Pantalla de computadora con imágen de hombre

Descripción generada automáticamente con confianza media

**03 - Cuentas**

**y**

**Credenciales**

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

**Preguntas de Auditoría**

**Cuentas y Credenciales**

|  |
| --- |
| **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 cuentas y credenciales en la función de seguridad de la información y ciberseguridad (SIC) permite proteger los activos organizacionales, logrando así una asignación controlada y revisable de derechos de acceso privilegiado. Esto incluye identificar a los usuarios que necesitan derechos específicos para cada sistema o proceso, asignando privilegios caso por caso y de acuerdo con políticas de control de acceso. Las medidas de seguridad incluyen también la asignación de cuentas individuales para evitar el uso de identificaciones genéricas, la autorización de acceso privilegiado solo para funciones administrativas y el uso de autenticación avanzada. Este enfoque minimiza el acceso no autorizado y facilita la gestión de privilegios temporales, asegurando que los derechos de acceso se otorguen solo por el tiempo necesario, bajo un procedimiento formal y documentado.

**1.1 Procesos de Aprovisionamiento y Control de Acceso**

Para formalizar y gestionar los derechos de acceso, se implementa un proceso de aprovisionamiento que requiere la autorización de los propietarios de información y la gerencia para el uso de recursos específicos. El proceso de aprovisionamiento incluye el mantenimiento de un registro central de los derechos de acceso y la eliminación de dichos derechos cuando ya no son necesarios. Además, se habilitan informes de auditoría y control que detallan las identidades y sus permisos, las aprobaciones de acceso y el seguimiento de cuentas compartidas o de grupo, así como el número de usuarios por aplicación o recurso. Este sistema permite una administración precisa y ágil de los derechos de acceso físico y lógico, con controles regulares para verificar que los derechos asignados se ajusten a las necesidades operativas.

**1.2 Rol de la Auditoría en la Gestión de Cuentas y Credenciales en SIC**

La auditoría en SIC juega un rol esencial en la validación y monitoreo continuo de los privilegios de acceso y las credenciales asignadas. Las auditorías incluyen revisiones periódicas de los privilegios, control de accesos, y revisiones de logs y reportes de excepción para asegurar que los derechos se alineen con las necesidades actuales de la organización. Además, los privilegios se revisan al ocurrir cambios en la estructura organizativa o al finalizar relaciones laborales, con un enfoque en el riesgo y el valor de los activos accesibles. La auditoría documenta las actividades de acceso privilegiado y evalúa continuamente los procesos de gestión de credenciales para identificar y corregir áreas de mejora, garantizando que las prácticas de acceso sean seguras, eficientes y adaptativas a las dinámicas organizativas.

