CAIGG

CONSEJO DE AUDITORÍA INTERNA GENERAL DE GOBIERNO

Ministerio Secretaría General de la Presidencia

"Guía GASIC N° 3" - Marzo 2024

Guía de Auditoría, Seguridad de la Información y Ciberseguridad N°3

SEGURIDAD EN LOS RECURSOS HUMANOS

ÍNDICE

Nota

PRESENTACIÓN

En cumplimiento con las instrucciones del Presidente de la República, Gabriel Boric Font, sobre fortalecimiento de la Política de Auditoría Interna de Gobierno; el Consejo de Auditoría Interna General de Gobierno, entidad asesora en materias de auditoría interna, control interno, probidad, gestión de riesgos y gobernanza del Supremo Gobierno, presenta a la Red de Auditoría Gubernamental, la GASIC N°3: Seguridad en los Recursos Humanos.

Esta guía es parte de una iniciativa del Consejo de Auditoría Interna General de Gobierno (CAIGG) que busca fortalecer la posición del sector público en materias de Seguridad de la Información y Ciberseguridad, dotando de instrumentos a los Auditores Internos y Servicios Públicos de instrumentos y herramientas que permitan desarrollar un levantamiento de información en base a las mejores prácticas y la legislación vigente.

Santiago, Marzo 2023.

Daniela Caldana Fulss
Auditora General de Gobierno

Capítulo 1

EL PROCESO DE GESTIÓN DE RECURSOS HUMANOS

El proceso de gestión de personas, también conocido como gestión de recursos humanos, se refiere al conjunto de prácticas y estrategias que las organizaciones implementan para administrar eficazmente a su personal. Este proceso abarca desde la atracción y selección de talento hasta su desarrollo, retención y, eventualmente, desvinculación.

Nota Importante

Estrictamente hablando, **Seguridad de la Información y Ciberseguridad** son dos conceptos diferentes.

La **"Seguridad de la Información"** es la preservación de la Confidencialidad, Integridad y Disponibilidad de la Información en los activos de información, en cualquier medio (incluso, las personas); por otro lado **"Ciberseguridad"** hace referencia exclusiva al ciberespacio y activos digitales.

En esta guía adoptamos el concepto de "Seguridad de la Información y Ciberseguridad", pero para evitar la redundancia y el exceso de texto, utilizaremos los conceptos de "Seguridad de la Información", "Ciberseguridad" o el acrónimo "SIC" como sinónimos para mejorar la comprensión lectora.

1.1 CARACTERÍSTICAS CLAVE DE LA GESTIÓN DE PERSONAS

Existen varios marcos y formas de ver este proceso, pero los componentes clave comunes a todos incluyen:

1. **Reclutamiento y Selección**
   Se identifican, atraen y eligen a los candidatos adecuados para las vacantes de la organización
2. **Formación y Desarollo**
   Proporciona a los empleados las habilidades y conocimientos necesarios para su crecimiento profesional y el éxito de la organización
3. **Evaluación del Desempeño**
   Mediante la cual se mide y analiza el rendimiento de los empleados para reconocer logros y áreas de mejora
4. **Compensación y Beneficios**
   Aborda la remuneración y las recompensas otorgadas a los empleados
5. **Relaciones Laborales**
   Gestiona la relación entre la organización y sus empleados, incluyendo la comunicación, resolución de conflictos y el bienestar del personal

¿Qué Tiene Que Ver la Seguridad de la Información con Esto?

El factor humano es a menudo la principal vulnerabilidad en la protección de datos. *A través de la capacitación, políticas y una cultura organizacional adecuada, los principios de seguridad de la información aplicados a la gestión de personas buscan minimizar los riesgos asociados con errores humanos, garantizar el acceso adecuado a la información y promover prácticas seguras entre los empleados, asegurando así la integridad y confidencialidad de la información de la organización.*

Fuente: Relevancia de la Gestión de Personas para el Cumplimiento de los Objetivos Organizacionales

1.1 Características Clave de la Gestión de Personas

01 Desarrollo y Capacitación

La formación continua y el desarrollo profesional aseguran en los empleados las habilidades necesarias para desempeñar sus roles de manera efectiva. Esto conduce a una mayor productividad y adaptabilidad a los cambios del mercado, permitiendo a la organización mantenerse competitiva.

02 Selección Adecuada

Un proceso de reclutamiento y selección riguroso garantiza que se contraten individuos con las habilidades, actitudes y valores alineados con la cultura y objetivos de la organización. Esto reduce la rotación de personal y mejora la cohesión del equipo, impulsando el logro de metas corporativas.

03 Motivación y Retención

Fomentar un ambiente de trabajo positivo, con reconocimiento, recompensas y oportunidades de crecimiento, motiva a dar lo mejor de sí. Empleados motivados y comprometidos son esenciales para la innovación, eficiencia operativa y la satisfacción del cliente, factores clave para el éxito organizacional.

04 Comunicación Efectiva

Una comunicación clara y abierta entre todos los niveles de la organización promueve la colaboración, reduce malentendidos y asegura que todos estén alineados hacia objetivos comunes. La transparencia y el flujo de información permiten la toma de decisiones informada y la rápida adaptación a desafíos externos.

El principal objetivo de esta guía es proporcionar al auditor una comprensión práctica de la intersección entre la gestión de recursos humanos y la ciberseguridad. A través de este material, se busca:

- **Ilustrar la Importancia Crítica de los Recursos Humanos en la Ciberseguridad**
  Los recursos humanos son a menudo la primera línea de defensa contra amenazas cibernéticas. La formación, conciencia y políticas adecuadas pueden marcar la diferencia entre una organización segura y una vulnerabilidad significativa.

