

02 - Atributos de Seguridad y Privacidad

**CASIG 4 – Control de Acceso e Identidades**

**Preguntas de Auditoría**

**Atributos de Seguridad y Privacidad**

|  |
| --- |
| **Competencias Básicas del Auditor**   1. **Conocimiento de Normativas y Estándares**: Familiaridad con marcos de referencia y estándares de la industria como NIST, ISO 27001, CIS, entre otros. 2. **Habilidades Analíticas**: Capacidad para analizar registros, logs y datos para identificar patrones anómalos o actividades sospechosas. 3. **Comprensión de Sistemas de Autenticación**: Entender diferentes mecanismos de autenticación, como autenticación de dos factores, tokens, certificados digitales, entre otros. 4. **Conocimiento de Tecnologías de Red**: Entender cómo funcionan las redes, protocolos y cómo se pueden explotar las vulnerabilidades relacionadas con el acceso. 5. **Habilidades de Comunicación**: Capacidad para comunicar hallazgos, riesgos y recomendaciones de manera clara a diferentes audiencias, desde técnicos hasta ejecutivos. 6. **Conocimiento de Herramientas de Auditoría**: Familiaridad con herramientas y software específicos utilizados para auditar sistemas y redes. 7. **Comprensión de la Gestión de Riesgos**: Capacidad para identificar, evaluar y priorizar riesgos asociados con la administración de cuentas y credenciales. 8. **Habilidades de Investigación**: Capacidad para investigar incidentes de seguridad, identificar la causa raíz y recomendar medidas correctivas. 9. **Conocimiento de Procesos de Negocio**: Entender cómo funcionan los procesos de negocio y cómo la administración de cuentas y credenciales se integra en ellos. 10. **Habilidades Interpersonales**: Capacidad para trabajar en equipo, gestionar conflictos y colaborar con diferentes departamentos y partes interesadas. 11. **Conocimiento de Legislación y Cumplimiento**: Estar al tanto de las leyes y regulaciones pertinentes que afectan la administración de cuentas y credenciales en la jurisdicción relevante. |

# Visión General

La gestión de atributos de seguridad y privacidad en la función de seguridad de la información y ciberseguridad (SIC) asegura que los datos sean manejados de acuerdo con políticas de seguridad y privacidad precisas, estableciendo y manteniendo asociaciones de atributos específicos con la información en almacenamiento, proceso o transmisión. Estos atributos permiten definir valores o rangos autorizados que facilitan la clasificación y protección de datos sensibles, asociando dinámicamente atributos de seguridad a sujetos y objetos mientras se crea y manipula la información. Este enfoque asegura que el acceso y los cambios en los atributos de seguridad y privacidad sean realizados solo por personal autorizado, manteniendo así la integridad y coherencia de estas asociaciones en todas las etapas del manejo de la información.

**1.1 Administración y Control de Atributos de Seguridad y Privacidad**

Para reforzar la administración de atributos, la organización proporciona a las personas autorizadas la capacidad de definir o modificar los valores de estos atributos, asegurando que se mantenga una coherencia en los sistemas distribuidos y que los atributos sean fácilmente interpretables por los usuarios a través de convenciones estándar. Los atributos de seguridad y privacidad se muestran de manera legible en cada objeto transmitido, indicando instrucciones específicas de manejo o diseminación según corresponda. Además, se implementan técnicas y tecnologías validadas que permiten el cambio de atributos solo a través de mecanismos de recalificación formalizados, asegurando que cualquier modificación en los atributos siga un proceso documentado y controlado.

