

**CASIG 4 - Gestión de Recursos Humanos**

**Preguntas de Auditoría**

**Acceso a Información**

**Competencias Básicas del Auditor**

1. **Conocimiento de las Normas y Regulaciones:** Un auditor debe estar familiarizado con las normas, regulaciones y estándares relevantes en el ámbito de la ciberseguridad (como ISO 27001, CIS, NIST CSF, etc.) y la gestión de personas (estatuto administrativo, normativa interna).
2. **Habilidades Analíticas:** La capacidad de analizar datos, identificar patrones y hacer conexiones entre información aparentemente no relacionada es esencial.
3. **Comunicación Efectiva:** Un auditor debe ser capaz de comunicar sus hallazgos de manera clara y concisa, tanto por escrito como verbalmente.
4. **Conocimiento Técnico:** Es esencial tener un conocimiento profundo de las tecnologías y sistemas que se están auditando. En particular, debe conocer el funcionamiento y arquitectura de los sistemas de apoyo para la gestión de recursos humanos (hrms).
5. **Conocimiento de las Amenazas Actuales:** El panorama de amenazas de ciberseguridad está en constante evolución. En particular, la de gestión de personas requiere un conocimiento en profundidad de las técnicas más comunes, como las de ingeniería social.
6. **Capacidad de Evaluación de Riesgos:** Evaluar y priorizar riesgos es una habilidad clave. Un auditor debe ser capaz de determinar qué áreas presentan el mayor riesgo y recomendar medidas para mitigar esos riesgos.

# Visión General

El acceso a la información dentro de la función de seguridad de la información y ciberseguridad (SIC) se gestiona mediante una designación de riesgo para cada puesto organizacional, lo cual permite establecer criterios de selección adecuados para los titulares de dichos puestos y adaptar sus autorizaciones de acceso de acuerdo con la necesidad operativa. Cuando un individuo termina su relación con la organización, se implementan medidas de seguridad que incluyen la desactivación de su acceso a sistemas, la revocación de autenticadores y credenciales, entrevistas de salida enfocadas en temas de seguridad, y la recuperación de cualquier propiedad relacionada con la seguridad de la organización. En caso de transferencia de personal, se revisan y ajustan las autorizaciones de acceso según los nuevos requisitos operativos, garantizando que el personal implicado esté debidamente informado sobre el proceso.

**1.1 Acuerdos de Acceso y Procedimientos de Revisión**

Para formalizar y asegurar el acceso adecuado a los sistemas organizacionales, se desarrollan y documentan acuerdos de acceso que deben ser revisados y actualizados regularmente. Los individuos que necesitan acceso a los sistemas y la información deben firmar estos acuerdos, y en caso de actualización de los términos, se les pide una nueva firma de conformidad. Además, la organización revisa y actualiza las designaciones de riesgo de los puestos de manera frecuente para autorizar y ajustar los accesos, reevaluando a las personas según las condiciones establecidas para garantizar que las autorizaciones estén en línea con la estructura y políticas de seguridad de la organización.