- **Profundizar en las Normativas Relevantes**
  Se pretende que los lectores comprendan los estándares y mejores prácticas en la gestión de la seguridad de la información. Con especial énfasis en los instrumentos de apoyo a las pruebas de auditoría.

- **Entender los Riesgos Asociados a la Gestión de Recursos Humanos**
  Desde el proceso de contratación hasta la capacitación y terminación del contrato, cada etapa del ciclo de vida del colaboador presenta riesgos únicos que deben ser gestionados adecuadamente para garantizar la seguridad de la información.

- **Comprender el Rol del Auditor Interno**
  La auditoría interna juega un papel crucial en la identificación y gestión de riesgos, así como en la garantía de que las políticas y procedimientos se siguen correctamente. Esta guía proporcionará las responsabilidades y técnicas del auditor interno en relación con la ciberseguridad y la gestión de recursos humanos.

1.2 MARCOS, ESTÁNDARES Y PRÁCTICAS BASE

En el desarrollo de este documento y su instrumento técnico, se recogen los conocimientos de varios estándares y marcos clave que pueden ayudar a las organizaciones a desarrollar e implementar una auditoría al proceso de gestión de personas con un enfoque en el cumplimiento de los controles de SIC. El uso de información referencial es clave para asegurar la adopción de mejores prácticas e incrementar el éxito en la implantación y evaluación del sistema de gobierno para la seguridad de la información.

REFERENCIA	DESCRIPCIÓN
Marco de Protección de la Infraestructura Crítica NIST CSF versión 1.1	**Desarrollado por el Instituto Nacional de Estándares y Tecnología, el CSF del NIST proporciona un enfoque flexible y basado en el riesgo para gestionar el riesgo de ciberseguridad, centrándose en cinco funciones principales: identificar, proteger, detectar, responder y recuperar.**
Objetivos de Control Para la Información y Tecnologías - COBIT 2019	**Es un conjunto integral de mejores prácticas para el gobierno y la gestión de TI empresarial, con un fuerte enfoque en la generación de valor organizacional. Define objetivos, prácticas de gestión y actividades para alcanzar los objetivos estratégicos**
Sistema de Gestión de Seguridad de la Información ISO 27001:2022	**Estándar internacional que establece un marco para la gestión de la seguridad de la información en organizaciones. Se centra en identificar, evaluar y mitigar los riesgos de seguridad de manera sistemática, garantizando la confidencialidad, integridad y disponibilidad de los activos de información. La norma abarca la implementación de controles y la mejora continua del sistema de gestión de seguridad de la información.**
Controles de Seguridad y Privacidad NIST 800-53	**Proporciona pautas para la gestión y protección de sistemas de información en el gobierno y la industria. Se centra en controles de seguridad y prácticas para salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información.**
Controles Críticos de Seguridad Controles CIS	**Conjunto de prácticas de seguridad cibernética diseñadas para mitigar riesgos y fortalecer la postura de seguridad de sistemas y redes. Compuestos por 20 controles fundamentales y 7 controles adicionales, abordan áreas como gestión de acceso, monitoreo y respuesta a incidentes. Provee un marco sólido para ayudar a las organizaciones a prevenir y responder efectivamente a amenazas cibernéticas.**

1.3 EL PROCESO DE GESTIÓN DE PERSONAS

El proceso de gestión de personas se encuentra definido en diferentes referencias relevantes, todas ellas presentan sutiles cambios. Es necesario adoptar una visión que permita establecer un punto en común para poder comprender dónde y cómo se implementan los controles de Seguridad de la Información y Ciberseguridad (SIC) . A pesar de que esta guía presenta los modelos en su totalidad (con el fin de entregar información completa y contextualizar al auditor) es importante considerar que no todas las actividades y subprocesos de la Gestión de personas son competencia directa de la función de SIC.

Ilustración n°1 Fuente: Elaboración Propia

1.3.1 MODELO INTEGRADO DE GESTIÓN DEL EMPLEO Y RECURSOS HUMANOS

Esta guía utiliza la visión adoptada en el modelo de gestión de personas para la administración central del estado
Este modelo cuenta con 5 componentes o subsistemas.

