

**GASIC 7 – Seguridad en Redes**

**Preguntas de Auditoría**

**Políticas asociadas a 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

Definir una política de seguridad de la información específica para la nube permite a las organizaciones alinear sus niveles aceptables de riesgo con las operaciones en la nube, asegurando el cumplimiento de normativas y estándares internacionales. Estas políticas no solo definen roles y responsabilidades, sino que también establecen procedimientos para la retención, almacenamiento y protección de datos, impactando significativamente en la confianza y seguridad de los servicios cloud utilizados por la organización.

**1.1 Definición y Consistencia de Políticas de Seguridad en la Nube**

Es fundamental que la organización defina una política de seguridad de la información específica para la computación en la nube, la cual debe ser consistente con sus niveles aceptables de riesgo. Al elaborar esta política, se deben considerar aspectos como el acceso y gestión de la información por parte del proveedor de servicios en la nube, la posibilidad de que los activos y aplicaciones se mantengan en entornos cloud, y la ejecución de procesos en servicios virtualizados de múltiples inquilinos. Además, es importante tener en cuenta las ubicaciones geográficas donde el proveedor puede almacenar datos, incluyendo consideraciones sobre jurisdicciones y cumplimiento legal. La dirección debe aprobar formalmente esta política y comunicarla a todos los empleados, contratistas y partes externas relevantes, asegurando su alineación con las mejores prácticas y legislaciones aplicables.

**1.2 Implementación de Procedimientos y Responsabilidades**

La implementación efectiva de las políticas requiere establecer procedimientos claros para la retención y almacenamiento de datos, incluyendo mecanismos de copia de seguridad y redundancia que cumplan con requisitos regulatorios y comerciales. Es necesario realizar pruebas de recuperación de datos en intervalos planificados para asegurar la integridad de las copias de seguridad. Asimismo, se deben definir y/o ampliar las políticas existentes para adaptarse al uso de servicios en la nube, asegurando que los usuarios comprendan sus roles y responsabilidades en este contexto. Esto incluye limitar estrictamente el acceso a datos sensibles desde dispositivos móviles y portátiles, y asignar responsabilidades claras en acuerdos contractuales con proveedores y subcontratistas, considerando el tipo de servicio en la nube utilizado (IaaS, PaaS o SaaS).

