

**GASIC 7 – Seguridad en Redes**

**Preguntas de Auditoría**

**Control de Acceso a la Nube**

**Competencias Básicas del Auditor**

1. **Conocimientos Técnicos:** Entender a fondo los aspectos técnicos relevantes, como sistemas de información, redes y regulaciones, para llevar a cabo auditorías efectivas.
2. **Comprensión del Negocio:** Comprender el contexto empresarial y los objetivos estratégicos para alinear la auditoría con las metas organizativas.
3. **Habilidades Analíticas:** Analizar datos para identificar patrones y tendencias, proporcionando insights que respalden la toma de decisiones informada.
4. **Habilidades de Comunicación:** Comunicar de manera clara y efectiva los hallazgos de la auditoría tanto por escrito como verbalmente a diversos públicos.
5. **Ética Profesional:** Actuar con integridad, manteniendo la confidencialidad y la objetividad durante el proceso de auditoría.
6. **Adaptabilidad:** Adaptarse a cambios en entornos tecnológicos, legales y empresariales para abordar nuevos desafíos.
7. **Gestión del Tiempo:** Gestionar eficientemente el tiempo y los recursos para cumplir con los plazos de auditoría.
8. **Enfoque en Resultados:** Concentrarse en lograr objetivos y proporcionar recomendaciones prácticas que contribuyan a la mejora continua.

# Visión General

El control de acceso en la nube es un pilar fundamental para garantizar la seguridad de los datos y servicios alojados en entornos cloud. Una gestión adecuada de los accesos asegura que solo los usuarios autorizados interactúen con los recursos, minimizando riesgos asociados a accesos no autorizados, pérdida de información o compromisos de cuentas. Implementar políticas robustas de control de acceso, basadas en autenticación avanzada y gestión centralizada, es crucial para mantener la integridad y la confidencialidad de los datos en la nube.

**1.1 Requisitos y Técnicas de Autenticación**

Para proteger los servicios en la nube, es esencial especificar los requisitos de acceso para cada servicio, asegurándose de que los procedimientos de autenticación del proveedor cumplan con los estándares del cliente. Esto incluye implementar técnicas avanzadas como la autenticación multifactor para administradores, garantizando que solo usuarios verificados puedan realizar cambios administrativos. Adicionalmente, el uso de tecnologías abiertas, como inicio de sesión único (SSO) y autenticación abierta, facilita una gestión segura y eficiente, reduciendo la dependencia de sistemas propietarios.

**1.2 Gestión de Accesos y Restricciones**

El control de acceso en la nube debe incluir la capacidad de restringir el acceso a datos, servicios y funciones específicas, según las políticas definidas por el cliente. Esto abarca gestionar el aprovisionamiento, desaprovisionamiento y modificaciones de roles de los usuarios de manera automatizada y controlada, minimizando errores humanos. Además, es crucial implementar controles para programas y utilidades que puedan anular medidas de seguridad, asegurando que no existan brechas que permitan eludir las políticas de acceso establecidas.

**1.3 Auditoría y Mejora Continua del Control de Acceso**

Desde la perspectiva de auditoría, es necesario mantener indicadores que permitan monitorear accesos no autorizados y medir el cumplimiento de las políticas de control de acceso a la nube. Estos datos deben ser analizados para identificar desviaciones y oportunidades de mejora. Las lecciones aprendidas de estos análisis deben traducirse en actualizaciones de políticas y procedimientos, fortaleciendo continuamente la gestión de accesos y reduciendo el riesgo de incidentes de seguridad en entornos cloud.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Especificar los requisitos para el acceso de los usuarios a cada servicio de nube separado que se utilice dentro de la política de control de acceso para el uso de servicios de red.  2. Verificar el procedimiento de gestión del proveedor del servicio en la nube para asignar información de autenticación secreta, como contraseñas, cumpla con los requisitos del cliente del servicio en la nube.  3. Abordar los procedimientos para el registro y la baja de usuarios la situación en la que el control de acceso de los usuarios se ve comprometido, como la corrupción o el compromiso de contraseñas u otros datos de registro de usuarios. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Utilizar suficientes técnicas de autenticación (por ejemplo, autenticación multifactor) para autenticar a los administradores del servicio en la nube del cliente del servicio en la nube en las capacidades administrativas de un servicio en la nube de acuerdo con los riesgos identificados.  2. Utilizar inicio de sesión único y autenticación abierta (a diferencia de las tecnologías de autenticación patentadas por los proveedores de servicios.  3. Garantizar que el acceso a la información en el servicio en la nube pueda restringirse de acuerdo con su política de control de acceso y que dichas restricciones se cumplan.  3.1 Incluir restricción del acceso a los servicios en la nube, las funciones del servicio en la nube y los datos de los clientes del servicio en la nube mantenidos en el servicio.  4. Implementar medidas, como controlar el acceso, para garantizar que la información registrada solo se utilice para los fines previstos.  5. Implementar un procedimiento, preferiblemente automático, para garantizar que la información registrada se elimine dentro de un período específico y documentado.  6. Proporcionar cuando sea necesario procedimientos de inicio de sesión seguros para cualquier cuenta solicitada por el cliente del servicio de nube para los usuarios del servicio de nube bajo su control.  7. Gestionar el acceso de los usuarios del servicio de nube bajo el control del cliente del servicio de nube, por ejemplo, proporcionando derechos administrativos para gestionar o cancelar el acceso.  8. Restringir los programas de utilidad capaces de anular potencialmente los controles de sistemas, objetos, redes, máquinas virtuales y aplicaciones. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Gestionar de manera oportuna y controlada, de acuerdo con las políticas internas de acceso de usuarios el aprovisionamiento de usuarios (incorporación), el desaprovisionamiento (terminación) y los cambios en las funciones laborales de las aplicaciones y plataformas operativas basadas en la nube. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Mantener indicadores para medir el acceso no autorizado de usuarios a la nube.  1.1 Deben existir indicadores para medir el cumplimiento de la política de control de acceso a 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 mejoras según lo aprendido o el análisis de datos realizado en relación con el cumplimiento de política de control de acceso a la nube. |

