claves para garantizar el acceso continuo a las claves de datos.  1.1 Mantener disponibles y encriptadas las copias de seguridad de los datos |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Mantener la información y los activos en el entorno de computación en la nube etiquetados.  2. Seguimiento e implementación de rutinas de integridad de entrada y salida de datos.  3. Deben existir copias de seguridad y la capacidad de claves para garantizar el acceso. |
| 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. Realizar mejores según lo encontrado en los seguimientos de rutinas de integridad.  2. Mantener actualizadas y verificadas las copias de seguridad. |

1. **Preguntas de Auditoría para Políticas asociadas a la Nube**

|  |
| --- |
| Temática: Protección de datos y copias de seguridad |
| En este punto se realiza para verificar que tan protegidos se encuentran los datos en la empresa para asegurar la confidencialidad e integridad de toda la información que se encuentre dentro de la nube. Esta auditoria aborda aspectos clave como la protección de claves, la gestión de copias de seguridad y la efectividad de los procesos establecidos por la organización para la protección de los datos. Al realizar la auditoria se no solo se estará asegurando el cumplimiento normativo sino también la prevención de amenazas que puedan ocasionar la pérdida o filtrado de información crucial en la empresa.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La información y los activos en el entorno de computación en la nube se etiquetan de acuerdo con los procedimientos establecidos por el cliente del servicio en la nube?   + ¿Existen procedimientos de gestión de cambios para actualizar las etiquetas de información y activos en el entorno de la nube?   + ¿Esta etiquetación de información y activos se encuentra documentada?   + ¿Se utiliza la funcionalidad proporcionada por el proveedor de servicios en la nube para admitir el etiquetado cuando sea apropiado? * ¿Se utiliza una fuente de tiempo externa y precisa para sincronizar los relojes del sistema de todos los sistemas de procesamiento de información relevantes dentro de la organización?   + ¿Se ha definido explícitamente un dominio de seguridad dentro de la organización para la sincronización de relojes?   + ¿Qué procedimiento se realiza si algún equipo se desconfigura?   + ¿Se facilita el seguimiento y la reconstitución de las líneas de tiempo de las actividades a través de la sincronización precisa de los relojes?   + ¿Se solicita información sobre la sincronización del reloj utilizada para los sistemas de proveedores de servicios en la nube? * ¿Se implementa la identificación automática de equipos como método de autenticación de la conexión?   + ¿Se emplean tecnologías que consideran la ubicación para validar la integridad de la autenticación basándose en la ubicación conocida del equipo?     - Evalúe la lista de tecnologías de autenticación implementadas para verificar si incluyen características de validación de ubicación.   + ¿Qué tecnologías son usadas para considerar la ubicación y validar la integridad de autenticación?   + Realice una revisión de configuraciones en los sistemas para verificar si la identificación automática de equipos está habilitada y configurada según las directrices establecidas.   + ¿Las tecnologías de autenticación basadas en ubicación cumplen con los estándares de seguridad establecidos? * ¿Se han definido claramente los requisitos para segregar redes y lograr el aislamiento de los inquilinos en el espacio compartido del servicio en la nube?   + ¿Se ha verificado que el proveedor de servicios en la nube cumple con estos requisitos?   + ¿Se ha comunicado claramente a todos los involucrados la importancia y los detalles de los requisitos para la segregación de redes en el entorno de servicio en la nube?   + ¿Se realizan evaluaciones regulares para verificar el cumplimiento continuo de los requisitos de segregación de redes, tanto internamente como con el proveedor del servicio en la nube? * ¿Existe una descripción documentada del proceso de terminación del servicio que abarque la devolución y eliminación de los activos del cliente?   + ¿La descripción del proceso de terminación del servicio enumera de manera exhaustiva todos los activos del cliente?   + ¿El cronograma para la terminación del servicio está documentado y establece plazos oportunos?     - Evalúe la coherencia entre el cronograma propuesto y las expectativas realistas para la devolución y eliminación de activos en un período de tiempo oportuno. * ¿Se han implementado rutinas de integridad de entrada y salida de datos en las interfaces de aplicaciones y bases de datos?   + Realice una revisión de código para identificar la presencia de comprobaciones de conciliación y edición en las rutinas relacionadas con la entrada y salida de datos.   + ¿Están definidos y documentados claramente los procedimientos para las comprobaciones de conciliación y edición en las interfaces de aplicaciones y bases de datos?   + ¿Se realizan pruebas periódicas para asegurar la eficacia de las rutinas de integridad de entrada y salida de datos? * ¿Los datos almacenados en bases de datos de producción en la nube están cifrados?   + ¿Las claves privadas utilizadas para el cifrado son conocidas exclusivamente por el cliente?     - Realice un escaneo de seguridad en la infraestructura en la nube para identificar posibles brechas en la implementación de cifrado de datos almacenados.   + ¿Qué medidas se han tomado para garantizar la seguridad de las claves privadas? * ¿Se cifran los datos en tránsito a través de redes en la nube?   + ¿Las claves privadas utilizadas para el cifrado son conocidas exclusivamente por el cliente?     - Revise la configuración de seguridad de las redes para confirmar la implementación de cifrado y verificar la utilización de claves privadas, y asegurarse de que estas claves son conocidas solo por el cliente.   + ¿Qué medidas se han tomado para garantizar la seguridad de las claves privadas? * ¿Se verifican regularmente los requisitos de respaldo establecidos?   + ¿Se han solicitado y revisado las especificaciones de la capacidad de copia de seguridad al proveedor de servicios en la nube cuando este proporciona capacidad de copia de seguridad como parte del servicio?   + ¿Cómo se asegura que las capacidades de copia de seguridad cumplan con los requisitos de la organización?   + ¿Cómo se garantiza la integridad y disponibilidad de los datos respaldados? * ¿Se protegen los almacenes de claves durante la transmisión, almacenamiento y copia de seguridad?   + ¿El acceso a los almacenes de claves está limitado a los trabajadores cuya función laboral lo requiere?   + ¿Cómo se audita y monitorea el acceso a los almacenes de claves? * ¿Se ha separado al proveedor de servicios de los procedimientos de aprovisionamiento y gestión de configuración?   + ¿La función de operaciones de seguridad dentro de la organización del cliente se limita a estas actividades?   + ¿Se documentan y auditan todas las actividades relacionadas con la gestión de configuración y aprovisionamiento? * ¿Se ha establecido un proceso formal para la copia de seguridad de las claves de datos en la nube?   + ¿Cada cuánto tiempo se realizan estas copias de seguridad de las claves de datos?¿Se mantienen de manera continua y están disponibles cuando sea necesario?     - ¿Se han realizado pruebas periódicas para garantizar la eficacia de la copia de seguridad y la capacidad de recuperación de claves?   + ¿Las copias de seguridad de las claves de datos están encriptadas y protegidas contra accesos no autorizados?   + ¿Se realiza una monitorización regular para verificar la integridad y la seguridad de las copias de seguridad encriptadas? * ¿Existe una procedimiento formal que prohíba el uso de copias que contengan datos de producción actual o históricos con información?   + ¿El personal está debidamente informado y capacitado sobre la prohibición de utilizar copias con datos de producción?     - Realice encuestas o entrevistas a empleados para evaluar su conocimiento sobre las políticas relacionadas con la prohibición de utilizar copias con datos sensibles.   + ¿Se implementan controles técnicos para prevenir o detectar el uso de copias con datos de producción actual o históricos? |