

**04 - Derechos de Acceso y Acceso Privilegiado**

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

**Preguntas de Auditoría**

**Derechos de Acceso y Acceso Privilegiado**

|  |
| --- |
| **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 derechos de acceso y acceso privilegiado es fundamental para controlar y proteger los sistemas y datos organizacionales, asegurando que los usuarios solo tengan acceso a los recursos necesarios para sus roles específicos. Este proceso implica un control estricto de la asignación de derechos de acceso privilegiado, asegurándose de que solo usuarios con las competencias necesarias y una autorización formal puedan acceder a estos privilegios. Los derechos de acceso privilegiado deben ser monitoreados y revisados regularmente, especialmente después de cambios organizacionales, y se deben emplear identidades individuales en lugar de cuentas genéricas para reducir riesgos. Asimismo, los accesos privilegiados temporales deben concederse únicamente para actividades específicas y de corta duración, registrando todos los accesos y manteniendo un control riguroso mediante tecnologías de gestión de acceso privilegiado.

**1.1 Procesos de Aprovisionamiento y Gestión de Derechos de Acceso**

Para el control efectivo de acceso, se establece un proceso de aprovisionamiento que asegura la autorización adecuada antes de conceder acceso a la información o sistemas. Este proceso considera los requisitos de seguridad y la naturaleza de la información, asegurando que los derechos de acceso se eliminen de manera oportuna cuando ya no sean necesarios, especialmente en casos de finalización de empleo. Se mantiene un registro centralizado de todos los derechos de acceso otorgados y se generan informes que permiten a la organización monitorear el estado de las cuentas y los accesos. Esto incluye detalles sobre los permisos específicos, las aprobaciones de acceso y la administración de cuentas de grupo, apoyando una gestión organizada y controlada de los accesos.

