

**05 - Control de Acceso**

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

**Preguntas de Auditoría**

**Control de Acceso**

|  |
| --- |
| **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 del control de acceso en SIC permite proteger los activos de información y asegurar que los usuarios solo accedan a los recursos necesarios para sus funciones, aplicando métodos de autenticación y autorización de acuerdo con la política de control de acceso. Esto incluye identificar y definir roles funcionales, asignando derechos de acceso basados en estos roles, y restringiendo el acceso a información sensible a aquellos con autorización válida. Para garantizar el cumplimiento, se emplean medidas de control de acceso físico y lógico que incluyen autenticación avanzada y monitoreo de accesos. La gestión de acceso dinámico se aplica a información altamente sensible, permitiendo el control granular y en tiempo real del acceso y el uso de la información, a la vez que se generan registros de auditoría para monitorear el uso y detectar intentos de uso indebido.

**1.1 Procesos y Documentación de Acceso**

El control de acceso también implica un proceso formalizado de aprovisionamiento, que establece la autorización adecuada antes de conceder el acceso. Este proceso incluye un repositorio central de derechos, el cual realiza un seguimiento de los permisos a lo largo del tiempo, facilitando las revisiones de acceso periódicas y la auditoría de los derechos asignados. Asimismo, se requiere que todos los usuarios firmen acuerdos de acceso, incluyendo cláusulas que garanticen el cumplimiento post-empleo de los requisitos de seguridad. Las cuentas y los privilegios se revisan y actualizan regularmente para mantener la seguridad de los activos en todo momento.