**1.3 Auditoría y Mejora Continua de Políticas en la Nube**

Desde una perspectiva de auditoría, es crucial que la dirección revise las políticas de seguridad de la información en intervalos planificados o ante cambios en la organización para garantizar su eficacia y precisión continuas. La alta dirección debe analizar regularmente las políticas implementadas para verificar su correcto funcionamiento y asegurar el cumplimiento de la legislación aplicable, especialmente en materia de protección de Información Personal Identificable (PII). Además, se deben aplicar mejoras basadas en las lecciones aprendidas y el análisis de cumplimiento, ajustando las políticas según sea necesario. Es recomendable solicitar confirmación al proveedor de servicios en la nube sobre sus políticas y procedimientos para la eliminación o reutilización segura de recursos, así como información sobre sus prácticas de desarrollo seguro, fomentando así una cultura de mejora continua en la seguridad 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. Definir una política de seguridad de la información para la computación en la nube como una política temática específica del cliente del servicio en la nube.  1.1 La política de seguridad de la información del cliente del servicio de nube para la computación en la nube debe ser consistente con los niveles aceptables de riesgos de seguridad de la información de la organización para su información y otros activos.  2. Considerar lo siguiente a la hora de definir la política de seguridad de la información para la computación en la nube:  2.1 La información almacenada en el entorno de computación en nube puede estar sujeta a acceso y gestión por parte del proveedor de servicios en nube.  2.2 los activos pueden mantenerse en el entorno de computación en la nube, por ejemplo, programas de aplicación.  2.3 Los procesos pueden ejecutarse en un servicio de nube virtualizado multi-inquilino.  2.4 Los usuarios del servicio en la nube y el contexto en el que utilizan el servicio en la nube.  2.5 Los administradores de servicios en la nube del cliente del servicio en la nube que tienen acceso privilegiado.  2.6 Las ubicaciones geográficas de la organización del proveedor de servicios en la nube y los países donde el proveedor de servicios en la nube puede almacenar los datos del cliente del servicio en la nube (incluso temporalmente).  3. Establecer políticas y procedimientos para la retención y el almacenamiento de datos y se implementarán mecanismos de copia de seguridad o redundancia para garantizar el cumplimiento de los requisitos reglamentarios, estatutarios, contractuales o comerciales. Se deben implementar pruebas de recuperación de copias de seguridad en disco o cinta a intervalos planificados.  4. Establecer una política formal disciplinaria o de sanciones para los empleados que hayan violado las políticas y procedimientos de seguridad. Informar a los empleados qué medidas podrían tomarse en caso de una infracción y se indicará como tal en las políticas y procedimientos.  5. Definir y/o ampliar sus políticas y procedimientos existentes de acuerdo con el uso de los servicios en la nube.  5.1 Hacer que los usuarios de los servicios en la nube sean conscientes de sus roles y responsabilidades en el uso del servicio en la nube. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. La dirección debe aprobar un documento formal de política de seguridad de la información que se comunicará y publicará a los empleados, contratistas y otras partes externas relevantes.  1.1 La Política de Seguridad de la Información deberá establecer la dirección de la organización y alinearse con las mejores prácticas, las leyes regulatorias, federales/estatales e internacionales cuando corresponda.  1.2 Complementar las políticas de seguridad de la información con una declaración sobre el apoyo y el compromiso para lograr el cumplimiento de la legislación de protección de PII aplicable y los términos contractuales acordados entre el procesador de PII de la nube pública y sus clientes (clientes de servicios de nube).  2. Aplicar medidas para limitar estrictamente el acceso a datos sensibles desde dispositivos portátiles y móviles, como ordenadores portátiles, teléfonos móviles y asistentes digitales personales (PDA), que suelen ser de mayor riesgo que los dispositivos no portátiles (por ejemplo, ordenadores de sobremesa en las instalaciones de la organización).  3.Asignar los acuerdos contractuales claramente responsabilidades entre el procesador de PII en la nube pública, sus subcontratistas y el cliente del servicio en la nube, teniendo en cuenta el tipo de servicio en la nube en cuestión (por ejemplo, un servicio de categoría IaaS, PaaS o SaaS)  4. Solicitar confirmación de que el proveedor del servicio en la nube tiene las políticas y procedimientos para la eliminación o reutilización segura de los recursos.  4.1 Solicitar información al proveedor del servicio en la nube sobre el uso de procedimientos y prácticas de desarrollo seguro por parte del proveedor del servicio en la nube.  5. Incluir al proveedor de servicios en la nube como un tipo de proveedor en la política de seguridad de la información para las relaciones con los proveedores.  5.1 Definir los SLA que respaldan los requisitos comerciales , aceptados por el proveedor de servicios y monitoreados por ambas partes.  5.2 Utilizar (como mínimo) los controles recomendados por Cloud Security Alliance proporcionados por los proveedores de servicios en la nube para garantizar la confidencialidad, integridad y disponibilidad de los sistemas. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. La dirección debe revisar la política de seguridad de la información a intervalos planificados o como resultado de cambios en la organización para garantizar su eficacia y precisión continuas. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. La alta dirección debe analizar las políticas implementadas para verificar si se encuentran funcionando adecuadamente. |
| 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. Aplicar mejoras según lo aprendido en el cumplimiento de la legislación de protección de PII aplicable. |

