

**CASIG 4 - Gestión de Recursos Humanos**

**Preguntas de Auditoría**

**Planificación de la Dotación Estratégica**

**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.

1. **Comunicación Efectiva:** Un auditor debe ser capaz de comunicar sus hallazgos de manera clara y concisa, tanto por escrito como verbalmente.
2. **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.
3. **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.
4. **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

La planificación de la dotación estratégica en la función de seguridad de la información y ciberseguridad (SIC) comienza con la realización de un inventario de recursos humanos empresariales y de TI, junto con una planificación detallada que permita rastrear el uso real de personal. Definir y documentar el proceso de planificación de dotación permite a la organización comprender tanto la demanda actual como la futura de recursos humanos necesarios para cumplir con las metas de SIC, el portafolio de iniciativas, la inversión futura y las necesidades operativas diarias. Identificar las carencias en áreas específicas asegura que la organización pueda responder proactivamente, evaluando y ajustando regularmente los requisitos de dotación de personal para SIC.

**1.2 Flexibilidad y Eficiencia en la Estructura de Recursos de SIC**

Para mantener una estructura de recursos flexible y eficiente, es importante establecer opciones que permitan responder a cambios organizacionales. Esto incluye el uso de transferencias, contratistas externos y acuerdos de servicio con terceros, proporcionando soporte adicional cuando las necesidades de personal evolucionan. Además, mantener un registro detallado del tiempo dedicado a tareas, proyectos y servicios facilita la retroalimentación constante para la planificación futura, permitiendo realizar ajustes que mejoren la eficiencia en la asignación de tiempo y recursos. La aplicación de la segregación de funciones también aporta información clave para optimizar los cargos actuales y futuros, asegurando que cada función en SIC esté estructurada de manera que maximice el cumplimiento de los objetivos organizacionales.

**1.3 Rol de la Auditoría en la Planificación de la Dotación Estratégica en SIC**

Desde la perspectiva de auditoría, la planificación de la dotación estratégica en SIC implica revisar el proceso de inventario y la planificación de recursos humanos, verificando que esté alineado con los objetivos y necesidades de la organización. La auditoría evalúa si el proceso de planificación es efectivo, si la información sobre el uso de tiempo en proyectos y tareas es precisa y si se aplican prácticas de segregación de funciones para optimizar la estructura de roles. Al proporcionar recomendaciones para mejorar la eficiencia y flexibilidad en la estructura de recursos, la auditoría respalda una dotación de personal adaptativa y robusta que responde eficazmente a las demandas de SIC y refuerza la capacidad de la organización para enfrentar nuevos desafíos y oportunidades en seguridad de la información.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Realizar un inventario de recursos humanos empresariales y de TI.  2. Realizar la planificación de personal, mediante un seguimiento de su uso real. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Definir y documentar el proceso de planificación de la dotación estratégica. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Entender la demanda actual y futura de recursos humanos para contribuir a lograr los objetivos de SIC y ofrecer servicios y soluciones conforme al portafolio de iniciativas relacionadas con SIC, al portafolio de  inversión futura y necesidades operativas diarias.  2. Identificar las carencias de personal en áreas o funciones correspondientes, o según corresponda según las necesidades SIC.  3. Evaluar los requisitos de dotación de personal para el área de SIC de forma periódica o ante cambios mayores.  4. Proporcionar recomendaciones sobre los planes de abastecimiento, así como de los procesos de contratación de personal empresarial y de SIC.  5. Verificar que se mantenga regularmente el inventario de recursos humanos empresariales y de TI.  6. Establecer una estructura de recursos flexible, como el uso de transferencias, contratistas externos y acuerdos de servicio con terceros, para apoyar el cambio en las necesidades organizacionales. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Mantener una información adecuada sobre el tiempo dedicado a las distintas tareas, trabajos, servicios o proyectos. |
| 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. Realizar modificaciones necesarias para asegurar la eficacia en el tiempo dedicado a las distintas tareas, trabajos, servicios o proyectos para retroalimentar la planificación de personal futura.  2. Utiliza la información obtenida de la aplicación de segregación de funciones para mejorar los cargos actuales y futuros. |