# 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 Cuentas y Credenciales

|  |
| --- |
| 3.1 Temática: Proceso del ciclo de vida de las cuentas |
| Evaluar el proceso de las cuentas implica una revisión exhaustiva de cada fase que involucra la gestión de cuentas de usuario, desde la creación hasta la eliminación. Se busca identificar riesgos, evaluar la efectividad de los controles y garantizar que las políticas y procedimientos estén en línea con los objetivos de seguridad y cumplimiento de la organización. Al fortalecer estos procesos, la organización se protege contra amenazas y vulnerabilidades, y asegura la integridad de sus sistemas y datos.   |  | | --- | | Es importante recordar que también hay cuentas de servicio, identidades de máquinas y otras identidades no humanas que deben administrarse. Complemente este control del Dominio Gestión de Personas cuando sea necesario. |   Para la evaluación, el auditor debe tener en consideración:  **3.1.1 Inventario y control de cuentas.**  Se enfoca en revisar detalladamente los procedimientos y controles implementados para gestionar el acceso a sistemas, aplicaciones y recursos, así como para mantener un inventario preciso de las cuentas y credenciales de los usuarios. El objetivo es prevenir accesos no autorizados, minimizar riesgos y asegurar el cumplimiento de las políticas de seguridad.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se realiza un inventario de las cuentas otorgadas en la organización? * ¿Cómo se asegura de que el inventario de cuentas sea conciliado con las cuentas activas en sistemas y aplicaciones? * ¿El proceso de recopilación del inventario garantiza que las nuevas cuentas sean recopiladas adecuadamente y a tiempo? * ¿El inventario esta actualizado con las cuentas y credenciales de usuario en uso? * ¿Cuál es la Frecuencia de las revisiones del inventario? * Compruebe que la frecuencia de revisión es la indicada en los modelos de control definidos por la organización. * ¿Los privilegios de administración están limitados adecuadamente y la organización dispone de un inventario de cuentas de administración que facilita su correcto control? * ¿La organización ha definido claramente los tipos de cuentas que están permitidos y prohibidos dentro del sistema? * ¿Existe un proceso formal para otorgar autorización de acceso a las cuentas dentro del sistema? * Compare las funciones y responsabilidades de los usuarios con los privilegios de acceso asignados para confirmar que sean coherentes y adecuados. * ¿Existen controles para evitar que los usuarios accedan a áreas o funciones del sistema que no están relacionadas con su uso previsto? * ¿Existe un registro de las cuentas deshabilitadas cuando los criterios necesarios se alcanzan? * ¿El registro considera el tiempo del evento que desencadena la expiración y la fecha real de expiración en los sistemas? * Asegúrese de que todas las cuentas tengan una fecha de vencimiento monitoreada y forzada. * ¿La organización tiene un proceso establecido para deshabilitar automáticamente las cuentas que han expirado? ¿Se consideran las cuentas las temporales o de emergencia? * Revise los registros que demuestren que las cuentas expiradas son automáticamente deshabilitadas en el sistema dentro de un período establecido. * ¿Se deshabilitan las cuentas que violan la política de la organización en cuanto a seguridad y acceso? * ¿La organización tiene un período de inactividad definido después del cual las cuentas son deshabilitadas? * Verifique los intentos de acceso a cuentas desactivadas a través de los registros de auditoría. * ¿Existe un mecanismo para detectar y reportar el uso atípico de las cuentas del sistema a los roles o personal definidos por la organización? * ¿Se alerta a los usuarios si se desvían del comportamiento normal de inicio de sesión, como la hora y/o el día, la ubicación de la estación de trabajo y la duración? * ¿Se lleva a cabo una revisión regular de las cuentas de usuario para asegurarse de que cumplan con los requisitos de administración de cuentas? * Revise registros de cuentas que demuestren la frecuencia y consistencia de las revisiones realizadas. * ¿Hay procedimientos establecidos para inhabilitar cuentas de personas en caso de descubrimiento de riesgos significativos que puedan afectar a la organización? * ¿Se lleva un seguimiento de las cuentas inhabilitadas para asegurarse de que las acciones correctivas se hayan implementado correctamente? * ¿Las revisiones de cuentas incluyen la verificación de que los privilegios y accesos asignados a cada cuenta son apropiados y necesarios?   **3.1.2 Procedimiento de ciclo de vida de cuentas y credenciales.**  Este proceso abarca todas las etapas desde la creación inicial de cuentas hasta su desactivación final, asegurando que los usuarios tengan el acceso apropiado durante su tiempo en la organización y que este acceso se revoque de manera segura cuando ya no sea necesario. Auditar y rotar las credenciales periódicamente para limitar el tiempo que pueden utilizarse para acceder a sus recursos.