1. **Preguntas de Auditoría para el Control de Acceso a la Nube**

|  |
| --- |
| Temática: Gestión de Acceso de los Usuarios a los Servicios de la Nube |
| La gestión de acceso de los usuarios a los servicios de la nube implica evaluar y verificar los controles y mecanismos utilizados para garantizar que solo las personas autorizadas tengan acceso a los recursos y datos almacenados en la nube. Debe revisar y analizar las políticas y procedimientos de control de acceso implementados, así como las configuraciones de seguridad y los registros de actividad. También debe evaluar la efectividad de las medidas de autenticación, como contraseñas, autenticación de dos factores u otros métodos utilizados para verificar la identidad de los usuarios.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existen políticas y procedimientos documentados para la gestión de acceso de usuarios a los servicios de la nube?   + ¿Se asegura que estas políticas estén alineadas con las mejores prácticas de seguridad de la nube?   + ¿Se han especificado claramente los requisitos para el acceso de los usuarios a cada servicio de nube dentro de la política de control de acceso para el uso de servicios de red?   + ¿El acceso a la información en el servicio en la nube puede restringirse de acuerdo con la política de control de acceso y se están cumpliendo esas restricciones? * ¿Se gestiona de manera oportuna y controlada el aprovisionamiento de usuarios de acuerdo con las políticas internas de acceso?   + Evalúe el tiempo promedio entre la solicitud de creación de un nuevo usuario y su efectiva incorporación para asegurarse de que esté en línea con las políticas internas establecidas.   + ¿Se lleva a cabo de manera controlada el desaprovisionamiento (terminación) de usuarios según las políticas internas?   + ¿Los cambios en las funciones laborales de los usuarios en aplicaciones y plataformas basadas en la nube se gestionan de manera controlada?   + ¿Existe un sistema de seguimiento para verificar y documentar la gestión de usuarios, incluyendo el aprovisionamiento, desaprovisionamiento y cambios en funciones laborales? * ¿Cómo se gestiona la creación, modificación y eliminación de identidades de usuario en los servicios de la nube?   + ¿Se han abordado de manera adecuada los procedimientos para el registro y la baja de usuarios en situaciones donde el control de acceso se ve comprometido, como la corrupción o el compromiso de contraseñas u otros datos de registro?   + ¿Se realiza una revisión periódica y actualización de los requisitos de acceso de los usuarios a los servicios de nube?¿Se sigue un proceso de revisión regular para garantizar la precisión de las identidades?     - Revise los registros de revisiones periódicas de los requisitos de acceso a los servicios de nube, asegurándose de que estas revisiones se realicen según la frecuencia especificada en la política de control de acceso.   + ¿Los procedimientos de registro y baja de usuarios incluyen medidas de auditoría para rastrear las acciones tomadas durante estas operaciones? * ¿Cuáles son los métodos de autenticación utilizados para acceder a los servicios en la nube?   + ¿Se implementa un sistema de autorización que limite el acceso a recursos específicos basándose en roles y necesidades?   + ¿El procedimiento de gestión del proveedor del servicio en la nube para asignar información de autenticación secreta cumple con los requisitos establecidos por el cliente del servicio en la nube?     - Evalúe los registros de asignación de información de autenticación secreta para confirmar que el proveedor del servicio en la nube sigue los procedimientos acordados con el cliente.   + ¿Se utilizan suficientes técnicas de autenticación, como autenticación multifactor, para autenticar a los administradores del servicio en la nube del cliente en las capacidades administrativas de acuerdo con los riesgos identificados?     - Revise la configuración de autenticación en el servicio en la nube para confirmar si se está utilizando inicio de sesión único y autenticación abierta.   + ¿Se promueve la conciencia de seguridad entre los usuarios para evitar prácticas riesgosas con sus credenciales? * ¿Se registran y supervisan las actividades de acceso de los usuarios en los servicios de la nube?   + ¿Existen mecanismos para evaluar la efectividad de los controles de acceso a los servicios de nube?     - Revise informes o registros de evaluaciones de la efectividad de los controles de acceso a servicios de nube, como auditorías internas o externas para revisar si se han implementado recomendaciones de evaluaciones anteriores para mejorar la efectividad de los controles de acceso.   + ¿Cómo se gestionan los registros de actividades y se utilizan para detectar posibles anomalías?   + ¿Existe un plan de respuesta a incidentes específico para situaciones en las que el control de acceso de los usuarios se ve comprometido?   + ¿Se implementan medidas de control de acceso, para garantizar que la información registrada solo se utilice para los fines previstos? * ¿Se gestiona el acceso de los usuarios del servicio de nube bajo el control del cliente, proporcionando derechos administrativos para gestionar o cancelar el acceso?   + Revise la documentación de gestión de acceso del servicio de nube para confirmar la asignación de derechos administrativos a los usuarios bajo el control del cliente.   + ¿Cómo se gestiona la duración de las sesiones de usuario en los servicios de la nube?   + ¿Se implementan controles para cerrar automáticamente sesiones activas? * ¿Se utiliza inicio de sesión único y autenticación abierta en lugar de tecnologías de autenticación patentadas por los proveedores de servicios?   + ¿Se proporcionan procedimientos de inicio de sesión seguros cuando sea necesario para cuentas solicitadas por el cliente del servicio de nube? * ¿La organización mantiene indicadores para medir el acceso no autorizado de usuarios a la nube?   + Revise la existencia de registros de acceso que permitan identificar cualquier intento o instancia de acceso no autorizado a recursos de la nube. Estos registros deben incluir información detallada sobre el usuario, la hora, el tipo de acceso y cualquier actividad sospechosa.   + ¿Existen indicadores para medir el cumplimiento de la política de control de acceso a la nube?   + Evalúe la documentación de la política de control de acceso a la nube y compararla con los indicadores mantenidos para medir el cumplimiento. Debe haber claridad en cómo se miden y evalúan los aspectos específicos de la política. * ¿Se ha realizado un análisis de datos para evaluar el cumplimiento de la política de control de acceso a la nube?   + ¿Las mejoras identificadas durante el análisis de datos se aplican de manera efectiva?   + ¿Existe un proceso formalizado para aplicar mejoras basadas en el aprendizaje o análisis de datos relacionados con el control de acceso a la nube? |