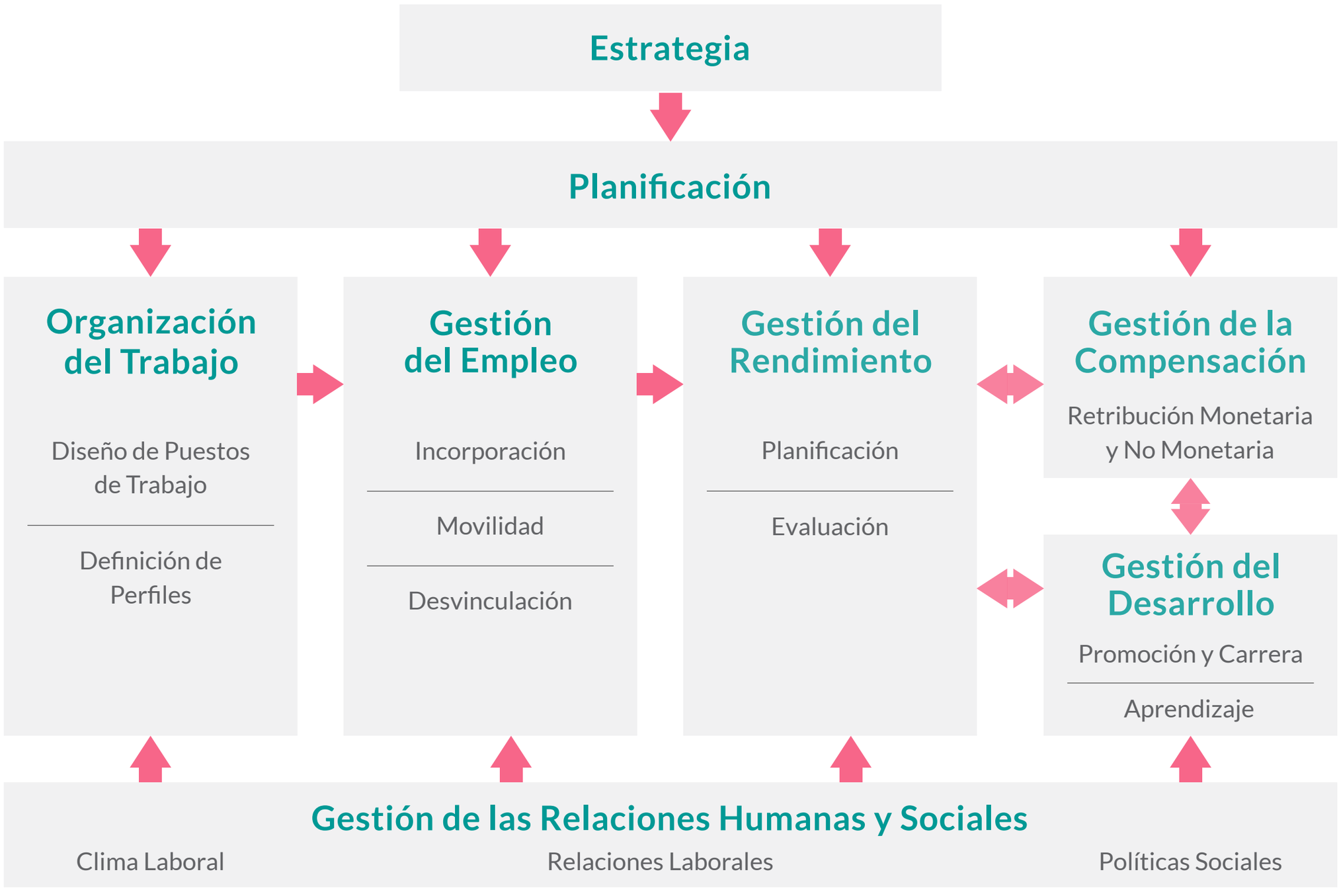


Ilustración n°2 Fuente: Modelo Integrado de la Gestión de Empleo y RRHH

El Subsistema de Planificación, tiene como función definir políticas para los demás subsistemas, a partir del input estratégico y con el mandato de mantener la coherencia general

01 El Subsistema de Organización del Trabajo, establece con mayores niveles de detalle qué funciones deberán cumplirse en cada puesto y precisar qué competencias deben exhibir los funcionarios que tendrán a su cargo la generación de estos resultados.

02 El Subsistema de Gestión del Empleo, tiene a su cargo la definición de los flujos de la dotación dentro de la estructura organizacional: ingresos, movimientos y egresos.

03 Corresponde a la tarea de especificar y traducir en términos cuantitativos, y cualitativos las necesidades dotacionales derivadas de la estrategia institucional

04 El Subsistema Gestión del Rendimiento, establece metas, supervisa y estimula el trabajo en pos de las mismas, para finalmente asignarle una evaluación a cada funcionario. Conduce necesariamente a dos subsistemas adicionales: Gestión de la Compensación, que retribuye los buenos desempeños, y Gestión del Desarrollo que toma a su cargo la función de promover el crecimiento laboral de las personas.

05 El Subsistema de Relaciones Humanas y Sociales, al igual que en el Subsistema de Planificación, corresponde a un proceso de características transversales en la base del modelo: la gestión de las relaciones humanas y sociales que se producen en la vida institucional y comprende las relaciones colectivas de trabajo, el clima organizacional y la gestión de las políticas sociales (especialmente beneficios en salud)

1.3.2 EL PROCESO DE GESTIÓN DE PERSONAS COMO CICLOS TEMPORALES

La teoría del Modelo de Ciclos Temporales sugiere que estos ciclos se repiten constantemente, con todos sus componentes sucediendo al mismo tiempo. Esto implica la integración de una visión clara, la evaluación de las habilidades presentes y futuras, el reconocimiento de la diferencia entre las demandas actuales y venideras, y la formulación de un plan para el crecimiento del personal. Todos estos aspectos se adaptan y modifican constantemente en función de las variaciones en las metas de la organización.

Ilustración n°3 Horizontes Temporales y Procesos de Gestión de Personas
Fuente: Construcción de un Modelo de Formación en Gestión de personas

Horizontes Temporales y Procesos de Gestión de Personas

CICLO DE CORTO PLAZO

En gestión de personas o Ciclo de Gestión del Desempeño, busca que los puestos de trabajo y la organización, estén provistos con individuos idóneos, con metas de desempeño definidas, pertinentes y recompensadas, de manera que sea posible asegurar el logro de los objetivos fijados.