1. **Prácticas de auditoría para Políticas asociadas a la Nube**

|  |
| --- |
| Temática: Definición de la Política |
| Las consideraciones dentro de la definición de la política de seguridad de la información en el contexto de la computación en la nube son cruciales por varias razones. En primer lugar, estas consideraciones abordan los desafíos específicos y las dinámicas únicas asociadas con el entorno de la nube, donde los datos pueden estar sujetos a gestión por parte del proveedor de servicios. La auditoría garantiza que las políticas estén diseñadas de manera efectiva para abordar la seguridad de los datos, la retención de información, la gestión de riesgos y el acceso a los recursos en un entorno virtualizado multi-inquilino. Además, la evaluación de estas consideraciones asegura que la política sea adecuada para la naturaleza dinámica y la geografía dispersa de la nube, así como para la diversidad de usuarios y administradores de servicios en la nube.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se ha definido una política de seguridad de la información específica para la computación en la nube?   + Verifique la aprobación y fecha de implementación de la política de seguridad de la información para la computación en la nube, asegurándose de que esté actualizada y vigente.   + ¿La política en la nube es temática específica del cliente del servicio en la nube?   + ¿Es consistente con los niveles aceptables de riesgos de seguridad de la información de la organización?     - Revisar registros de evaluaciones de riesgos para confirmar que la política se alinea con los niveles aceptables de riesgo definidos por la organización.     - ¿Existen procedimientos claros para notificar y gestionar incidentes de seguridad relacionados con la nube?   + ¿Se aborda adecuadamente la protección de la información y otros activos del cliente en la nube?   + ¿Cómo se definen y comunican los roles y responsabilidades de los usuarios que interactúan con servicios en la nube?   + ¿La política aborda las consideraciones geográficas de la ubicación del proveedor de servicios en la nube y el almacenamiento de datos del cliente?     - Verifique acuerdos contractuales y registros que indiquen la implementación de la política en cuanto a la ubicación geográfica del proveedor de servicios en la nube y el almacenamiento de datos del cliente. * ¿La política de seguridad de la información aborda adecuadamente el acceso y la gestión de la información almacenada en el entorno de computación en la nube por parte del proveedor de servicios en la nube?   + ¿Se tienen medidas específicas en la política para gestionar el acceso privilegiado de los administradores de servicios en la nube del cliente?   + ¿Cómo se garantiza la seguridad de la información cuando los datos están sujetos a acceso y gestión por parte del proveedor de servicios en la nube? * La política de seguridad de la información contempla la posibilidad de que activos, como programas de aplicación, ¿se mantengan en el entorno de computación en la nube?   + Revise registros o documentación de implementación que indiquen si hay programas de aplicación u otros activos en el entorno de la nube y si se alinean con la política. * ¿La política aborda la posibilidad de que los procesos se ejecuten en un servicio de nube virtualizado multiinquilino?   + Verifique si se establece disposiciones específicas sobre la ejecución de procesos en entornos de nube virtualizados multiinquilino. * ¿Se aborda adecuadamente la consideración del contexto de los usuarios del servicio en la nube y cómo utilizan el servicio? * ¿La política disciplinaria está claramente comunicada a los empleados?¿Están actualizadas y reflejan las medidas disciplinarias actuales?   + ¿Las políticas y procedimientos se informan claramente a los empleados sobre las medidas que podrían tomarse en caso de una infracción? * ¿El proveedor del servicio en la nube tiene políticas y procedimientos establecidos para la eliminación o reutilización segura de los recursos?   + ¿Se ha solicitado información al proveedor del servicio en la nube sobre el uso de procedimientos y prácticas de desarrollo seguro?   + ¿El proveedor de servicios en la nube está incluido como un tipo de proveedor en la política de seguridad de la información para las relaciones con los proveedores?   + ¿Se han definido SLA respaldando los requisitos comerciales, aceptados por el proveedor de servicios en la nube y monitoreados por ambas partes?   + ¿La organización utiliza, como mínimo, los controles recomendados por Cloud Security Alliance proporcionados por los proveedores de servicios en la nube? * ¿La dirección realiza revisiones planificadas de la política de seguridad de la información?   + Verifique la existencia de un programa formal de revisiones periódicas en la documentación.   + Revise los registros de cambios implementados como resultado de las revisiones para evaluar si indican mejoras en la eficacia o precisión de la política. * ¿La alta dirección realiza análisis regulares de las políticas implementadas para verificar su eficacia?   + ¿Existe un proceso formalizado para llevar a cabo la revisión y análisis de las políticas implementadas? |