1. **Preguntas de Auditoría para la Planificación de la Dotación Estratégica**

|  |
| --- |
| Temática: Identificación de recursos humanos en la organización |
| Esta auditoría tiene como objetivo asegurarse de que se mantenga un registro preciso y completo de los empleados, sus roles, responsabilidades, habilidades y cualquier otra información relevante.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existen registros de descripciones de puestos, organigramas y contratos laborales del personal de seguridad de la información y ciberseguridad? * ¿Se ha obtenido la documentación relacionada con estructura organizativa y personal en áreas empresariales y de TI?   + ¿Existe en la política de Seguridad de la Información la definición y mandato para los roles específicos de la función SIC?   + ¿Está claro en los procedimientos de la función de SIC, TI y cualquier otro proceso relacionado los roles, responsabilidades y funciones específicos del personal SIC? * ¿Se ha verificado y documentado la cantidad de personal necesario para las actividades empresariales y en actividades de la función de seguridad de la información y ciberseguridad?   + ¿Existen proyecciones y estudios basados en información comparable de la   + industria, tales como benchmarking, estudios comparados, informes técnicos o análisis internos que prevean la necesidad de dotación estratégica?     - Verifique que las proyecciones se han discutido con la dirección y esta está consciente de la necesidad y riesgos de subdotar la función SIC. |