CICLO DE MEDIANO PLAZO

En gestión de personas o Ciclo de Gestión del Desarrollo, no se centra en las metas de corto plazo sino en los objetivos que permitirán que la organización sea eficaz en el futuro para cumplir su misión. Busca la preparación de las personas de todos los niveles de la organización, a objeto de proveer las competencias requeridas para desarrollarse en los escenarios venideros contemplados en la estrategia. Se trata de un ciclo que articula, por la vía de preparar las capacidades de las personas y de los equipos, para el éxito futuro.

CICLO DE LARGO PLAZO

En gestión de personas o Ciclo de Gestión del Cambio Organizacional, se centra en las transformaciones necesarias para orientar a la organización, en su conjunto, hacia los horizontes de largo plazo vinculados a la misión institucional considerando contextos cambiantes. Es este ciclo, el que informa de los requerimientos futuros en cuanto a capacidad de los equipos y de las personas, al ciclo de mediano plazo

CICLO TRANSVERSAL

También entendido como Proceso de Planificación y Soporte de la Estrategia de Personas, cuya preocupación radica en examinar las capacidades y rol de la función de Gestión de Personas en la planificación y control de las actividades asociadas. Es especialmente relevante el posicionamiento e influencia del área, así como los sistemas de soporte para su desempeño. En este ciclo, se consideran las políticas de recursos humanos presentes en la organización; los contenidos que ésta abarca; cómo ha sido gestada y difundida. Respecto a la planificación, se considerará el horizonte temporal con el que se planifica la Gestión de Personas; los contenidos de dicha planificación; la existencia y calidad de indicadores (cumplimiento presupuestario, actividades programadas), además de las lógicas de medición del cumplimiento y presupuesto anual.

1.3.3 LA MIRADA DESDE LAS TECNOLOGÍAS: EL PROCESO SEGÚN COBIT 2019

COBIT 2019 es un marco de gestión y gobierno de TI *desarrollado por ISACA que proporciona un* ***enfoque integral para el desarrollo, implementación, monitoreo y mejora de las prácticas de TI.*** *Aunque COBIT 2019 aborda aspectos de ciberseguridad, no debe utilizarse exclusivamente para este propósito, ya que su alcance es más amplio y abarca todas las áreas de la gestión de TI. La ciberseguridad requiere enfoques y herramientas específicas que pueden no estar detalladas en profundidad en COBIT, por lo que* ***es esencial complementar con otros marcos o estándares especializados en seguridad de la información.***

APO07 de COBIT 2019 se refiere a "Gestionar los Recursos Humanos". Es uno de los procesos de gestión dentro del dominio de "Alinear, Planificar y Organizar" de COBIT.

COBIT no entrega una visión de procesos “clásica” como la que se acostumbra a ver, si no que todas las etapas, que se denominan “prácticas de gestión” se relacionan entre ellas a través de interfaces de entrada y salida de elementos documentales. No es propósito de esta guía analizar en profundidad este mecanismo, por lo que se presentan las prácticas de gestión en la siguiente ilustración:

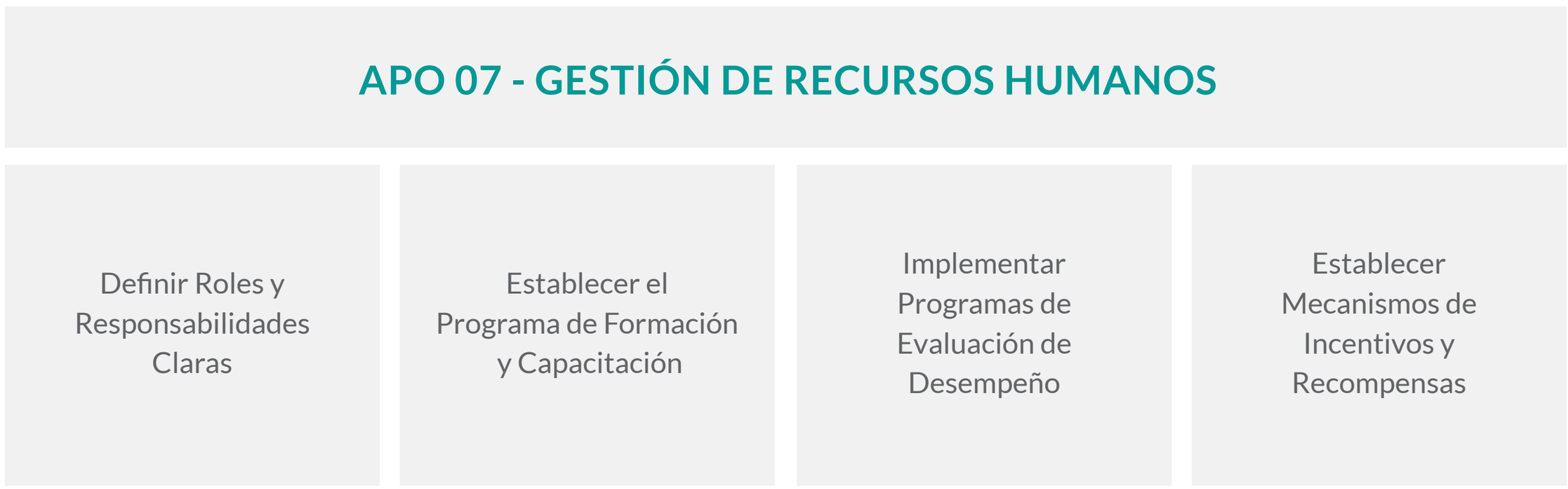


Ilustración n°4 APO07 Fuente: COBIT 2019

1.3.4 ALCANCE DE LA GUÍA METODOLÓGICA

Las áreas de enfoque delinean los aspectos críticos de la gestión de personas que tienen un impacto directo en la seguridad de la información. Estas áreas no solo representan las etapas y procesos clave en el ciclo de vida del empleado dentro de la organización, sino que también subrayan cómo las interacciones humanas, las decisiones y las conductas pueden influir en la integridad, confidencialidad y disponibilidad de los datos. Al abordar cada área de enfoque, se busca identificar potenciales vulnerabilidades y fortalecer las prácticas que garantizan una gestión segura de la información en el contexto humano.