|  |
| --- |
| Temática: Retención y almacenamiento de datos |
| La auditoría de la retención y almacenamiento de datos en la computación en la nube es esencial para asegurar el cumplimiento normativo, la protección de datos sensibles y la garantía de la seguridad y disponibilidad continua de la información. Al evaluar prácticas como la redundancia, copias de seguridad y procedimientos de eliminación segura, se fortalece la capacidad de respuesta ante incidentes y se mitigan riesgos potenciales, previniendo pérdidas financieras y daños a la reputación. Además, la auditoría contribuye a la eficiencia operativa al gestionar de manera efectiva los recursos y garantizar que las políticas estén alineadas con regulaciones específicas. En última instancia, este proceso de auditoría facilita la mejora continua de las prácticas de seguridad, promoviendo la resiliencia empresarial y asegurando la integridad y confidencialidad de los datos almacenados en la nube.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización ha establecido políticas y procedimientos claros para la retención y el almacenamiento de datos?   + ¿Se han establecido periodos específicos de retención de datos en la nube?   + ¿Se implementan mecanismos de copia de seguridad o redundancia para garantizar el cumplimiento de los requisitos reglamentarios, estatutarios, contractuales o comerciales?   + ¿Se realizan pruebas de recuperación de copias de seguridad en disco o cinta a intervalos planificados?   + ¿Cómo se determina la duración de retención de datos y qué factores se tienen en cuenta?   + ¿Existe documentación que respalde la realización y los resultados de las pruebas de recuperación de copias de seguridad?     - Verifique la disponibilidad de informes de análisis post-prueba que indiquen las lecciones aprendidas y las mejoras implementadas después de las pruebas.   + ¿Los datos se categorizan según su importancia y sensibilidad para determinar las políticas de retención?   + ¿Con qué frecuencia se realizan las copias de seguridad y cómo se verifica su integridad?   + ¿Existen procedimientos claros y seguros para la eliminación de datos cuando ya no son necesarios? * ¿Existen medidas implementadas para limitar estrictamente el acceso a datos sensibles desde dispositivos portátiles y móviles?   + ¿Están claramente definidos los tipos de datos considerados como sensibles y sujetos a restricciones de acceso desde dispositivos portátiles y móviles?   + ¿Se proporciona capacitación regular al personal sobre las medidas y restricciones de acceso desde los diferentes dispositivos?   + ¿Se realizan evaluaciones periódicas para garantizar el cumplimiento de las medidas de seguridad? |

|  |
| --- |
| Temática: Protección de identificación personal (PII) |
| La protección de la Información de Identificación Personal (PII) en entornos de computación en la nube es crucial debido a la sensibilidad y privacidad asociadas con estos datos. La PII incluye información personal como nombres, direcciones y números de identificación, cuyo acceso no autorizado puede tener consecuencias graves, como robo de identidad o violaciones de privacidad.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La Dirección ha aprobado formalmente un documento de política de seguridad de la información?   + Verifique la fecha de emisión y aprobación del documento de política de seguridad de la información para asegurarse de que esté actualizado y vigente.   + ¿Establece claramente la dirección de la organización y se alinea con las mejores prácticas y las leyes regulatorias pertinentes?   + ¿Existe una declaración explícita en la política que respalde y se comprometa a cumplir con la legislación de protección de PII y los términos contractuales de la nube pública? * ¿Se han establecido acuerdos contractuales claros que definan las responsabilidades entre el procesador de PII en la nube pública, sus subcontratistas y el cliente del servicio en la nube?   + ¿Las responsabilidades asignadas en los acuerdos contractuales son específicas y adecuadas para el tipo de servicio en la nube utilizado (IaaS, PaaS, SaaS, etc.)?   + ¿Cómo se adaptan los acuerdos contractuales a diferentes tipos de servicios en la nube (IaaS, PaaS, SaaS)?   + ¿Se han establecido cláusulas contractuales para abordar la subcontratación y las responsabilidades asociadas?   + ¿Existen mecanismos para evaluar regularmente el cumplimiento de estas responsabilidades?   + ¿Cómo se comunican y cumplen los términos contractuales con los clientes de servicios de nube en relación con la protección de PII?     - ¿Cómo se asegura la comunicación efectiva de las mejoras a todas las partes interesadas relevantes? * ¿Se ha identificado la legislación de protección de PII aplicable a la organización?   + ¿Se ha implementado un proceso de aprendizaje continuo para mantenerse actualizado sobre las novedades en la legislación de protección de PII?   + ¿La organización ha aplicado mejoras específicas en sus procesos y políticas de manejo de PII en función de lecciones aprendidas durante auditorías anteriores o incidentes de seguridad?   + ¿Se han llevado a cabo evaluaciones periódicas de la efectividad de las mejoras implementadas en el cumplimiento de la legislación de protección de PII? |