**1.2 Rol de la Auditoría en la Gestión de Derechos de Acceso y Acceso Privilegiado en SIC**

La auditoría desempeña un papel crucial en la validación y control de los derechos de acceso y acceso privilegiado, revisando periódicamente los permisos asignados para asegurar que se ajusten a las necesidades operativas actuales. Esta revisión incluye logs y reportes de excepciones, y considera los cambios en el personal, como ascensos o término de relación laboral, para ajustar o eliminar accesos según sea necesario. Además, la auditoría verifica que todos los accesos privilegiados estén registrados y documentados, y evalúa el cumplimiento de los controles para proteger la información y asegurar que los derechos de acceso continúen alineados con las políticas de seguridad y los objetivos 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. Controlar la asignación de derechos de acceso privilegiado a través de un proceso de autorización de acuerdo con la política de control de acceso específica del tema pertinente. La asignación debe considerar:  1.1 Identificar a los usuarios que necesitan derechos de acceso privilegiado para cada sistema o proceso.  1.2 Asignar derechos de acceso privilegiado a los usuarios según sea necesario y caso por caso de acuerdo con la política específica del tema sobre control de acceso (es decir, solo a personas con la competencia necesaria para llevar a cabo actividades que requieren un acceso privilegiado o con base en el requisito mínimo para sus roles funcionales).  1.3 Mantener un proceso de autorización (es decir, determinar quién puede aprobar derechos de acceso privilegiado o no otorgar derechos de acceso privilegiado hasta que se complete el proceso de autorización) y un registro de todos los privilegios asignados;  1.4 Definir e implementar los requisitos para la expiración de los derechos de acceso privilegiado;  1.5 Tomar medidas para garantizar que los usuarios conozcan sus derechos de acceso privilegiado y cuándo se encuentran en el modo de acceso privilegiado. Las posibles medidas incluyen el uso de identidades de usuario específicas, configuraciones de interfaz de usuario o incluso equipos específicos;  1.6 Los requisitos de autenticación para los derechos de acceso privilegiado pueden ser más altos que los requisitos para los derechos de acceso normales. Puede ser necesario volver a autenticarse o aumentar la autenticación antes de trabajar con derechos de acceso privilegiados;  1.7 Regularmente, y después de cualquier cambio organizacional, revisar a los usuarios que trabajan con derechos de acceso privilegiado para verificar si sus deberes, roles, responsabilidades y competencia aún los califica para trabajar con derechos de acceso privilegiado.  1.8 Establecer normas específicas para evitar el uso de identificaciones de usuario de administración genéricas (como “root”), dependiendo de las capacidades de configuración de los sistemas. Administrar y proteger la información de autenticación de dichas identidades.  1.9 Otorgar acceso privilegiado temporal solo durante el período de tiempo necesario para implementar cambios o actividades aprobados (por ejemplo, para actividades de mantenimiento o algunos cambios críticos), en lugar de otorgar derechos de acceso privilegiado de forma permanente. Esto a menudo se conoce como procedimiento “break glass” y, a menudo, se automatiza mediante tecnologías de gestión de acceso privilegiado;  1.10 Registrar todos los accesos privilegiados a los sistemas con fines de auditoría;  1.11 No compartir o vincular identidades con derechos de acceso privilegiado a múltiples personas, asignando a cada persona una identidad separada que permita asignar derechos de acceso privilegiado específicos. Las identidades se pueden agrupar para simplificar la gestión de los derechos de acceso privilegiado;  1.12 Utilizar únicamente identidades con derechos de acceso privilegiado para realizar tareas administrativas y no para tareas generales del día a día [es decir, revisar el correo electrónico, acceder a la web (los usuarios deben tener una identidad de red normal separada para estas actividades)].  1.13 Autorizar el acceso a la red solo para necesidades operativas convincentes y documentar la justificación de dicho acceso en el plan de seguridad del sistema  1.14 Requerir que los usuarios de cuentas (o roles) del sistema con acceso a funciones de seguridad o información relevante para la seguridad se les asignen cuentas o roles sin privilegios al acceder a funciones que no sean de seguridad. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Crear y documentar el proceso de aprovisionamiento para asignar o revocar los derechos de acceso físico y lógico otorgados a la identidad autenticada de una entidad, esta debe incluir:  1.1 Obtener autorización del propietario de la información y otros activos asociados para el uso de la información y otros activos asociados. La aprobación por separado de los derechos de acceso por parte de la gerencia también puede ser apropiada.  1.2 Considerar los requisitos empresariales y la política y las normas específicas de la organización en materia de control de acceso.   1.3 Considerar si se accede a funciones de seguridad implementadas en hardware, software y firmware  1.4 Considerar si se accede a información relevante para mantener la seguridad de la información de la organización.  1.3 Garantizar que los derechos de acceso se eliminen cuando alguien no necesite acceder a la información y otros activos asociados, en particular garantizar que los derechos de acceso de los usuarios que han dejado la organización se eliminen de manera oportuna.  1.4 Considerar otorgar derechos de acceso temporal por un período de tiempo limitado y revocarlos en la fecha de expiración, en particular para el personal temporal o el acceso temporal requerido por el personal.  1.5 Garantizar que los derechos de acceso se activen (por ejemplo, por parte de los proveedores de servicios) solo después de que se completen con éxito los procedimientos de autorización.  1.6 Mantener un registro central de los derechos de acceso otorgados a un identificador de usuario (ID, lógico o físico) para acceder a la información y otros activos asociados.  1.7 Eliminar o ajustar los derechos de acceso físico y lógico, lo que puede hacerse mediante la eliminación, revocación o reemplazo de claves, información de autenticación, tarjetas de identificación o suscripciones.  1.8 Crear y utilizar diferentes de informes dentro del proceso de aprovisionamiento. Los informes deben incluir:  1.8.1 Listas de identidades y sus accesos asociados.  1.8.2 La persona que aprueba el acceso a información específica.  1.8.3 La gestión de cuentas de grupo y de supervisión.  1.8.4 El número de usuarios que acceden a una determinada aplicación o recurso de información. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Revisar periódicamente los privilegios asignados a roles definidos por la organización o clases de usuarios para validar la necesidad de tales privilegios. Se deben reasignar o eliminar privilegios, si es necesario, para reflejar correctamente la misión organizacional y las necesidades empresariales.  2. Revisar periódicamente las definiciones de control de acceso, los logs y los informes de excepción. Asegurar que todos los privilegios de acceso son válidos y están alineados con los miembros actuales del personal y sus roles asignados.  3. Considerar en las revisiones regulares de los derechos de acceso físico y lógico lo siguiente:   3.1 Los derechos de acceso de los usuarios después de cualquier cambio dentro de la misma organización (por ejemplo, cambio de trabajo, ascenso, descenso) o término de la relación laboral.  3.2 Autorizaciones de derechos de acceso privilegiados.  4. Considerar que los derechos de acceso de un usuario a la información y otros activos asociados deben revisarse y ajustarse o eliminarse antes de cualquier cambio o cese de empleo, basado en la evaluación de factores de riesgo tales como:  4.1 Si el termino o cambio es iniciado por el usuario o por la administración y el motivo del cese.  4.2 Las responsabilidades actuales del usuario.  4.3 El valor de los activos actualmente accesibles. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1.Registrar la ejecución de funciones privilegiadas. |