Reclutamiento y Selección	Verificar la existencia y aplicación de controles de seguridad durante el proceso de contratación, como verificaciones de antecedentes y acuerdos de confidencialidad.
Formación y Capacitación	Evaluar la eficacia de los programas de capacitación en seguridad de la información y si se actualizan regularmente para abordar amenazas emergentes.
Acceso a la Información	Examinar cómo se otorgan, modifican y revocan los privilegios de acceso a la información, y si estos procesos están adecuadamente controlados y auditados.
Respuesta a Incidentes	Evaluar la preparación del personal para responder a incidentes de seguridad y si están familiarizados con los procedimientos de notificación y escalada.
Desvinculación de Empleados	Verificar que existen procedimientos para revocar el acceso a sistemas y datos cuando un empleado deja la organización y que estos se aplican de manera efectiva.
Cultura de Seguridad	Evaluar la conciencia y actitud del personal hacia la seguridad de la información y si la cultura organizacional promueve prácticas seguras.

Estas áreas de enfoque y alcance dan forma a los controles que este dominio desarrolla, los cuales se encuentran desarrollados en el punto 3.3 “Desarrollo de un plan de auditoria para la Gestión de Personas enfocado en SIC”

Capítulo 2

ENFOQUE SIC SOBRE EL PROCESO DE GESTIÓN DE PERSONAS

2.1 CONTROLES DE SEGURIDAD EN EL CICLO LA CAPACITACIÓN

¿Por qué es importante la capacitación, aprendizaje y desarrollo en seguridad de la información para los empleados fuera de la función SIC?

Primera Línea de Defensa	Los empleados son a menudo el primer punto de contacto con amenazas cibernéticas, como el phishing. Una formación adecuada los prepara para reconocer y manejar estas amenazas, reduciendo el riesgo de brechas de seguridad.
Cumplimiento Normativo	Capacitar al personal ayuda a las organizaciones a cumplir con estas normativas y evitar sanciones.
Cultura de Seguridad	Cuando los empleados entienden la importancia de la ciberseguridad, es más probable que adopten prácticas seguras en su trabajo diario.
Adaptación a Amenazas Evolutivas	La formación continua asegura que el personal esté al tanto de las últimas tácticas y técnicas utilizadas por los ciberdelincuentes, permitiendo a la organización mantenerse un paso adelante.
Protección de Activos Valiosos	Capacitar al personal en ciberseguridad protege estos activos valiosos de amenazas, garantizando la continuidad del negocio y protegiendo la reputación de la empresa.

Capacitación y Desarrollo

La capacitación, es decir, el desarrollo de habilidades técnicas, operativas y administrativas en todos los niveles del personal ayudan a los miembros de la organización a desempeñar su trabajo actual y genera beneficios que pueden prologarnse durante toda la vida laboral, ayudando en el desarrollo de las personas para asumir futuras responsabilidades. Muchos programas que se inician solo para capacitar a un empleado concluyen ayudándolo a su desarrollo e incrementando su potencial como empleado intermedio, o, incluso, de nivel ejecutivo.

> ***La detección de necesidades de capacitación (DNC) es un proceso sistemático mediante el cual se identifican y analizan las carencias o brechas entre las habilidades y conocimientos actuales de los empleados y las habilidades y conocimientos requeridos para el desempeño óptimo de sus funciones dentro de la organización.*** *Esta detección tiene como objetivo principal determinar las áreas específicas donde se requiere capacitación o formación adicional para mejorar la productividad, eficiencia y calidad del trabajo.*

Aunque en ocasiones la diferencia entre capacitación y desarrollo profesional es tenue, se entiende por desarrollo los programas dirigidos en especial a empleados de niveles medios y superiores, a corto, mediano y largo plazos a los cuales se les da una preparación que les servirá en el futuro. Aunque pareciera que la distinción entre capacitación y desarrollo es imprecisa, es la tabla 9-1 se presenta un cuadro de sus diferencias.

Diferencias Entre Capacitación y Desarrollo

RESPONDE A	**CAPACITACIÓN** QUÉ HACER, QUÉ DIRIGIR	**DESARROLLO** QUÉ HACER, QUÉ DIRIGIR
Definición	**Actividad sistemática y programada mediante la cual se intenta preparar al trabajador para que desempeñe sus funciones asignadas en forma eficiente**	**Educación que busca el crecimiento profesional y prepara al empleado para futuras posiciones**
Objetivo	**Integrar al personal al proceso productivo**	**Acrecentar conocimientos, habilidades y actitudes de acuerdo con la filosofía organizacional**
Nivel	**Trabajadores en general**	**Ejecutivos (Mandos medios y superiores)**
Plazo	**Corto Plazo**	**Mediano y Largo Plazo**
Tipo de Educación	**Perfeccionamiento Técnico**	**Aprendizaje integral con miras al desempeño futuro**

El ciclo de capacitación, reportado en "Fundamentos de Gestión de Personas", desarrollado en base a Werther se puede definir en base a 4 etapas, todas relevantes para la gestión de la seguridad de la información:

