

**GASIC 7 – Seguridad en Redes**

**Preguntas de Auditoría**

**Legal y Regulatorio**

**Competencias Básicas del Auditor**

1. **Conocimiento de las Normas y Regulaciones:** Un auditor debe estar familiarizado con las normas, regulaciones y estándares relevantes en el ámbito de la ciberseguridad (como ISO 27001, CIS, NIST CSF, etc.) y la gestión de personas (estatuto administrativo, normativa interna).
2. **Habilidades Analíticas:** La capacidad de analizar datos, identificar patrones y hacer conexiones entre información aparentemente no relacionada es esencial.
3. **Comunicación Efectiva:** Un auditor debe ser capaz de comunicar sus hallazgos de manera clara y concisa, tanto por escrito como verbalmente.
4. **Conocimiento Técnico:** Es esencial tener un conocimiento profundo de las tecnologías y sistemas que se están auditando. En particular, debe conocer el funcionamiento y arquitectura de los sistemas de apoyo para la gestión de recursos humanos (hrms).
5. **Conocimiento de las Amenazas Actuales:** El panorama de amenazas de ciberseguridad está en constante evolución. En particular, la de gestión de personas requiere un conocimiento en profundidad de las técnicas más comunes, como las de ingeniería social.
6. **Capacidad de Evaluación de Riesgos:** Evaluar y priorizar riesgos es una habilidad clave. Un auditor debe ser capaz de determinar qué áreas presentan el mayor riesgo y recomendar medidas para mitigar esos riesgos.

# Visión General

La auditoría de los aspectos legales y regulatorios de la seguridad en la nube es un proceso en el que se evalúa el cumplimiento de las leyes, regulaciones y estándares relacionados con la seguridad y protección de datos en un entorno de nube, según el contexto de la empresa. Es crucial considerar los acuerdos entre el proveedor del servicio y el cliente, que abarcan la asignación de funciones y responsabilidades relacionadas con el servicio en la nube, incluyendo la protección contra malware, respaldos y pruebas de seguridad, entre otros. Por lo tanto, esta revisión implica que los acuerdos contractuales se verifiquen solicitando pruebas de que los estándares de seguridad se apliquen adecuadamente para garantizar la seguridad de la información.

**1.1 Leyes y regulaciones**

Dependiendo de la ubicación del proveedor y del cliente, existen diferentes leyes de seguridad de datos que deben cumplirse. Un ejemplo de reglamento enfocado en la seguridad de los datos de los usuarios es el Reglamento General de Protección de Datos (GDPR), que tiene como objetivo fortalecer y unificar la protección de los datos en la Unión Europea y establece normas estrictas en cuanto a la privacidad de los datos personales. También se consideran los marcos regulatorios dentro de una empresa, como NIST o ISO, que tienen controles sobre la seguridad de los datos en la nube.

**1.2 Acuerdos contractuales**

La auditoría de los acuerdos contractuales es esencial para garantizar que los términos y condiciones establecidos en los contratos cumplan con los estándares de seguridad y privacidad requeridos. Es vital verificar que el contrato establezca claramente la responsabilidad del proveedor de cumplir con las leyes y regulaciones pertinentes, como GDPR u otras, según la naturaleza de los datos almacenados. Además, debe definir las obligaciones del proveedor de servicio, como mantener la seguridad de la información en los datos que se encuentren 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. Identificar las autoridades pertinentes para la operación combinada del cliente del servicio en la nube y del proveedor del servicio en la nube.  2. Confirmar las funciones y responsabilidades de seguridad de la información relacionadas con el servicio en la nube, como se describe en el acuerdo de servicio.  2.1. Protección de malware;  2.2. Respaldo;  2.3. Controles criptográficos;  2.4. Gestión de la vulnerabilidad;  2.5. Administracion de incidentes;  2.6. Control del cumplimiento técnico;  2.7. Pruebas de seguridad;  2.8. Auditoría;  2.9. Recopilación, mantenimiento y protección de pruebas, incluidos registros y pistas de auditoría;  2.10. Protección de la información tras la terminación del contrato de servicio;  2.11. Autenticación y control de acceso;  2.12. Gestión de identidad y acceso.  3. Tener un procedimiento para identificar los requisitos de licencia específicos de la nube antes de permitir que se instale cualquier software con licencia en un servicio en la nube. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Considerar la cuestión de que las leyes y regulaciones relevantes pueden ser las de las jurisdicciones que rigen al proveedor de servicios en la nube, además de las que rigen al cliente del servicio en la nube.  1.1 Las obligaciones del responsable del tratamiento de la PII a este respecto pueden estar definidas por ley, reglamento o contrato. Incluir estas obligaciones en asuntos en los que el cliente del servicio en la nube utiliza los servicios del público.  1.2 El encargado del tratamiento de la IIP en la nube pública deberá elaborar y aplicar una política relativa a la eliminación de la IIP y ponerla a disposición del cliente del servicio en la nube.  1.3 Cuando se apliquen acuerdos contractuales específicos a la transferencia internacional de datos, como las Cláusulas Contractuales Modelo, las Normas Corporativas Vinculantes o las Normas de Privacidad Transfronteriza, también deberán identificarse los acuerdos y los países o circunstancias en los que se aplican dichos acuerdos.  2. Solicitar pruebas del cumplimiento por parte del proveedor del servicio en la nube de las regulaciones y estándares pertinentes requeridos para el negocio del cliente del servicio en la nube.  2.1 Implementar controles de seguimiento adecuados para garantizar que se cumplan las obligaciones contractuales. |
| 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. Tener identificadores claros donde se reconozcan a las autoridades pertinentes para la operación combinada.  1.1. Tener confirmadas las funciones y responsabilidades de seguridad de la información relacionadas con el servicio en la nube.  1.2 Deben existir un procedimiento para identificar los requisitos de licencia específicos de 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. Aplicar sanciones según los controles de seguimiento para garantizar que se cumplan las obligaciones contractuales.  1.1 Mejora y verificación por medio de pruebas del cumplimiento por parte del proveedor del servicio en la nube de las regulaciones y estándares pertinentes. |