**1.2 Rol de la Auditoría en el Control de Acceso en SIC**

La auditoría verifica que los privilegios de acceso estén alineados con los roles y responsabilidades de cada usuario. Las revisiones de control de acceso y los registros de auditoría permiten identificar cualquier uso no autorizado o discrepancia en los permisos asignados, asegurando que los accesos se ajusten a las políticas de seguridad. Los logs generados en el control de acceso se conservan por períodos definidos, cumpliendo con los requisitos regulatorios y brindando evidencia en caso de futuras investigaciones. La auditoría, al revisar y actualizar constantemente los derechos y accesos, refuerza la seguridad y la conformidad con las políticas de control de acceso 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. Identificar las acciones de usuario que se pueden realizar en el sistema sin identificación o autenticación de acuerdo con la misión organizacional y las funciones empresariales. Coordinarse con las unidades de negocio que gestionan la autenticación dentro de las aplicaciones utilizadas en los procesos de negocio, con el fin de asegurar que los controles de autenticación hayan sido administrados adecuadamente.   2. Identificar de forma unívoca y por roles funcionales todas las actividades de procesamiento de información. Coordinarse con las unidades de negocio para asegurarse de que todos los roles están definidos de manera consistente, incluidos los roles definidos por el propio negocio dentro de las aplicaciones de procesos del negocio.  3. Definir y mantener el control de acceso basado en roles, a través de la determinación y documentación de los derechos de acceso necesarios para que cada rol dentro de la empresa lleve a cabo con éxito las tareas asignadas. Considerar lo siguiente para respaldar los requisitos de restricción de acceso:  3.1 No permitir el acceso a información sensible por parte de usuarios con identidades desconocidas o de forma anónima. El acceso público o anónimo solo debe otorgarse a lugares de almacenamiento que no contengan información sensible.  3.2 Proporcionar mecanismos de configuración para controlar el acceso a la información en sistemas, aplicaciones y servicios.  3.3 Controlar a qué datos puede acceder un usuario en particular.  3.4 Controlar qué identidades o grupo de identidades tienen qué acceso, como lectura, escritura, eliminación y ejecución.  3.5 Proporcionar controles de acceso físicos o lógicos para el aislamiento de aplicaciones sensibles, datos de aplicaciones o sistemas.  3.6 Evitar que existan software que se ejecuten con niveles de privilegio más altos que los usuarios que los ejecutan.  3.7 Evitar que los usuarios sin privilegios ejecuten funciones privilegiadas.  2. Verificar que el acceso a la información clasificada que requiera protección especial se otorgue únicamente a las personas que:  2.1 Dispongan de una autorización de acceso válida que se demuestre por los deberes gubernamentales oficiales asignados.  2.2 Satisfacer los criterios de seguridad del personal asociado.  2.3 Haber leído, entendido y firmado un acuerdo de confidencialidad.  4. Considerar las técnicas y procesos de gestión de acceso dinámico para proteger información sensible que tiene un alto valor para la organización cuando la organización:  4.1 Necesita un control granular sobre quién puede acceder a dicha información durante qué período y de qué manera.  4.2 Quiere compartir dicha información con personas ajenas a la organización y mantener el control sobre quién puede acceder a ella.  4.3 Quiere gestionar dinámicamente, en tiempo real, el uso y distribución de dicha información.  4.4 Quiere proteger dicha información contra cambios no autorizados, copia y distribución (incluida la impresión).  4.5 Quiere monitorear el uso de la información.  4.6 Quiere registrar cualquier cambio que se produzca en dicha información en caso de que se requiera una futura investigación.  5. Proteger mediante técnicas de gestión de acceso dinámico la información a lo largo de todo su ciclo de vida (es decir, creación, procesamiento, almacenamiento, transmisión y eliminación), incluyendo:  5.1 Establecer normas sobre la gestión del acceso dinámico basadas en casos de uso específicos que consideren:  5.1.1 Otorgar permisos de acceso basados en la identidad, el dispositivo, la ubicación o la aplicación.  5.1.2 Aprovechar el esquema de clasificación para determinar qué información debe protegerse con técnicas de gestión de acceso dinámico.  6.2 Establecer procesos operativos, de seguimiento y de elaboración de informes e infraestructura técnica de apoyo.  7. Los sistemas de gestión de acceso dinámico deben proteger la información mediante:  7.1 Exigir autenticación, credenciales apropiadas o un certificado para acceder a la información.  7.2 Restringir el acceso, por ejemplo, a un período de tiempo determinado (por ejemplo, después de una fecha dada o hasta una fecha particular).  7.3 Utilizar cifrado para proteger la información.  7.4 Definir los permisos de impresión de la información.  7.5 Registrar quién accede a la información y cómo se utiliza la información.  7.6 Generar alertas si se detectan intentos de mal uso de la información.  8. Centralizar el control de acceso para todos los activos de la empresa a través de un servicio de directorio o un proveedor de SSO, donde sea compatible. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Documentar y garantizar que todos los usuarios (internos, externos y temporales) y su actividad en los sistemas de TI (aplicación de negocio, infraestructura de TI, operaciones, desarrollo y mantenimiento de sistemas) se puedan identificar de manera unívoca.   1.1 Identificar y documentar las funciones de las personas que requieren separación.   2. Documentar y proporcionar una justificación en el plan de seguridad del sistema, las acciones del usuario que no requieran identificación o autenticación.  2.1 El acceso a la información y otros activos asociados debe estar restringido de acuerdo con la política específica establecida sobre el control de acceso.   2.2 Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal intenta acceder sin autorización o hacer uso inapropiado de los privilegios otorgados, ya sea durante casos de rescisión de personal por parte de la organización o durante sus actividades diarias.   3. Desarrollar y documentar acuerdos de acceso a los sistemas de la organización. Requerir a las personas que requieren acceso a la información y los sistemas de la organización:  3.1. Firmar acuerdos de acceso apropiados antes de que se le conceda acceso.  3.2. Volver a firmar los acuerdos de acceso para mantener el acceso a los sistemas de la organización cuando los acuerdos de acceso hayan sido actualizados o con una frecuencia definida por la organización.  3.3 Reconocer que se les notificó a las personas sobre los requisitos post-empleo aplicables y legalmente vinculantes para la protección de la información de la organización.  4. Realizar repositorio de derechos en el sistema que realiza un seguimiento de los privilegios otorgados a los usuarios a lo largo del tiempo y registra las solicitudes de acceso, las aprobaciones, las fechas de inicio y finalización, y los detalles relacionados con el acceso específico que se otorga. Estos datos se pueden usar al auditar el acceso, realizar revisiones de derechos de usuario y determinar si se aprobaron las actividades de acceso.  5. Establecer y mantener un inventario de los sistemas de autenticación y autorización de la empresa, incluidos los alojados en el sitio o en un proveedor de servicios remoto.    6. Establecer y seguir un proceso, preferiblemente automatizado, para:  6.1 Otorgar acceso a los activos de la empresa tras una nueva contratación, concesión de derechos o cambio de rol de un usuario.   6.2 Revocar el acceso a los activos de la empresa, mediante la desactivación de cuentas. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Administrar oportunamente todos los cambios en los derechos de acceso (creación, modificación y eliminación), basándose únicamente en transacciones aprobadas y documentadas que hayan sido autorizadas por personas designadas por la dirección.  2. Realizar revisiones de control de acceso de los activos de la empresa para validar que todos los privilegios estén autorizados, de forma periódica, como mínimo una vez al año, o con mayor frecuencia.  3. Revisar y actualizar el inventario, como mínimo, anualmente o con mayor frecuencia.   4. Revisar y actualizar los acuerdos de acceso con una frecuencia definida por la organización.  5. Llevar a cabo revisiones gerenciales periódicas de todas las cuentas y privilegios relacionados. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Mantener un registro de auditoría del acceso a la información dependiendo de su sensibilidad y de los requisitos regulatorios.  1.1 Los datos generados por el registro deben mantenerse durante un período definido y luego destruirse. |