|  |
| --- |
| Temática: Restricción a los Programas de Utilidad |
| Esto implica una revisión exhaustiva de las políticas y medidas implementadas para prevenir y mitigar el riesgo asociado con herramientas que podrían comprometer la seguridad de sistemas, objetos, redes, máquinas virtuales y aplicaciones. Esto abarca la evaluación de las políticas de acceso y autorización para la instalación y ejecución de programas de utilidad, así como la implementación de controles técnicos que restrinjan el uso de herramientas potencialmente peligrosa.Este levantamiento puede incluir análisis específicos tales como:¿Cómo se gestiona el acceso y la autorización para la instalación y ejecución de programas de utilidad?Realice una revisión de los controles de acceso para garantizar que solo usuarios autorizados puedan ejecutar estos programas.¿Cómo se asegura de que solo los usuarios autorizados tengan permisos para instalar y ejecutar programas de utilidad? ¿Se utilizan mecanismos de autenticación y autorización?¿Existe una lista autorizada de programas de utilidad que pueden ser utilizados y están permitidos?Realice una auditoría para verificar la existencia de un inventario y su precisión, asegurando que solo se permitan las herramientas necesarias.¿Se lleva a cabo una revisión periódica de la lista de programas de utilidad permitidos y se actualiza según sea necesario?¿Se implementan controles de acceso y restricciones para prevenir la ejecución no autorizada de programas de utilidad?Revise los registros de eventos para identificar y analizar la actividad de ejecución de herramientas, asegurando la detección temprana de comportamientos inusuales.¿Cuál es el proceso para monitorear la actividad relacionada con la ejecución de programas de utilidad y cómo se abordan los eventos detectados?Realice pruebas de ejecución de programas de utilidad no autorizados en entornos controlados para evaluar la efectividad de las restricciones implementadas.¿Se documentan y monitorean las excepciones a la restricción de programas de utilidad, y se justifican adecuadamente? |