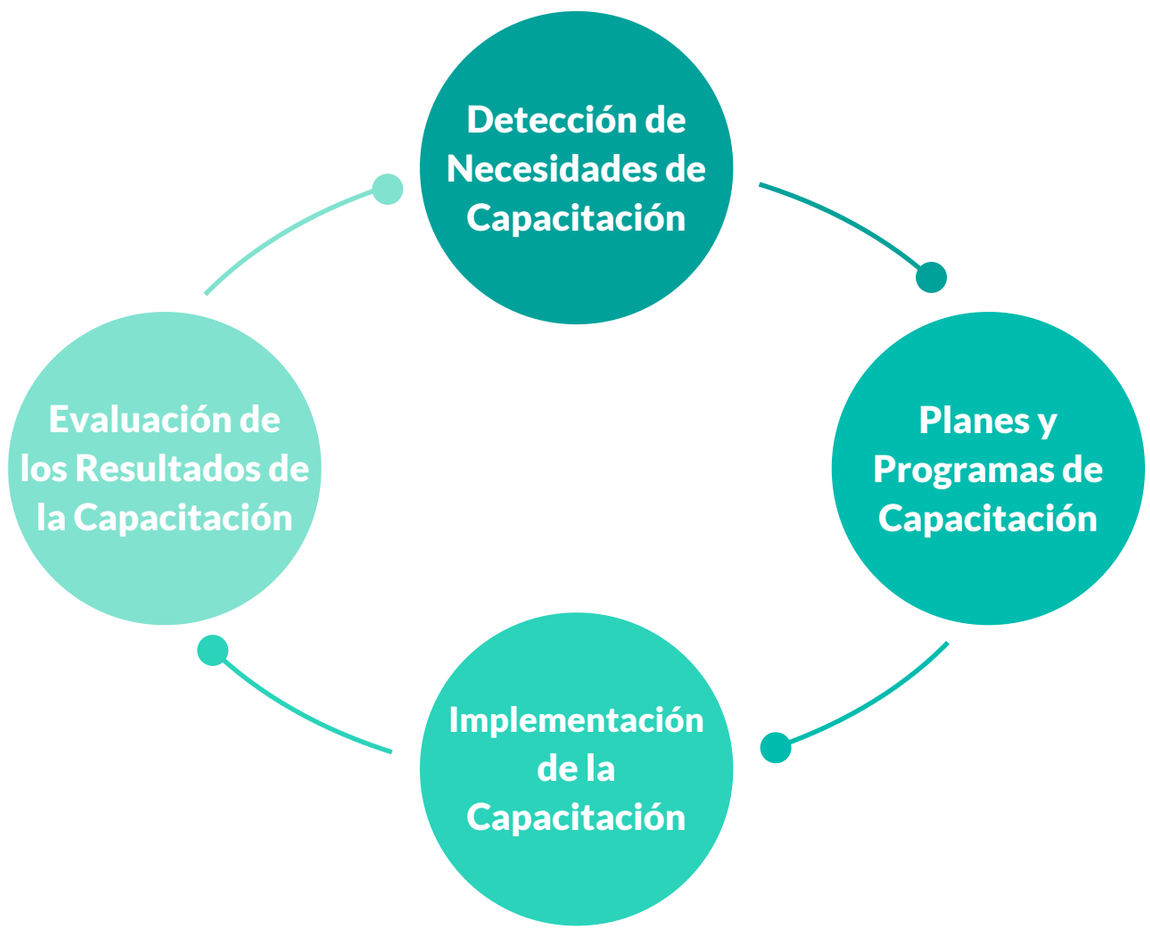


Ilustración n°5 Ciclo de Capacitación. Fuente: Fundamentos de Gestión de Personas

2.2 INTEGRACIÓN DEL CICLO DE CAPACITACIÓN Y LA FUNCIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Para ejemplificar los conceptos revisados anteriormente, se entrega a continuación una tabla que relaciona las actividades contenidas en el proceso de capacitación, y como se expresan en términos de necesidades (o controles) específicos de SIC, así como breves ilustraciones de cómo pueden ser auditados.

ETAPA	CONTROL DE CIBERSEGURIDAD	COMPROBACIÓN
Detección de necesidades de capacitación	1. Evaluación de de conciencia de seguridad 2. Análisis de incidentes previos 3. Análisis de DNC 4. Análisis de Perfiles de cargo 5. Políticas de usuario final 6. Manuales de uso aceptable de activos	1. ¿Se identificaron correctamente las necesidades de capacitación, basados en los riesgos críticos? 2. ¿Se analizaron incidentes anteriores para determinar puntos débiles a atender?
Planes y programas de capacitación	1. Validación de contenido de capacitación 2. Registro de cambios en programas	1. ¿Se validó el contenido para asegurar información actual en referencia a la tecnología que la organización utiliza y de acuerdo con sus necesidades propias y generales?
Implementación de la capacitación	1. Contratacion de servicios externos 2. Desarrollo de talleres internos 3. Autenticación en plataformas de programas 4. Registro de asistencia 5. Registro de cambios en programas	1. ¿Se verifica la identidad de los participantes? 2. ¿Se lleva un registro adecuado? 3. ¿Están protegidos los materiales?
Evaluación de Resultados de la capacitación	1. Análisis retroalimentación post-capacitación 2. Comparación de Resultados con Objetivos	1. ¿Se recopiló retroalimentación? 2. ¿Mejoraron las métricas de seguridad? 3. ¿Se alcanzaron los objetivos propuestos?