# Preguntas de Auditoría para el Control de Acceso

|  |
| --- |
| 3.1 Temática: Definición y segregación de roles y responsabilidades en el Control de Acceso |
| En esta dimensión de la auditoría se revisa y evalúa cómo la organización ha establecido y aplicado las funciones y responsabilidades específicas de los usuarios en relación con el acceso a sistemas y recursos. En otras palabras, se trata de verificar si se han definido claramente quiénes tienen acceso a qué, y si se han implementado medidas para prevenir la acumulación excesiva de privilegios en manos de un solo individuo o grupo. Durante este análisis, se examina si la organización ha identificado los roles o funciones que existen en su estructura, así como los niveles de acceso y permisos asociados con cada uno de ellos.  Para ello, el auditor debe considerar lo siguiente:  **3.1.1 Separación de funciones por roles**  Definir las autorizaciones de acceso al sistema para respaldar la separación de funciones. Este levantamiento puede incluir análisis específicos tales como:   * ¿Se han definido roles específicos en el sistema que reflejan las funciones y responsabilidades de los diferentes usuarios? * ¿Existe una política que prohíbe la asignación de permisos que puedan generar conflictos de intereses o comprometer la seguridad de la información? * ¿Se requiere una justificación y aprobación para la asignación de roles y permisos que otorguen acceso a funciones críticas? * ¿Las políticas establecen cómo se deben tratar los cambios en las funciones de los usuarios y cómo se ajustarán sus permisos correspondientes? * ¿Se mantiene un registro o documento que documente los derechos de acceso asignados a cada rol o función en el sistema? * ¿La alta dirección revisa y aprueba los documentos que establecen las políticas y procedimientos?   **3.1.2 Segregación de cuentas**  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización ha implementado políticas y procedimientos para la segregación de cuentas de usuario privilegiadas? * ¿Se ha identificado y documentado qué cuentas de usuario requieren privilegios especiales o de administración en el sistema? * ¿La asignación de privilegios se basa en el principio de mínimo privilegio, otorgando solo los permisos necesarios para llevar a cabo tareas específicas? * ¿La organización tiene mecanismos para gestionar activamente las cuentas de usuario privilegiadas, incluyendo la revisión y eliminación de privilegios no utilizados? * ¿Se utilizan soluciones tecnológicas para registrar y monitorear de manera continua las actividades realizadas en cuentas de usuario privilegiadas? * ¿La organización cuenta con protocolos establecidos para responder ante actividades inusuales o sospechosas detectadas en cuentas privilegiadas?   **3.1.3 Revisión de cambios en los derechos de acceso**  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización tiene un proceso para identificar de manera unívoca todas las actividades de procesamiento de información en el entorno? * ¿Existe una documentación que detalla las actividades de procesamiento de información y los roles funcionales asociados a cada una? * ¿Se requiere una verificación de la identidad de los usuarios antes de otorgarles una identificación única en los sistemas de TI? * ¿La organización mantiene un registro centralizado de las identificaciones únicas asignadas a cada usuario y los sistemas a los que tienen acceso? * ¿Se mantiene un registro actualizado de todos los roles funcionales y las actividades de procesamiento de información asociadas a cada uno? * ¿Existe un proceso establecido para aprobar y documentar las transacciones que autorizan cambios en los derechos de acceso, con roles específicos designados por la dirección para otorgar dichas autorizaciones? * ¿Se mantiene un registro detallado de todas las transacciones? * ¿La organización tiene controles para asegurarse de que los cambios en los derechos de acceso se basen únicamente en transacciones aprobadas y autorizadas por las personas designadas por la dirección? * ¿Se utiliza un proceso de revisión y aprobación para asegurarse de que los cambios en los derechos de acceso sean coherentes con las necesidades operativas y los principios de seguridad? * ¿Existe un mecanismo para detectar y abordar cualquier cambio no autorizado en los derechos de acceso? * ¿La organización realiza revisiones periódicas de todas las cuentas de usuario y privilegios relacionados en los sistemas de TI? ¿Se documentan los resultados de las revisiones gerenciales, incluyendo cualquier cambio o ajuste realizado en cuentas o privilegios? * ¿Las revisiones gerenciales abarcan tanto las cuentas de usuario internas como las cuentas de usuario externas y temporales? |