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existe un procedimiento documentado para solicitar la creación, eliminación o cambio de identidad de usuario? * ¿El procedimiento establece claramente cómo deben realizarse las solicitudes para los diferentes tipos de identidades (manual, electrónica, mesa de ayuda)? * ¿Las instrucciones son claras sobre cómo realizar las solicitudes según el tipo de identidad, y si incluye ejemplos o instrucciones paso a paso? * Revise la documentación del procedimiento de gestión de cuentas de administración (ej. construcción del identificador de usuario, distribución de la contraseña/credencial, plazos específicos para la realización de solicitudes, expectativas de cumplimiento y dónde deben enrutarse las solicitudes, etc.).   + Mantenga un registro de auditoría detallado de las acciones críticas de Gestión de usuarios, que incluyen crear, eliminar, mover, renombrar y más, junto con detalles sobre quién hizo qué, cuándo y desde dónde. * ¿El procedimiento define plazos específicos para la realización de las solicitudes? * ¿Se establecen direcciones claras sobre dónde deben enrutarse las solicitudes? * ¿Existe un mecanismo establecido para recibir y enviar comunicaciones sobre la creación, eliminación o cambios en las identidades de usuario? * Verifique la utilización de mensajes automatizados, mensajes verbales o documentos impresos en relación a la gestión de identidades. * Verifique que todos los nombres de usuario y las credenciales de autenticación de la cuenta se transmitan a través de redes que utilizan canales cifrados. * ¿Las cuentas de usuario se crean de acuerdo con las políticas y procedimientos establecidos? * Revise registros de auditoría que demuestren que se siguen los criterios y procedimientos al habilitar cuentas. * Los siguientes elementos deben tenerse en cuenta al crear la identidad: * La función del solicitante dentro de la organización. * Cómo se utilizará la identidad. * Si el acceso otorgado al propietario de la identidad se basará en roles, reglas o necesidades específicas del usuario. * Si la identidad se puede replicar a partir de un rol existente o será necesario crear un nuevo rol para satisfacer las necesidades del usuario * Compruebe que la organización realiza una lista de verificación de seguridad que se complete antes de habilitar una cuenta. Esto incluye asignar los permisos mínimos necesarios y garantizar que se configuren las contraseñas de manera segura. * Verifique que las cuentas de usuario antiguas y no utilizadas permanezcan deshabilitadas al monitorear cada vez que se habilita una cuenta de usuario para verificar su necesidad. * ¿Qué procedimientos se siguen para modificar cuentas de usuario existentes, como cambios en roles o privilegios? * Verifique si se completa un formulario de solicitud de cambio que incluye detalles específicos del cambio. Evalúe como se realiza la revisión y como se procede a aplicar el cambio siguiendo los procedimientos establecidos. * ¿Cómo se maneja la deshabilitación y eliminación de cuentas de usuario cuando un empleado deja la organización? * ¿Cuál es el mecanismo automatizado utilizado por la organización para gestionar cuentas del sistema y registrar las acciones de creación, modificación, habilitación, deshabilitación y eliminación de cuentas? * Verifique las soluciones IAM que tienen la organización. Deberían automatizar el inicio, la captura, el registro y la gestión de las identidades de los usuarios y sus permisos de acceso correspondientes. Los productos deben incluir un servicio de directorio centralizado que escala conforme la organización crece. * Evalúe el mecanismo de establecimiento de diferentes procesos de revisión de nivel apropiado de riesgo para el acceso de nivel superior, así como una revisión de los derechos existentes para prevenir el arrastre de privilegios. * ¿Cómo se aseguran de que las acciones automatizadas de gestión de cuentas sean revisadas y aprobadas antes de su implementación? * Verifique si los requerimientos relacionados con cuentas a las aplicaciones y sistemas de información se realiza de forma manual. Compruebe si existe un responsable de esta tarea, por ejemplo: Grupo de Gestión de Cuentas de la Gerencia de TI. * ¿Existe un proceso para alinear los procesos de administración de cuentas con los procesos de despido y transferencia de personal? * ¿Existe un procedimiento de terminación para garantizar que las credenciales se revoquen o cambien cuando un empleado se va? * Verifique las cuentas para garantizar que el acceso del usuario se revoque después de la terminación y que las cuentas se eliminen de acuerdo con las políticas. * ¿Existe un proceso automatizado para revocar el acceso a sistemas mediante la desactivación de cuentas inmediatamente después de la terminación o el cambio de responsabilidades de un empleado o contratista? * ¿La organización tiene establecido un período de tiempo definido para la inactividad después del cual los usuarios deben cerrar sesión de manera automática? * Revise la configuración de seguridad de sistemas y aplicaciones clave para verificar si existe una configuración de cierre de sesión automático y cómo está definido. * ¿La organización bloquea automáticamente las sesiones de la estación de trabajo después de un período estándar de inactividad? * ¿Se detecta y diagnostica rápidamente el motivo de los bloqueos de cuentas? * Verifique las credenciales obsoletas, sesiones de escritorio remoto interrumpidas y asignaciones de unidades defectuosas.   **3.1.3 Contraseñas de cuentas.**  Esta auditoría se centra en revisar y evaluar la robustez, efectividad y cumplimiento de las políticas y prácticas relacionadas con la creación, gestión y almacenamiento de contraseñas utilizadas para acceder a sistemas y recursos.  Después de crear una identidad, generalmente se asigna una contraseña inicial. Esta contraseña inicial puede generarse de forma manual o electrónica y es comunicada al usuario por el departamento de TI, se debe considerar la emisión y el mantenimiento de las contraseñas de los usuarios. Los parámetros, las estructuras y el uso adecuado de las contraseñas deben detallarse en la política de seguridad de la organización. El mantenimiento de las contraseñas de los usuarios es un componente vital de un proceso IAM eficaz.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización requiere que se otorgue una contraseña temporal a los usuarios al asignarles una nueva identidad? * ¿La contraseña temporal es cambiada por el usuario durante el intento inicial de inicio de sesión? * ¿Se utilizan métodos seguros para transferir la contraseña temporal a los usuarios como correos electrónicos? * Verifique mediante registros que los usuarios cambien su contraseña temporal en su primer inicio de sesión. * ¿Los parámetros de contraseña cumplen con la política de la organización y/o los requisitos aplicables de la industria? * Verifique la Longitud, complejidad, requisitos de cambio, historia. * Utilice pruebas de fuerza bruta y ataques de diccionarios combinados para comprobar la fortaleza y configuración de las contraseñas. * ¿Se suprimen las contraseñas de todos los resultados de los campos de búsqueda de los sistemas de información? * ¿Los archivos de contraseña están encriptados y restringidos? * ¿La organización localiza las cuentas de usuario que son vulnerables porque sus contraseñas están configuradas para no caducar nunca? * Verifique que se aplica una política de caducidad de contraseña segura para evitar el robo de credenciales. * Verifique si la herramienta de gestión de credenciales realiza esta tarea de forma automática y programable, permitiendo que las claves se cambien más a menudo de lo que es común en las instalaciones de sistemas de control habituales. * Evalúe los cambios y restablecimientos de contraseña más recientes realizados por los usuarios, y obtenga información instantánea sobre los usuarios que cambian sus contraseñas con frecuencia.   **3.1.4 Administración de las cuentas del estado privilegiado.**  Evaluar este punto implica una revisión crítica y exhaustiva de cómo una organización maneja y controla las cuentas con privilegios elevados. Estas cuentas, a menudo denominadas cuentas con privilegios administrativos o de superusuario, tienen acceso amplio y significativo a sistemas, aplicaciones y datos, lo que las convierte en objetivos críticos en términos de seguridad y gestión de riesgos. A pesar de tener acceso ilimitado a los servidores y a los datos, la actividad de los usuarios privilegiados a menudo pasa desapercibida.  Las cuentas de usuarios privilegiados tienen acceso sin restricciones a todos los servidores, aplicaciones y bases de datos críticos incluidos los permisos para crear o eliminar perfiles de usuario y administrar los privilegios de los usuarios. Esto plantea un importante desafío de seguridad para una organización, porque cuando las cuentas de usuario con privilegios se ven comprometidas, pueden causar daños irreparables a la organización.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización tiene un procedimiento para identificar usuarios privilegiados? * Verifique si los roles de los usuarios privilegiados están bien definidos y si los usuarios privilegiados están capacitados de acuerdo con sus responsabilidades. * ¿Existe políticas y procedimientos para la creación y gestión de cuentas privilegiadas, identificando el proceso y los pasos involucrados? * ¿Cómo se monitorean las asignaciones de roles o atributos privilegiados? * Revise los registros de auditoría y los informes generados por herramientas de monitoreo para verificar que se realice un seguimiento regular. * Los accesos realizados con cuentas de usuario privilegiados deben ser registrados y controlados periódicamente. * Revise el material de capacitación y/o acuerdos de usuario para asegurar que a los usuarios con altos privilegios se les ha enseñado sobre los roles y responsabilidades de seguridad asociados a altos privilegios * ¿Existe un proceso de supervisión de cambios en las funciones o atributos privilegiados? * ¿Cómo se lleva a cabo el proceso de revocación de acceso a funciones o atributos privilegiados?   **3.1.5 Asignación y funciones de los gestores de cuentas.**  La auditoría se enfoca en revisar cómo se designa a los gestores de cuentas, cómo se monitorean sus actividades y si se establecen controles adecuados para evitar riesgos como acceso indebido o abuso de privilegios.  