

**08 – Uso de Programas de Utilidad y Controles de Aplicaciones**

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

**Preguntas de Auditoría**

**Uso de Programas de Utilidad y Control de Aplicaciones**

|  |
| --- |
| **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

El control sobre los programas de utilidad en SIC busca mitigar los riesgos asociados a su capacidad de anular controles de seguridad, limitando su uso a personal autorizado y confiable. Estos programas, que a menudo tienen altos niveles de acceso, requieren medidas como la identificación y autenticación única de los usuarios, la documentación de niveles de autorización y restricciones de uso en situaciones específicas. Las organizaciones eliminan o desactivan programas de utilidad innecesarios, asegurando una separación lógica de estos respecto al software de aplicación y limitando su disponibilidad para proteger la integridad de los sistemas de información.

**1.1 Medidas de Control sobre Programas de Utilidad**

Para evitar conflictos de segregación de funciones y riesgos de acceso no autorizado, los programas de utilidad están reservados exclusivamente para un número restringido de usuarios y cuentan con controles de registro de uso. También se limita la disponibilidad de dichos programas a las duraciones necesarias, minimizando así el tiempo y el alcance de su uso. Estas medidas se complementan con la separación lógica y, en algunos casos, la segregación de comunicaciones de red para mantener la integridad de los sistemas de aplicaciones.

**1.2 Evaluación desde la Auditoría en el Uso de Programas de Utilidad**

La auditoría en SIC verifica la efectividad de estos controles, revisando registros de uso y cumplimiento de las pautas de autenticación, autorización y segregación lógica. Esta evaluación se centra en la validación de prácticas que aseguran que los programas de utilidad se utilicen de manera segura y solo por personas autorizadas, manteniendo la separación de funciones y la protección de la infraestructura crítica 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 los programas de utilidad que puedan anular los controles del sistema y de las aplicaciones |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 2. Considerar las siguientes pautas para el uso de programas de utilidad que pueden anular los controles del sistema y de aplicación:  2.1 Limitación del uso de programas de utilidad al número mínimo práctico de usuarios autorizados de confianza;  2.2 Uso de procedimientos de identificación, autenticación y autorización para programas de utilidad, incluida la identificación única de la persona que usa el programa de utilidad;  2.3 Definición y documentación de niveles de autorización para programas de utilidad;  2.4 Autorización para uso ad hoc de programas de utilidad;  2.5 No poner programas de utilidad a disposición de los usuarios que tienen acceso a aplicaciones en sistemas donde se requiere segregación de funciones;  2.6 Eliminar o deshabilitar todos los programas de utilidad innecesarios;  2.7 Como mínimo, separación lógica de los programas de utilidad del software de aplicación. Cuando sea práctico, segregar las comunicaciones de red para dichos programas del tráfico de aplicaciones;  2.8 Limitación de la disponibilidad de los programas de utilidad (por ejemplo, durante la duración de un cambio autorizado);  2.9 Registro de todos los usos de los programas de utilidad. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. |  |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles |  |
| NIVEL 5 [Optimizado]: La organización se centra en la mejora continua y está diseñada para girar y responder a las oportunidades y los cambios. |  |

# Preguntas de Auditoría para el Uso de Programas de Utilidad y Controles de Aplicaciones

|  |
| --- |
| 3.1 Temática: Autorización y control de acceso del personal a los Programas de Utilidad |
| En este control se lleva a cabo una revisión detallada y sistemática de cómo se han establecido y aplicado las políticas y procedimientos que determinan quién tiene permiso para acceder y utilizar estos programas, así como cómo se controla dicho acceso. Esto implica analizar las medidas de seguridad implementadas para asegurarse de que solo el personal autorizado y confiable tenga la capacidad de utilizar estos programas y que se cumplan los niveles adecuados de seguridad.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se ha verificado que solo los usuarios autorizados y de confianza tienen acceso a los programas de utilidad? * ¿Se ha revisado la lista de usuarios con acceso a programas de utilidad y se ha comparado con una lista de usuarios autorizados? * ¿Los usuarios con acceso a programas de utilidad están restringidos a un número mínimo práctico de usuarios autorizados de confianza? * ¿Se ha verificado que los programas de utilidad requieren identificación, autenticación y autorización antes de su uso? * ¿Se ha revisado la documentación y los procedimientos de acceso a programas de utilidad para verificar si se mencionan los requisitos de identificación y autenticación? * ¿Se están utilizando procedimientos de identificación, autenticación y autorización para acceder a programas de utilidad, y se registra la identificación única de la persona? * ¿Se ha verificado que se han definido y documentado los niveles de autorización para el uso de programas de utilidad? * ¿Se ha revisado la documentación de políticas de seguridad para programas de utilidad para verificar si se describen claramente los niveles de autorización? * ¿Existen niveles de autorización claramente definidos y documentados para el uso de programas de utilidad? * ¿Se ha verificado si existe un proceso formal para otorgar autorización ad hoc para el uso de programas de utilidad? * ¿Se ha entrevistado al personal de seguridad o se ha revisado la documentación para confirmar si hay un procedimiento establecido para la autorización ad hoc? * ¿Existe un proceso para autorizar de manera controlada el uso ad hoc de programas de utilidad? * ¿Se ha verificado si se prohíbe el acceso a programas de utilidad para usuarios que tienen acceso a aplicaciones que requieren segregación de funciones? * ¿Se ha revisado la lista de usuarios con acceso a programas de utilidad y se ha comparado con los usuarios con acceso a aplicaciones? * ¿Los usuarios con acceso a aplicaciones que requieren segregación de funciones no tienen acceso a programas de utilidad? |

|  |
| --- |
| **3.2 Temática: Independencia y disponibilidad de los Programas de Utilidad** |
| Auditar la independencia y disponibilidad de los programas de utilidad busca examinar detalladamente cómo se asegura que estos programas operen de manera separada y autónoma de otros sistemas y aplicaciones, y cómo se garantiza su disponibilidad y funcionamiento cuando sea necesario. Esta auditoría implica revisar las medidas y los procedimientos implementados para garantizar que los programas de utilidad no interfieran con otras operaciones y que estén disponibles y funcionando correctamente cuando se requieran. Este levantamiento puede incluir análisis específicos tales como:   * ¿Se ha verificado si se han eliminado o deshabilitado los programas de utilidad innecesarios? * ¿Se ha revisado la lista de programas de utilidad para identificar programas que no se utilizan y se ha confirmado si han sido eliminados o deshabilitados? * ¿Se han eliminado o deshabilitado los programas de utilidad que no son necesarios? * ¿Se ha verificado si existe una separación lógica de los programas de utilidad del software de aplicación y si se ha segregado el tráfico de red? * ¿Se ha revisado la arquitectura de red y sistemas para determinar si existe una separación lógica de programas de utilidad y tráfico de aplicaciones? * ¿Los programas de utilidad están separados lógicamente del software de aplicación, y las comunicaciones de red están segregadas cuando es posible? * ¿Se ha verificado si se limita la disponibilidad de los programas de utilidad durante cambios autorizados y si se registran todos los usos de los programas de utilidad? * ¿Se han revisado los registros de cambios autorizados y los registros de uso de programas de utilidad? * ¿Los programas de utilidad solo están disponibles durante cambios autorizados, y todos los usos están registrados? |