**1.2 Rol de la Auditoría en la Gestión de Atributos de Seguridad y Privacidad en SIC**

Desde la perspectiva de auditoría, la gestión de atributos de seguridad y privacidad en SIC se supervisa mediante revisiones periódicas de los atributos definidos, verificando su coherencia con las políticas de seguridad de la organización. La auditoría revisa y documenta todos los cambios realizados en los atributos de seguridad, evaluando que estos se mantengan alineados con las políticas y procedimientos establecidos. Esta supervisión permite detectar cualquier desajuste o necesidad de actualización, promoviendo una mejora continua en la gestión de atributos y garantizando que las prácticas de seguridad y privacidad evolucionen conforme a las necesidades de la organización.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Proporcionar los medios para asociar los tipos de atributos de seguridad y privacidad con valores de atributo de seguridad y privacidad para la información en almacenamiento, en proceso y/o en transmisión.  2. Asegurar de que las asociaciones de tributos se realicen y se conserven con la información.  3. Establecer los siguientes atributos de seguridad y privacidad permitidos a partir de los atributos definidos para sistemas o atributos de seguridad y privacidad.  4. Determinar los siguientes valores de atributos o rangos permitidos para cada uno de los atributos establecidos: Valores de atributos definidos por la organización o rangos para atributos establecidos.  5. Asociar dinámicamente atributos de seguridad y privacidad con sujetos y objeto de acuerdo con las políticas de seguridad y privacidad a medida que se crea y combina la información.  6. Proporcionar a personas autorizadas (o procesos que actúen en nombre de personas) la capacidad de definir o cambiar el valor de los atributos de seguridad y privacidad asociados.   7. Mantener la asociación e integridad de atributos de seguridad y privacidad a sujetos y objetos.  8. Proporcionar la capacidad de asociar atributos de seguridad y privacidad con sujetos y objetos por personas autorizadas (o procesos que actúan en nombre de personas).  9. Mostrar atributos de seguridad y privacidad en forma legible por humanos en cada objeto que el sistema transmite a los dispositivos de salida para identificar instrucciones especiales de diseminación, manejo o distribución usando convenciones de nomenclatura estándar legibles por humanos.  10. Implementar técnicas y tecnologías definidas por la organización al asociar atributos de seguridad y privacidad a la información.  11.Cambiar los atributos de seguridad y privacidad asociados con la información solo a través de mecanismos de recalificación validados usando técnicas o procedimientos definidos por la organización.  12. Proporcionar a las personas autorizadas la capacidad de definir o cambiar el tipo y el valor de los atributos de seguridad y privacidad disponibles para la asociación con sujetos y objetos. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Proporcionar una interpretación coherente de los atributos de seguridad y privacidad transmitidos entre los componentes del sistema distribuido.   2. Requerir que el personal asocie y mantengan la asociación de atributos de seguridad y privacidad definidos por la organización con sujetos y objetos definidos por la organización de acuerdo con las políticas de seguridad y privacidad definidas por la organización. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Revisar atributos de seguridad y privacidad definidos por la organización para ver si es aplicable con una frecuencia definida por la organización. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Auditar cambios en los atributos. |