Esta tabla es una primera aproximación a lo que el Auditor Interno debe tener en cuenta cuando considera los controles de ciberseguridad en el ámbito de los recursos humanos. Cada organización puede tener un proceso de formación y reclutamiento diferente, por lo que es de vital importancia que el equipo tenga una comprensión profunda de los flujos de la organización y su lógica de trabajo.

2.3 CONTROLES DE SEGURIDAD EN EL PROCESO DE RRHH

Generalmente, las organizaciones se preocupan de comenzar a formar a su personal en la etapa de desarrollo. Esto es notable en algunas versiones de los estándares de controles, donde todas las competencias se observan "durante el empleo".

Sin embargo, a medida que los conocimientos de Seguridad de la Información y Ciberseguridad se vuelven accesibles a todo el publico (sobre todo, aquellos básicos), las organizaciones requerirán que buena parte de su fuerza laboral tenga conocimientos mínimos en esta área.

El auditor deberá poner especial cuidado en verificar que cada etapa del proceso se realiza con la diligencia requerida y observando los controles de SIC requeridos. En el siguiente modelo se presentan los temas más relevantes a ser considerados en el desarrollo de esta actividad.

¿Cómo es la relación entre la función de la seguridad de la información y ciberseguridad (SIC) y la gestión de personas?

01

Atracción

En esta etapa, la función SIC deberá colaborar con la identificación de las características y niveles de capacidad necesarios en la dotación de personal para la organización. Esto incluye comprender al personal externo e interno, y diseñar estrategias a largo plazo que habiliten el resto del proceso.

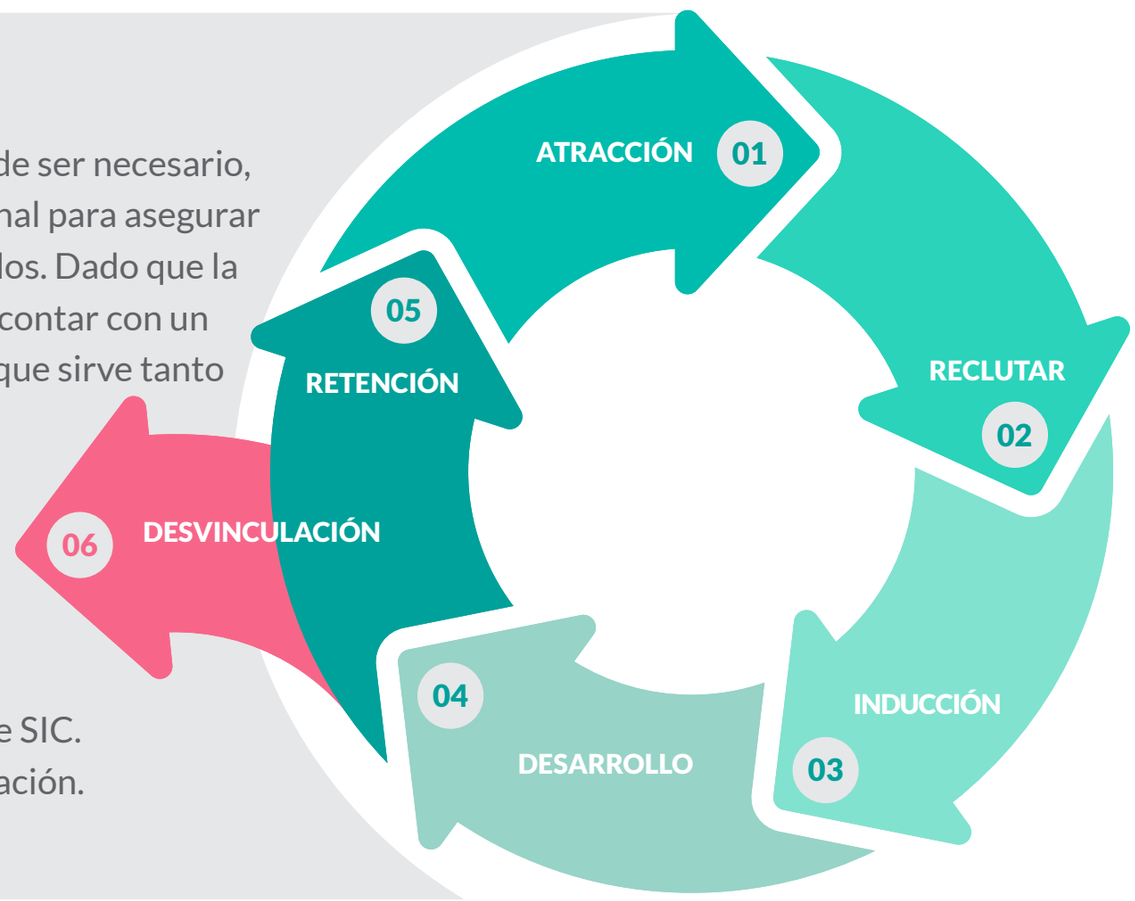
Algunas de las actividades donde interactúan ambas funciones

- Planificación de la Dotación Estratégica
- 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.
- Identificar las carencias de personal en áreas o funciones correspondientes, o según corresponda según las necesidades SIC.

02

Reclutamiento

La función SIC deberá apoyar en la elaboración de criterios y, de ser necesario, participar directamente en las entrevistas y pruebas de personal para asegurar que los candidatos cumplen con los requerimientos establecidos. Dado que la naturaleza de estas pruebas es técnica, es una buena práctica contar con un especialista evaluador. A demás, esta etapa es el primer filtro que sirve tanto para: eliminar candidatos con antecedentes no deseables y vincular candidatos con ciertas habilidades deseadas.