1. **Preguntas de Auditoría para lo Legal y Regulatorio**

|  |
| --- |
| Temática: Leyes y Regulaciones |
| Este proceso implica revisar y evaluar el cumplimiento de una organización con las leyes y regulaciones aplicadas en esta organización que pueden variar según la industria, la ubicación geográfica y el tipo de negocio. La auditoría legal garantiza que la organización cumple con estas leyes, lo que evita sanciones legales, multas y otras consecuencias adversas.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se han identificado claramente las autoridades pertinentes para la operación combinada del cliente del servicio en la nube y del proveedor del servicio en la nube?   + Revise la documentación contractual, acuerdos de nivel de servicio (SLA) y otros documentos pertinentes para verificar la identificación de las autoridades y sus roles en la operación combinada.   + ¿Las funciones y responsabilidades de seguridad de la información relacionadas con el servicio en la nube están confirmadas y documentadas según lo descrito en el acuerdo de servicio? * ¿Se tiene implementado un procedimiento para identificar los requisitos de licencia antes de permitir que se instale software con licencia?   + ¿Existe un procedimiento establecido para identificar los requisitos de licencia específicos de la nube antes de permitir la instalación de cualquier software con licencia?     - ¿El procedimiento establece claramente quién es responsable de la identificación de requisitos de licencia antes de la instalación en la nube?   + Verifique la existencia de formularios o documentos estandarizados utilizados para recopilar información sobre requisitos de licencia antes de instalar software en la nube.   + ¿Cómo se garantiza el cumplimiento continuo con los términos de las licencias durante la operación en la nube?   + ¿El procedimiento incluye pasos claros para evaluar y verificar la conformidad de los requisitos de licencia del software con las políticas de la nube antes de la instalación?   + ¿Se lleva a cabo formación y concientización periódica para aquellos responsables de identificar requisitos de licencia antes de instalar software en la nube? * ¿Se documentan claramente las obligaciones del responsable del tratamiento de la información personal en términos de leyes, reglamentos o contratos? * ¿La organización considera las leyes y regulaciones pertinentes de las jurisdicciones que rigen tanto al proveedor de servicios en la nube como al cliente del servicio en la nube?   + ¿Cuándo se aplican acuerdos contractuales específicos a la transferencia internacional de datos, como Cláusulas Contractuales Modelo, Normas Corporativas Vinculantes o Normas de Privacidad Transfronteriza, se identifican adecuadamente los acuerdos y los países o circunstancias a los que se aplican?   + ¿Las obligaciones del responsable del tratamiento de la PII respecto a las leyes, reglamentos o contratos están claramente definidas y se incorporan en asuntos en los que el cliente utiliza servicios en la nube pública?   + ¿El encargado del tratamiento de la PII en la nube pública ha desarrollado y aplicado una política sobre la eliminación de la información personal identificable (IIP) y la ha puesto a disposición del cliente del servicio en la nube? * ¿Se han solicitado pruebas del cumplimiento por parte del proveedor del servicio en la nube con las regulaciones y estándares relevantes para el negocio del cliente?   + Obtenga confirmación del departamento legal o de cumplimiento de la organización de que se han solicitado y recibido pruebas de cumplimiento del proveedor del servicio en la nube.   + ¿Existen controles de seguimiento implementados para garantizar el cumplimiento de las obligaciones contractuales con el proveedor del servicio en la nube?     - ¿Existe un proceso para identificar los países o circunstancias en los que se aplican estos acuerdos?     - Revise los contratos y acuerdos con el proveedor del servicio en la nube para identificar cláusulas específicas relacionadas con el cumplimiento y los controles de seguimiento. * ¿Se ha establecido un proceso documentado para la revisión regular y la actualización de las pruebas de cumplimiento del proveedor del servicio en la nube?   + ¿Quién realiza este proceso de identificar y documentar los acuerdos contractuales en base a la transferencia internacional de datos?   + ¿Se documentan y archivan adecuadamente las pruebas de cumplimiento recibidas del proveedor del servicio en la nube? * ¿Se han establecido identificadores claros donde se reconozcan a las autoridades pertinentes para la operación combinada?   + Revise la documentación organizacional para identificar si hay identificadores claros, como roles o designaciones, para las autoridades responsables de la operación combinada.   + ¿Se han confirmado y documentado las funciones y responsabilidades de seguridad de la información relacionadas con el servicio en la nube?   + ¿Existe un procedimiento documentado para identificar los requisitos de licencia específicos de la nube? * ¿Se aplican sanciones de manera consistente según los controles de seguimiento para garantizar el cumplimiento de las obligaciones contractuales?   + Revise los registros de sanciones aplicadas en situaciones específicas donde se violaron las obligaciones contractuales. Comparar estas sanciones con los controles de seguimiento establecidos en la política de la empresa.   + ¿Se realiza mejora y verificación a través de pruebas para evaluar el cumplimiento del proveedor del servicio en la nube con las regulaciones y estándares pertinentes?     - Evalúe los informes de pruebas de cumplimiento realizadas por terceros o internamente para verificar que se estén llevando a cabo de manera regular y que se esté evaluando el cumplimiento del proveedor del servicio en la nube con las regulaciones y estándares aplicables.   + ¿Existe evidencia de que las sanciones aplicadas han llevado a mejoras en el cumplimiento por parte del proveedor del servicio en la nube? |