# Preguntas de Auditoría para los Atributos de Seguridad y Privacidad

|  |
| --- |
| 3.1 Temática: Asociación y capacidades de los atributos |
| La práctica consiste en buscar y garantizar que los atributos trabajen de manera sinérgica y coherente para fortalecer la postura general de seguridad. Se analiza cómo los diferentes atributos, están vinculados en la protección de los activos de información y verificar si estos atributos interactúan de manera eficiente para establecer una defensa sólida contra amenazas y riesgos. Los atributos deben estar diseñados para adaptarse a nuevas amenazas y tecnologías emergentes, lo que garantiza una respuesta efectiva a los desafíos futuros.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización tiene definidos atributos de seguridad y privacidad? * ¿Están los atributos de seguridad y privacidad alineados con las necesidades y los riesgos de la organización? * ¿Se establece una frecuencia definida para la revisión de los atributos de seguridad y privacidad? * ¿Los atributos de seguridad y privacidad se asocian adecuadamente con sujetos y objetos definidos por la organización? * Revise la documentación para identificar cómo se establece la asociación entre los atributos y los sujetos (usuarios, roles) y objetos (archivos, recursos) dentro de la organización. * ¿Las políticas de seguridad y privacidad establecen claramente la asociación de atributos con sujetos y objetos? * ¿Se realiza un análisis de la efectividad de los atributos en cada revisión? * ¿La organización tiene un método establecido para asociar tipos de atributos de seguridad y privacidad con valores de atributo para la información en almacenamiento, en proceso y/o en transmisión? * Verifique si se han establecido procedimientos o guías internas que describan cómo se realiza la asociación de tipos y valores de atributos. * ¿Se han implementado medidas para garantizar la integridad y precisión de la asociación de tipos y valores de atributos? * ¿Se realiza una revisión periódica de los tipos y valores de atributos de seguridad y privacidad para garantizar su relevancia y adecuación? * ¿Se tiene un proceso establecido para asegurar que las asociaciones de atributos se realicen y conserven adecuadamente con la información?   + Examine los registros o ejemplos de asociaciones de atributos pasadas para verificar si se siguió el proceso y si se registraron de manera adecuada.   + ¿Se han definido los atributos de seguridad y privacidad permitidos basados en los atributos definidos para sistemas o en atributos específicos definidos por la organización?   + ¿Los atributos de seguridad y privacidad permitidos se aplican de manera coherente a la información según su naturaleza y requisitos?   + ¿Se ha proporcionado capacitación y orientación adecuadas al personal sobre cómo establecer y mantener las asociaciones de atributos de seguridad y privacidad?   + ¿Se considera los principales atributos de seguridad y privacidad? Para la evaluación, el auditor debe tener en consideración los siguientes atributos:     - Confidencialidad     - Integridad     - Disponibilidad     - Autenticidad     - No repudio     - Privacidad     - Control de acceso     - Seguridad en tránsito     - Cifrado * ¿La organización ha definido claramente los valores específicos de los atributos o los rangos permitidos para cada uno de los atributos establecidos? * Solicite ejemplos de atributos y sus respectivos valores o rangos permitidos para verificar si están claramente definidos y documentados. * ¿Los valores de atributos definidos por la organización o los rangos establecidos están alineados con las necesidades y requisitos de seguridad de la organización? * Realice entrevistas con los responsables de la definición de atributos para confirmar que los valores o rangos se eligieron considerando las necesidades de seguridad. * ¿Se ha implementado un proceso de aprobación y autorización para la definición de nuevos valores de atributos o rangos permitidos? * ¿Los valores de atributos definidos o los rangos permitidos son comunicados de manera clara a los usuarios y partes interesadas relevantes? * ¿Se establecen asociaciones dinámicas entre atributos de seguridad y privacidad, sujetos y objetos, según las políticas de seguridad y privacidad de la organización?   + ¿Las políticas de seguridad y privacidad que rigen la asociación dinámica de atributos son coherentes con los objetivos y regulaciones de la organización?   + Compare las políticas de seguridad y privacidad con las regulaciones pertinentes (como leyes de privacidad o estándares de seguridad) para verificar la coherencia y el cumplimiento.   + ¿Se sigue un proceso estandarizado y documentado para llevar a cabo la asociación dinámica de atributos de seguridad y privacidad?   + ¿Se documentan y mantienen registros completos de las asociaciones dinámicas de atributos, incluidos los sujetos, objetos y políticas involucradas? * ¿Cuáles son los criterios y requisitos para autorizar a personas o procesos a cambiar los valores de los atributos?   + ¿Se mantiene un registro de las modificaciones realizadas a los valores de los atributos y quién las realizó?   + ¿Se implementan controles de supervisión para asegurarse de que los cambios en los valores de los atributos sean apropiados y legítimos? * ¿La organización tiene un sistema o método para mantener la asociación e integridad de los atributos de seguridad y privacidad entre sujetos y objetos? * ¿Se realiza una revisión periódica de la asociación e integridad de los atributos de seguridad y privacidad para asegurarse de que sigan siendo relevantes y adecuados? * ¿La organización tiene un sistema para asociar atributos de seguridad y privacidad con sujetos y objetos definidos por la organización? * Inspeccione la infraestructura técnica y los sistemas para verificar si existe la capacidad de asociar atributos con sujetos y objetos de manera efectiva. * ¿Los procesos para asociar atributos de seguridad y privacidad con sujetos y objetos son controlados y realizados por personas autorizadas? * Evalúe los registros de auditoría para verificar si las asociaciones de atributos con sujetos y objetos son realizadas por personas con la autorización adecuada. * ¿Se implementa la función de mostrar atributos de seguridad y privacidad en objetos transmitidos a dispositivos de salida? * Observe si la interacción en tiempo real con el sistema para confirmar si los objetos transmitidos a los dispositivos de salida efectivamente muestran atributos de seguridad y privacidad. * ¿Se definen instrucciones especiales de diseminación, manejo o distribución para los objetos transmitidos? * ¿Se utilizan convenciones de nomenclatura estándar legibles por humanos definidas por la organización? * Obtenga muestras de objetos transmitidos y examinar visualmente si los atributos de seguridad y privacidad están presentes y son comprensibles. * ¿Existe un mecanismo establecido para permitir a las personas autorizadas definir o modificar los atributos de seguridad y privacidad asociados con sujetos y objetos? * Analice registros de cambios anteriores en los atributos de seguridad y privacidad para determinar si hay evidencia de que personas autorizadas han realizado modificaciones. * ¿Existen restricciones y controles adecuados para asegurar que solo personas autorizadas puedan realizar cambios en los atributos? * ¿Los cambios en los atributos de seguridad y privacidad son sometidos a aprobaciones y revisiones antes de ser implementados? * ¿Existen procedimientos y directrices establecidos para garantizar la interpretación coherente de los atributos de seguridad y privacidad en el sistema distribuido? * Entreviste a los responsables del diseño y la implementación del sistema distribuido para confirmar si hay procedimientos definidos para mantener la coherencia en la interpretación de los atributos. * ¿Se ha realizado una evaluación de riesgos para identificar posibles brechas en la interpretación de los atributos de seguridad y privacidad en el sistema distribuido? |
| 3.2 Temática: Implementación de nuevas tecnologías, mecanismo y monitoreo de los atributos de seguridad y privacidad |
| En esta práctica se examina cómo la organización evalúa y selecciona nuevas tecnologías. Se verifica si se lleva a cabo un análisis de riesgos para comprender cómo estas tecnologías pueden afectar la seguridad y la privacidad de la información. La organización supervisa continuamente las tecnologías implementadas. Se evalúa si se establecen sistemas de monitoreo y alerta temprana para identificar posibles amenazas o vulnerabilidades.  Al auditar los cambios se evalúa cómo se solicitan, aprueban e implementan las modificaciones. Se busca asegurar que haya un enfoque sistemático y controlado para realizar cambios, minimizando el riesgo de alteraciones no autorizadas.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización ha definido claramente las técnicas y tecnologías que se deben utilizar para asociar atributos de seguridad y privacidad a la información?   + Evalúe si existen registros de decisiones tomadas por la alta dirección o equipos responsables en relación con las técnicas y tecnologías seleccionadas.   + ¿Se están implementando las técnicas y tecnologías definidas de manera efectiva para asociar los atributos de seguridad y privacidad a la información?   + ¿Se dispone de registros que demuestren la implementación exitosa de las técnicas y tecnologías?   + ¿La implementación de las técnicas y tecnologías cumple con los requisitos de seguridad y privacidad establecidos por regulaciones y normativas relevantes? * ¿La organización cuenta con procedimientos y técnicas definidos para el cambio de atributos de seguridad y privacidad?   + Solicite ejemplos de procedimientos y técnicas definidos para el cambio de atributos de seguridad y privacidad y validar su existencia y adecuación.   + ¿Los mecanismos de recalificación son validados antes de realizar cambios en los atributos?   + ¿Se utilizan técnicas o procedimientos específicos definidos por la organización para validar la recalificación de atributos? * ¿Se ha establecido un mecanismo claro para interpretar y comprender los atributos de seguridad y privacidad transmitidos entre los componentes del sistema distribuido?   + ¿Se asegura que los atributos de seguridad y privacidad se mantengan consistentes y no se alteren durante la transmisión entre los componentes del sistema distribuido?   + ¿Existen registros o registros de auditoría que rastreen la transmisión de atributos de seguridad y privacidad entre los componentes del sistema distribuido?   + Verifique si los registros incluyen detalles sobre los atributos transmitidos, los componentes involucrados y las marcas de tiempo correspondientes.   + ¿El equipo técnico comprende cómo se aplican los atributos de seguridad y privacidad en cada etapa del proceso de transmisión? * ¿Se realiza un seguimiento y registro de los cambios en los atributos de seguridad y privacidad?   + Verifique si existe documentación que describa cómo se registran y monitorean los cambios en los atributos de seguridad y privacidad.   + ¿Se lleva a cabo una revisión periódica de los cambios realizados en los atributos?   + ¿Se documentan las justificaciones y aprobaciones para los cambios en los atributos? ¿Se siguen procesos formales para implementar cambios en los atributos?   + ¿Se realiza una evaluación de riesgos antes de realizar cambios en los atributos? |