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

Desde la perspectiva de auditoría, el control de acceso a la información en SIC se verifica mediante la recopilación de datos sobre el cumplimiento de los acuerdos de acceso, permitiendo identificar áreas de mejora y adoptar medidas correctivas. Las lecciones aprendidas del cumplimiento de estos acuerdos se integran en los procesos y procedimientos, fortaleciendo las políticas de acceso y asegurando que todos los controles se adapten continuamente a las necesidades de la organización. La auditoría supervisa también que se realicen reevaluaciones periódicas y se ajusten las designaciones de riesgo, promoviendo una mejora constante en la gestión de acceso a la información y un cumplimiento óptimo de los requisitos de seguridad.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Asignar una designación de riesgo a todos los puestos organizacionales.  2. Establecer criterios de selección para las personas que ocupan esos puestos.  3. Incluir las siguientes medidas de seguridad de la información al momento de terminar con las funciones del personal:  3.1 Deshabilitar el acceso al sistema.  3.2 Terminar o revocar cualquier autenticador y credencial asociado con el individuo.  3.3 Llevar a cabo entrevistas de salida que incluyan una discusión sobre temas de seguridad de la información.  3.4 Recuperar toda la propiedad relacionada con el sistema organizacional relacionada con la seguridad.  3.5 Conservar el acceso a la información y los sistemas de la organización anteriormente controlados por el individuo despedido.  4.Incluir las siguientes medidas de seguridad de la información al momento de transferir al personal:  4.1 Revisar y confirmar la necesidad operativa actual de autorizaciones de acceso lógico y físico actuales a los sistemas e instalaciones cuando las personas son reasignadas o transferidas a otros puestos dentro de la organización.  4.2 Iniciar el proceso de transferencia o reasignación mediante los pasos estipulados en el proceso de transferencia y en los tiempos acordados.  4.3 Modificar la autorización de acceso según sea necesario para que corresponda con cualquier cambio en la necesidad operativa debido a la reasignación o transferencia 4.4 Notificar al personal implicado dentro de este proceso de la transferencia o reasignación del personal |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Desarrollar y documentar acuerdos de acceso para sistemas organizacionales, estos se deben revisar y actualizar frecuentemente.  2. Verificar que las personas que requieran acceso a la información y los sistemas de la organización deban:  2.1 firmar acuerdos de acceso apropiados antes de que se le conceda acceso.  2.2 volver a firmar los acuerdos de acceso para mantener el acceso a los sistemas de la organización cuando los acuerdos de acceso se hayan actualizado. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Revisar y actualizar las designaciones de riesgo de puesto frecuentemente antes de autorizar el acceso al sistema.  2. Reevaluar a las personas de acuerdo con las condiciones definidas por la organización que requieren una nueva evaluación y, cuando así se indique, la frecuencia de la nueva evaluación. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Recopilar datos relevantes para medir el cumplimiento de los acuerdos de acceso a información. |
| NIVEL 5 [Optimizado]: La organización se centra en la mejora continua y está diseñada para girar y responder a las oportunidades y los cambios. | 1. Utilizar los datos recopilados para identificar áreas de mejora e implementar acciones correctivas y preventivas para mantener la mejora continua dentro de los acuerdos de acceso a información.  2. Utilizar las lecciones aprendidas en relación con el cumplimiento de los acuerdos de acceso a información para mejorar los procesos y procedimientos relacionados. |

# Preguntas de Auditoría para el Acceso a la Información

|  |
| --- |
| Temática: Acceso a la información |
| En esta evaluación, el auditor debe examinar minuciosamente cómo se otorgan y gestionan los permisos de acceso a sistemas, aplicaciones y recursos dentro de una organización, en importante también realizar un análisis de los registros, documentos y evidencias que respalden estas asignaciones de derechos de acceso. Esto con el fin de garantizar que los empleados y usuarios externos tengan únicamente los derechos necesarios para realizar sus funciones, evitando accesos indebidos o excesivos que puedan comprometer la seguridad de los datos y la privacidad de la información y que exista la documentación adecuada que respalde quiénes tienen acceso a qué recursos y por qué razón.  Para la evaluación, el auditor debe tener en consideración: Asignación de derechos al acceso a la información Este levantamiento puede incluir análisis específicos tales como:   * ¿Existe un proceso formalizado para asignar una designación de riesgo de acceso a la información y los sistemas de información a todos los puestos en la organización?   + ¿Cómo se determinan los criterios utilizados para asignar el nivel de riesgo a cada puesto?     - ¿Existen registros documentados que respalden las designaciones de riesgo para cada puesto?     - ¿Se consideran factores como la experiencia laboral, habilidades técnicas, habilidades blandas y requisitos de educación al establecer los criterios de selección?     - ¿Quiénes son responsables de establecer y mantener estos criterios de selección? ¿Los responsables y su nivel de autoridad están identificados en la Política de Seguridad, de Gestión de Personas o cualquier otro instrumento de alto nivel que los avale?   + ¿Quiénes son responsables de realizar la asignación de riesgo y cómo se garantiza la imparcialidad y objetividad en este proceso?   + ¿Se revisan periódicamente las designaciones de riesgo existentes para asegurar que sigan siendo adecuadas en función de los cambios en las responsabilidades y el entorno laboral? * ¿Existe un proceso de revisión por parte de la alta dirección para garantizar que las asignaciones de riesgo sean coherentes con los objetivos estratégicos de la organización y con los resultados de la evaluación de ciberriesgos? * ¿Existe un mecanismo para recibir retroalimentación de los candidatos o empleados con respecto a los criterios de selección? * ¿Se documentan los criterios de selección de manera clara y accesible para los responsables de la contratación y el proceso de selección? * ¿Cómo se garantiza que los criterios de selección no sean discriminatorios y cumplan con las leyes y regulaciones laborales? * ¿Se ha definido un proceso para abordar excepciones o casos especiales que no cumplan con todos los criterios de selección establecidos?  3.1.1 Documentación relevante de acceso a la información Este levantamiento puede incluir análisis específicos tales como:   * ¿Los acuerdos de acceso a sistemas están adecuadamente documentados y actualizados? * ¿Los acuerdos de acceso detallan de manera completa los privilegios, responsabilidades y restricciones? * ¿Se lleva a cabo una revisión y actualización regular de los acuerdos de acceso? * ¿Los propietarios de sistemas y usuarios autorizados participan en la revisión y actualización de los acuerdos? |