Los gestores de cuentas, como administradores de sistemas, supervisores de TI o roles similares, tienen la responsabilidad de gestionar y supervisar el acceso a sistemas, aplicaciones y recursos críticos. Por lo tanto, es esencial que estas asignaciones se realicen de manera adecuada y que las funciones de los gestores se alineen con las necesidades de seguridad y operacionales de la organización.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La asignación de gestores de cuenta se realiza de acuerdo con una política establecida? * ¿Existe un proceso formal para designar a los gestores de cuenta? * ¿Los gestores de cuenta son responsables de aprobar o revisar las solicitudes de acceso a recursos y sistemas? * Examine las credenciales y privilegios de los gestores de cuenta para asegurarse de que tengan los permisos apropiados y que exista un registro de cambios realizados. * ¿Los gestores de cuenta están capacitados en el manejo adecuado de solicitudes de acceso y asignación de privilegios? * Revise los registros de capacitación o evidencia de programas de formación. * Entreviste a gestores de cuenta seleccionados y verificar si están conscientes de sus responsabilidades y si han aprobado o revisado solicitudes recientes. * ¿Existe un procedimiento establecido para notificar a los gestores de cuenta y al personal correspondiente cuando ya no se requieran las cuentas? * Solicite ejemplos de notificaciones de recientes casos en los que se dieron de baja o se transfirieron usuarios, y verificar si las notificaciones fueron enviadas a los gestores apropiados y al personal correspondiente. * ¿La organización tiene un mecanismo para notificar a los gestores de cuenta y al personal cuando el uso del sistema o la necesidad de saber cambia para un individuo? * Revise si se han registrado casos recientes de cambios y si se notificaron adecuadamente a los gestores y al personal relevante. * Verifique que las notificaciones se realicen dentro de los plazos establecidos y que las acciones necesarias se lleven a cabo después de las notificaciones, como la eliminación de cuentas o la modificación de privilegios. * ¿Se requiere la aprobación de un personal autorizado antes de crear nuevas cuentas personales y compartidas o grupales? * Revise las solicitudes de creación de cuentas para verificar si existen evidencias claras de aprobación por parte de personal con la autoridad correspondiente, como un supervisor o un administrador de TI. * Revise las solicitudes de creación de cuentas para asegurarse de que cada solicitud tenga una sección o campo donde se indique quién dio la aprobación. * ¿Las aprobaciones se basan en criterios predefinidos y apropiados, como la necesidad de acceso para llevar a cabo funciones laborales específicas?   **3.1.6 Cuentas grupales o compartidas.**  Las cuentas grupales o compartidas son una herramienta común para facilitar el acceso a recursos en sistemas y aplicaciones, pero su uso inadecuado puede aumentar los riesgos de seguridad. Esta auditoría se enfoca en examinar cómo se crean, administran y controlan estas cuentas, así como en verificar si se siguen las mejores prácticas para mitigar riesgos.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización tiene un proceso establecido para solicitar nuevas cuentas compartidas/grupales? * ¿Se requiere la aprobación de personal autorizado antes de crear nuevas cuentas? * ¿Qué criterios se utilizan para determinar qué cuentas requieren aprobación antes de su creación? * ¿Se definen claramente los grupos y roles en la organización, y se documenta su propósito y responsabilidades? * Revise si la documentación de la organización que describe la estructura de grupos y roles, y verificar si esta información es clara y comprensible. * ¿La membresía de los grupos y roles está basada en las necesidades funcionales y de seguridad de cada usuario? * Examine la membresía de cada usuario en grupos y roles para asegurarse de que esté respaldada por las funciones laborales y requisitos de seguridad. * ¿La organización tiene un proceso establecido para asignar y retirar a los usuarios de grupos y roles? * ¿Se establecen claramente los privilegios y atributos de acceso para cada cuenta de usuario según las necesidades de la organización? * ¿Se implementan controles para evitar que las cuentas de usuario tengan privilegios o atributos excesivos o innecesarios? * ¿La organización tiene un proceso documentado para cambiar los autenticadores de cuentas grupales o compartidas cuando se elimina a una persona del grupo? * Verifique si hay instrucciones explícitas para cambiar los autenticadores en caso de eliminación de usuarios. * Seleccione una muestra de casos donde se haya eliminado a personas del grupo con cuentas compartidas y verifique si se siguió el proceso de cambio de autenticadores para cada caso. * ¿El proceso de cambio de autenticadores se lleva a cabo en un plazo razonable después de que alguien es eliminado del grupo? * ¿Se realizan revisiones periódicas para verificar la autorización de las cuentas personales, grupales y de servicio activas? * Verifique que se documenten las fechas de las revisiones y las acciones tomadas en caso de encontrar cuentas no autorizadas. * Solicite acceso a los registros de cuentas activas, incluyendo información sobre quién autorizó la creación de la cuenta y qué permisos se han asignado. * Verifique la precisión y actualización de estos registros. |