|  |
| --- |
| 3.2 Temática: Identificación y el Control de Acceso de los activos |
| Auditar que se implementa la identificación y el control de acceso de los activos se refiere a examinar y evaluar cómo una organización maneja la identificación y el acceso a sus recursos digitales, como sistemas, datos y aplicaciones. Esta auditoría implica revisar cómo se implementan los mecanismos de control para garantizar que solo las personas autorizadas puedan acceder a la información o los sistemas correspondientes.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existen políticas y procedimientos claros que describen cómo se lleva a cabo la identificación y el mantenimiento del inventario de sistemas de autenticación y autorización? ¿El inventario incluye tanto los sistemas alojados en el sitio como los proporcionados por proveedores de servicios remotos? ¿Se identifica en el inventario qué sistemas están relacionados con la autenticación y autorización de usuarios y acceso a la información? * ¿La organización tiene políticas y procedimientos establecidos para autenticar todo el acceso a los activos de información según el rol del individuo o las reglas del negocio? * ¿Las normas de control de acceso se basan en una evaluación de los requisitos de la organización y los riesgos asociados con la seguridad de la información con relación a los activos identificados? * ¿La organización tiene un proceso documentado para otorgar acceso a los activos de la organización después de una nueva contratación, concesión de derechos o cambio de rol de un usuario? * ¿Existe un proceso para revisar y actualizar periódicamente las normas de control de acceso en función de los cambios en los requisitos de la organización y las amenazas de seguridad que puedan afectar a los activos identificados? * ¿Se implementan controles técnicos y físicos para hacer cumplir las normas de control de acceso, como sistemas de autenticación, cerraduras electrónicas, tarjetas de acceso, etc. que puedan afectar a los activos identificados? * ¿Existe un sistema o herramienta automatizada preferiblemente para gestionar y agilizar el proceso de desactivación de cuentas en caso de que se tenga que realizar de acuerdo a una alerta de seguridad que pueda afectar a algún activo identificado? |