# Preguntas de Auditoría para los Derechos de Acceso y Acceso Privilegiado

|  |
| --- |
| 3.1 Temática: Gestión de Acceso Privilegiado |
| La gestión de acceso privilegiado se ocupa de las cuentas, personas o sistemas que tienen derechos elevados para acceder a controlar o administrar partes críticas de una organización, como sistemas, datos y configuraciones de red. La relevancia de esta categoría radica en que los usuarios con acceso privilegiado pueden realizar cambios fundamentales en la infraestructura, por lo que un acceso indebido puede provocar graves daños. Ciertos requisitos de cumplimiento requieren controles estrictos sobre quién tiene acceso privilegiado y cómo se maneja ese acceso. El seguimiento y registro de actividades privilegiadas es crucial para detectar y responder a posibles violaciones de seguridad, y el auditor podrá comprobar si la organización gestiona el acceso privilegiado.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existe una política documentada de control de acceso privilegiado? * ¿Se prohíbe compartir de identidades con acceso privilegiado? * ¿Cómo se identifican y registran los usuarios con acceso privilegiado? * ¿Existe un proceso formal de autorización para otorgar derechos de acceso privilegiado? * ¿Se revisan periódicamente las asignaciones de acceso privilegiado? * ¿Se registran todos los accesos privilegiados? * ¿Hay mecanismos implementados para garantizar que los usuarios estén al tanto cuando operen con acceso privilegiado? * ¿Se requiere una autenticación más robusta para acceder con privilegios elevados? * ¿Se prohíben las cuentas genéricas de administración (como "root")? * ¿Cómo se maneja el acceso privilegiado temporal? * ¿Se autoriza el acceso a la red basado en justificaciones operativas convincentes documentadas? * ¿La organización implementa sistemas tecnológicos para la gestión del acceso privilegiado? Para la evaluación, el auditor debe tener en consideración las siguientes herramientas:   1. CyberArk  2. Thycotic  3. StrongDM  4. Centrify |

|  |
| --- |
| **3.2 Temática: Proceso de Aprovisionamiento de Acceso** |
| El proceso de aprovisionamiento de acceso se refiere a cómo se asignan y revocan los derechos de acceso a los usuarios. Este proceso ayuda a asegurar que solo las personas adecuadas tengan acceso a los recursos adecuados en el momento adecuado.  Es deseable que esta actividad sea automatizada y documentada, ya que de esta forma se reduce la carga administrativa y mejoran la eficiencia. La revocación oportuna de derechos evita el acceso no autorizado, especialmente en casos de empleados que dejan la organización.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Está documentado el proceso de aprovisionamiento? * ¿El proceso considera obtener autorización formal antes de otorgar derechos de acceso? ¿Esta autorización se encuentra documentada correctamente, de tal forma que se asegure su trazabilidad y autenticidad? * ¿Cómo se garantiza la eliminación oportuna de derechos de acceso para empleados que abandonan la organización? * ¿Existen mecanismos para otorgar acceso temporal y garantizar su revocación oportuna? * ¿Hay un registro centralizado de derechos de acceso? * ¿Existen informes relacionados con el proceso de aprovisionamiento? Si es así, ¿cuáles son y con qué frecuencia se generan? |

|  |
| --- |
| **3.3 Temática: Segregación de Funciones, el Principio de Menor Privilegio y la Revisión de los Privilegios de Acceso** |
| La revisión regular de los derechos de acceso y los privilegios garantiza que se mantenga el principio de "menor privilegio". Con esto, se busca garantizar que el acceso esté alineado con los roles actuales del personal y evita el acceso excesivo. La detección y corrección oportuna de problemas de acceso puede prevenir o minimizar posibles brechas de seguridad. Este levantamiento puede incluir análisis específicos tales como:   * ¿Con qué frecuencia se revisan los privilegios asignados a los roles o clases de usuarios? * ¿Esta frecuencia se encuentra de acuerdo con lo establecido en las políticas y procedimientos de seguridad de la organización? * ¿Se revisan regularmente las definiciones de control de acceso y los registros relacionados? * ¿Cómo se asegura que los privilegios de acceso estén alineados con los roles actuales del personal? * Revise si existe una matriz de segregación de funciones. * Revise que la matriz se encuentra alineada con las funciones y descripciones de cargo. * Revise que las áreas de riesgo determinadas por la matriz efectivamente se consideran en el diseño de los procedimientos de operación diarios. * Revise que, donde no sea posible separar las funciones, existan controles compensatorios tales como la supervisión y auditoría continua a través de terceras partes. * En las revisiones regulares, ¿se consideran los cambios internos de la organización y las autorizaciones de acceso privilegiado? |

|  |
| --- |
| 3.4 Temática: Revisión de los Privilegios Previo a Cambios |
| Esta categoría se refiere a la revisión de los derechos de acceso antes de cambios significativos como promociones, transferencias o terminación del empleo. Es relevante porque asegura que el acceso no necesario se revoca o ajusta, minimizando el riesgo de acceso inapropiado (Prevención de Acceso Residual). La evaluación basada en factores de riesgo permite una toma de decisiones más informada y efectiva sobre el acceso.  Tener implementado estas actividades facilita una transición fluida durante los cambios en la organización, garantizando que los empleados tengan el acceso adecuado según sus nuevos roles.  Este levantamiento puede incluir análisis específicos tales como:   * Antes de cualquier cambio organizacional, ¿se revisan y ajustan los derechos de acceso de un usuario? * Si la respuesta es sí, verifique que esto se encuentra reflejado y documentado en los procesos organizacionales. * Verifique que existen registros que sirvan como respaldo para la pregunta anterior. * ¿Se consideran factores de riesgo como el motivo del cese o cambio, las responsabilidades actuales y el valor de los activos accesibles al evaluar el acceso previo a un cambio o terminación de funciones? |