|  |
| --- |
| Temática: Planificación de recursos humanos |
| Inventario de recursos humanos El inventario de recursos humanos implica revisar la precisión y actualidad de la información sobre los empleados, sus roles y habilidades, y cómo se utiliza esta información para tomar decisiones estratégicas y operativas. La auditoría busca garantizar que la organización tenga un registro confiable de su personal, lo que es fundamental para garantizar la SIC y la gestión efectiva de riesgos. Este levantamiento puede incluir análisis específicos tales como:   * ¿Se verifica la actualización regular del inventario de los recursos humanos de la función SIC?   + Verifique si existe un proceso automatizado para recopilar y mantener la   + información actualizada de los empleados. De ser manual, asegúrese que se mantienen registros trazables y mantenidos en un sistema de gestión documental. Estos registros deberían considerar:     - Cargo     - Ubicación     - Nivel de Acceso     - Privilegios Necesarios     - Riesgos Potenciales     - Dependencias Jerárquicas * ¿Se registran cambios relevantes como contrataciones, desvinculaciones o cambios de puesto?   + Verifique que existe un proceso que notifique de los cambios a los dueños de controles de identidad y control de acceso según sea definido por la organización.   + Verifique que este proceso se realiza de forma automática * ¿Se verifica precisión y completitud de datos en el inventario?   + Verifique que todos los datos relevantes del inventario de RRHH se encuentran completos.   + Compruebe que los datos son verídicos, por ejemplo, contra los procesos y perfil de cargo. * ¿El inventario está alineado con objetivos empresariales, necesidades organizacionales en función de la seguridad de la información y ciberseguridad, y mejores prácticas?   + Verifique que la nomenclatura y descripción de los cargos definidos en el   + Inventario se adecúa a lo definido en la Política de Seguridad de la Información.   + Verifique que los cargos y perfiles se alinean con prácticas estándar, por ejemplo:     - NICCS     - ECSF  Registro de tiempo y asignación de recursos Registro de tiempo y asignación de recursos se refiere a revisar y evaluar cómo la organización registra y gestiona el tiempo que los empleados dedican a diversas tareas, proyectos o responsabilidades, así como cómo se asignan los recursos humanos para cumplir con los objetivos de la organización. Esta auditoría se enfoca en asegurarse de que los recursos humanos se utilicen de manera eficiente y efectiva para lograr los objetivos estratégicos y operativos. Este levantamiento puede incluir análisis específicos tales como:   * ¿Se utilizan registros de tiempo para rastrear dedicación a tareas, trabajos o proyectos? * ¿Se comparan registros de tiempo con actividades planificadas y resultados esperados?   + Verifique que existe un registro de desviaciones del tiempo requerido para las actividades.   + Verifique que los registros de desviaciones se han elevado a la jefatura correspondiente, indicando los riesgos que la implementación de proyectos y controles pueden materializar en la organización.   + ¿Existe un estudio de causa raíz de las desviaciones en los tiempos de trabajo requeridos? * ¿Los sistemas de registro de tiempo son fiables, accesibles y precisos?   + Realice pruebas de falsos positivos y negativos, pruebas de estrés y validación para asegurar que los sistemas de registros funcionan según lo establecido.   + ¿Se verifican consistencia y exactitud de registros de tiempo respecto a otras fuentes?     - Verifique otros registros, por ejemplo, los dispuestos por la jefatura de RRHH o general y que permitan contrastar los datos recabados por la función SIC sobre su personal   + ¿Se abordan discrepancias o inconsistencias en registros de tiempo? ¿Existen planes con acciones correctivas? ¿Hay evidencia que estos planes se han   + llevado a cabo? ¿Hay evidencia de que estos planes han generado algún efecto en los participantes?   + Verifique los indicadores asociados a las actividades correctivas para la asignación de recursos.  Inventario de recursos humanos El inventario de recursos humanos implica revisar la precisión y actualidad de la información sobre los empleados, sus roles y habilidades, y cómo se utiliza esta información para tomar decisiones estratégicas y operativas. La auditoría busca garantizar que la organización tenga un registro confiable de su personal, lo que es fundamental para garantizar la SIC y la gestión efectiva de riesgos. Este levantamiento puede incluir análisis específicos tales como:   * ¿Se verifica la actualización regular del inventario de los recursos humanos de la función SIC?   + Verifique si existe un proceso automatizado para recopilar y mantener la   + información actualizada de los empleados. De ser manual, asegúrese que se mantienen registros trazables y mantenidos en un sistema de gestión documental. Estos registros deberían considerar:     - Cargo     - Ubicación     - Nivel de Acceso     - Privilegios Necesarios     - Riesgos Potenciales     - Dependencias Jerárquicas * ¿Se registran cambios relevantes como contrataciones, desvinculaciones o cambios de puesto?   + Verifique que existe un proceso que notifique de los cambios a los dueños de controles de identidad y control de acceso según sea definido por la organización.   + Verifique que este proceso se realiza de forma automática * ¿Se verifica precisión y completitud de datos en el inventario?   + Verifique que todos los datos relevantes del inventario de RRHH se encuentran completos.   + Compruebe que los datos son verídicos, por ejemplo, contra los procesos y perfil de cargo. * ¿El inventario está alineado con objetivos empresariales, necesidades organizacionales en función de la seguridad de la información y ciberseguridad, y mejores prácticas?   + Verifique que la nomenclatura y descripción de los cargos definidos en el   + Inventario se adecúa a lo definido en la Política de Seguridad de la Información.   + Verifique que los cargos y perfiles se alinean con prácticas estándar, por ejemplo:     - NICCS     - ECSF  Registro de tiempo y asignación de recursos Registro de tiempo y asignación de recursos se refiere a revisar y evaluar cómo la organización registra y gestiona el tiempo que los empleados dedican a diversas tareas, proyectos o responsabilidades, así como cómo se asignan los recursos humanos para cumplir con los objetivos de la organización. Esta auditoría se enfoca en asegurarse de que los recursos humanos se utilicen de manera eficiente y efectiva para lograr los objetivos estratégicos y operativos. Este levantamiento puede incluir análisis específicos tales como:   * ¿Se utilizan registros de tiempo para rastrear dedicación a tareas, trabajos o proyectos? * ¿Se comparan registros de tiempo con actividades planificadas y resultados esperados?   + Verifique que existe un registro de desviaciones del tiempo requerido para las actividades.   + Verifique que los registros de desviaciones se han elevado a la jefatura correspondiente, indicando los riesgos que la implementación de proyectos y controles pueden materializar en la organización.   + ¿Existe un estudio de causa raíz de las desviaciones en los tiempos de trabajo requeridos? * ¿Los sistemas de registro de tiempo son fiables, accesibles y precisos?   + Realice pruebas de falsos positivos y negativos, pruebas de estrés y validación para asegurar que los sistemas de registros funcionan según lo establecido.   + ¿Se verifican consistencia y exactitud de registros de tiempo respecto a otras fuentes?     - Verifique otros registros, por ejemplo, los dispuestos por la jefatura de RRHH o general y que permitan contrastar los datos recabados por la función SIC sobre su personal   + ¿Se abordan discrepancias o inconsistencias en registros de tiempo? ¿Existen planes con acciones correctivas? ¿Hay evidencia que estos planes se han   + llevado a cabo? ¿Hay evidencia de que estos planes han generado algún efecto en los participantes?   + Verifique los indicadores asociados a las actividades correctivas para la asignación de recursos. |