|  |
| --- |
| Temática: Cese de derechos al acceso a la información |
| Esta evaluación implica revocar de manera oportuna y efectiva los permisos de acceso de aquellos usuarios que ya no tienen una necesidad legítima de acceder a ciertos recursos. Esto puede ocurrir al finalizar un contrato laboral, cuando un contrato con un proveedor externo llega a su fin, o cuando los roles y responsabilidades de un individuo cambian dentro de la organización. La evaluación asegura que este proceso se lleve a cabo de manera sistemática, evitando que se retengan accesos no autorizados. Para la evaluación, el auditor debe tener en consideración: Cese de derechos debido al termino de las funciones del personal Este levantamiento puede incluir análisis específicos tales como:   * ¿Se tienen procedimientos claros y efectivos para deshabilitar el acceso al sistema cuando un empleado finaliza su función? ¿El personal está informado sobre sus responsabilidades en cuanto a la seguridad de la información durante la terminación del empleo? * ¿Se revocan oportunamente las cuentas y credenciales del personal que ha dejado la organización? * ¿El acceso a los sistemas se desactiva de manera oportuna y adecuada cuando se finalizan las funciones del personal? * ¿Se realizan entrevistas de salida que aborden aspectos de seguridad de la información?  Cese de derechos debido al transferencia del personal Este levantamiento puede incluir análisis específicos tales como:   * ¿Se establecen procedimientos para ajustar las autorizaciones de acceso durante la transferencia de personal? * ¿Los cambios en las autorizaciones de acceso se comunican de manera efectiva al personal transferido? * ¿Existen mecanismos para notificar al personal implicado sobre las medidas de seguridad durante la transferencia?  Revisar los acuerdos de acceso Este levantamiento puede incluir análisis específicos tales como:   * ¿Los indicadores clave de cumplimiento definidos en los acuerdos de acceso se identifican y monitorean? * ¿Los datos y evidencias recopilados demuestran el cumplimiento efectivo de los acuerdos de acceso? * ¿Se implementan acciones correctivas en función de áreas de incumplimiento identificadas? * ¿Las lecciones aprendidas de auditorías anteriores se consideran en la mejora de los acuerdos de acceso? |

|  |
| --- |
| Temática: Mejora continua |
| El auditor debe verificar que los datos recopilados de los procesos se utilicen de manera eficiente para identificar áreas de mejora en la organización, que las lecciones aprendidas sean un *feedback* para el mejoramiento de los procesos y procedimientos, y que se implementen acciones correctivas y/o preventivas basados en la información recopilada. Este levantamiento puede incluir análisis específicos tales como:   * ¿Las áreas de mejora se derivan de análisis de tendencias, análisis de datos y lecciones aprendidas? * ¿La organización cuenta con indicadores específicos y relevantes para evaluar el cumplimiento de este control? Algunos ejemplos de indicadores pueden ser:   + Frecuencia con la que los empleados solicitan permisos o autorizaciones para acceder a información restringida   + Cantidad y calidad de comentarios y retroalimentación relacionados con problemas de acceso o inquietudes de seguridad.   + Número de incidentes de filtración de información reservada desde cuentas con privilegios altos.   + Numero de escenarios de riesgo por falta de segregación de funciones no tratable. * ¿Las acciones correctivas son adecuadamente documentadas y supervisadas?   + ¿Las mejoras implementadas demuestran un impacto positivo en el cumplimiento y eficiencia? * ¿Se implementan acciones correctivas y preventivas basadas en áreas de mejora identificadas? * ¿Las lecciones aprendidas de auditorías y desafíos anteriores se documentan y consideran para la planificación de los proyectos de seguridad?   + Verifique que existen iniciativas basadas en la detección de no conformidades, sobre todo aquellas que guardan relación con riesgos críticos.   + ¿Las mejoras basadas en lecciones aprendidas se verifican y evalúan en términos de eficacia y cumplimiento? |