|  |
| --- |
| 3.3 Temática: Estructura organizacional |
| El objetivo principal de analizar la estructura organizacional es garantizar que la organización tenga una estructura bien definida y funcional que permita una gestión efectiva de recursos humanos y una toma de decisiones coherente, la cual esté en constante revisión ante cambios que surjan y que requiera cambiar la estructura organizacional para adaptarse a estos cambios. Este levantamiento puede incluir análisis específicos tales como:   * ¿Se verificó la estructura organizativa en áreas funcionales de SIC para identificar áreas críticas para el cumplimiento de las necesidades organizacionales?   + Verifique que las necesidades organizacionales se basan en la apreciación al riesgo y al cumplimiento de los objetivos estratégicos.     - Verifique que el diseño de la estructura organizativa funcional ha sido validado por un comité estratégico de seguridad de la información o mecanismo similar.   + Compruebe si existe una revisión documental y entrevistas con los líderes de las áreas funcionales para determinar la criticidad de su operación.   + Verifique que las áreas críticas cuentan con la supervisión, independencia, autoridad y recursos necesarios para dar respuesta a su función. * ¿Se evalúa si la estructura actual permite adaptarse a cambios en necesidades?   + ¿Existen mecanismos para identificar y abordar rápidamente necesidades emergentes?     - ¿Se han examinado incidentes y casos previos de desviación de tiempos de finalización de tareas o necesidades emergentes especiales y su causa raíz?       * Verifique que para cada caso se ha identificado los mecanismos de detección, los mecanismos de comunicación con el liderazgo organizacional y las acciones tomadas para remediarlo.     - ¿La función SIC realiza ejercicios de planificación de escenarios para simular situaciones de emergencia y evaluar cómo se respondería a ellas?     - ¿Se han tomado medidas respecto al resultado de estas simulaciones?     - ¿Se han levantado alertas y propuestas a la alta dirección en base al resultado de estos ejercicios?   + ¿Se evalúa si se requiere personal adicional en función de cambios organizacionales?     - Examine registros de reuniones de planificación estratégica y decisiones de gestión que indiquen los cambios necesarios.     - Contraste los registros con los informes financieros y presupuestarios para identificar posibles restricciones que afecten la adaptabilidad de la estructura.     - Verifique que se ha notificado del riesgo de no adaptar la estructura organizacional de la función SIC.     - Verifique si la organización ha realizado un análisis comparativo con la estructura de personal en organizaciones de industrias y funciones similares.     - Verifique la organización ha comparado las tasas de crecimiento y tamaño de la fuerza laboral en función de los factores como: riesgo, tamaño y complejidad de las operaciones. Considere las recomendaciones de mejores prácticas como los informes sectoriales ENISA y NIST. * ¿Se evalúan acuerdos de servicio con terceros para soportar cambios organizacionales? * ¿Se verifica eficacia en el uso de contratistas externos para recursos adicionales? |