Algunas actividades donde interactúan ambas funciones

- Definir una estrategia de verificación de antecedentes
- Identificar potenciales candidatos "gemas en bruto" y con especialidades o modos de pensar deseables para la función de SIC.
- Evaluar los riesgos y controles propios del proceso de contratación.

03

Inducción

Fuera de las actividades de entrega del cargo e inducción a las tareas, es en esta etapa donde el nuevo colaborador deberá comenzar a integrar los principios y la cultura de SIC. Esto incluye una comprensión en profundidad de las políticas y reglamentos que rigen la seguridad de la información dentro de la organización, así como sus responsabilidades y los canales de asistencia que la organización ha puesto a disposición de él para este fin.

Algunas de las actividades donde interactúan ambas funciones

- Definir canales de comunicación con los Puntos de Contacto establecidos para el reporte de incidentes
- Diseñar y ejecutar campañas tempranas de concienciación y capacitación
- Entrenar al personal en el acceso a la información personal y en los acuerdos de confidencialidad

04

Desarrollo

La etapa de desarrollo se puede comprender en dos estadios: Primero, aquel desarrollo que es propio para la función de SIC. Segundo, aquel desarrollo que es extensible a toda la organización. En ambos casos, la función de seguridad deberá apoyar en el desarrollo de la detección de necesidades de capacitación. Este proceso se encuentra detallado en los puntos anteriores: 2.1 y 2.2

Algunas de las actividades donde interactúan ambas funciones

- Entrenar al personal de la función SIC en las nuevas herramientas y capacidades necesarias para el mejor cumplimiento de su función.
- Entrenar a todo el personal en los principios de SIC aplicables a su trabajo.
- Entrenar a todo el personal en su responsabilidad como propietarios o usuarios de activos de información.
- Entrenar a todo el personal los procesos de respuesta a incidentes.

05

Retención

Aunque no se encuentra contemplado en ningun estándar, se puede considerar incluir objetivos asociados a la seguridad de la información en los planes de compensación de los responsables de las áreas de tecnología, siempre que sea observando criterios de gestión apropiados y sólo cuando el nivel de dependencia de ciberseguridad de la organización lo vuelva necesario.

06

Desvinculación

Durante esta etapa convergen diferentes controles: Acceso e Identidades, Gestión de Personas y por supuesto, la Protección de los Datos. La función de SIC debe propiciar la recepción de información a tiempo de las desvinculaciones y apoyar el establecimiento de canales de información claros, oportunos y continuamente auditados entre la función TI, la función SIC y la gestión de personas, a fin de realizar y comprobar los cambios en los sistemas de información (SI) que lo requieran.

Algunas de las actividades donde interactúan ambas funciones

- Revisar la validez de las responsabilidades y debes después de la terminación o cambio de empleo.
- El proceso de terminación o cambio de empleo también debe aplicarse al personal externo (es decir, proveedores) ante una terminación del personal, del contrato o del puesto con la organización, o cuando hay un cambio de puesto dentro de la organización.
- Eliminar o suspender los accesos a los SI y a los activos de información físicos o virtuales a aquellos desvinculados de la organización.

Capítulo 3

ROL DEL AUDITOR INTERNO EN EL PROCESO DE GESTIÓN DE PERSONAS

El papel del auditor interno es esencial, es este el profesional que se encuentra en la tercera línea de defensa y proporciona una capa de control y supervisión para garantizar que la organización esté llevando a cabo los procesos de gestión de personas de manera segura y observando los requisitos de la seguridad de la información

Los auditores internos realizan tanto auditorías de desempeño como evaluaciones de cumplimiento. Mientras que las evaluaciones de cumplimiento se centran los requisitos normativos externos y las políticas y procedimientos internos relacionados, las auditorías de desempeño requieren un análisis y evaluación de aquello que permite alcanzar el desempeño deseado, y en base a eso, definir el un programa de auditoría efectivo. Evaluar la efectividad y eficiencia de una organización es mucho más demandante, pero es crítico para determinar si el gobierno de la ciberseguridad soporta los objetivos y estrategias de la organización.

Fuente: GTAG 17, 2012.

En términos generales, los principales objetivos de la auditoría interna cuando respecta al Proceso de Gestión de Personas:

- **Determinar si la función de seguridad de la información interactúa de forma afectiva con el proceso de gestión de personas.**
- **Determinar si la dotación de la organización cuenta con las capacidades, conocimientos y habilidades necesarios para minimizar los riesgos de SIC**
- **Evaluar los ciberriesgos que puedan afectar negativamente el cumplimiento de la misión organizacional**

3.1 EL ROL DEL AUDITOR INTERNO

El rol del auditor interno está en verificar que todos los procesos, controles y buenas prácticas revisadas en esta guía y en los criterios adoptados por cada organización se llevan a cabo. En ningún caso, el auditor interno tendrá las facultades ni responsabilidad de la implementación de los procesos ni de la modificación de los instrumentos documentales o tecnológicos de la organización. Su participación en el aseguramiento del éxito de las actividades de seguridad se limitará a la evaluación independiente, objetiva y efectiva de los componentes de la función de ciberseguridad y determinar si el liderazgo de la organización es efectivo. Para ello, el auditor interno podrá realizar:

Evaluación de políticas y procedimientos

Los auditores internos pueden evaluar si las políticas y procedimientos de seguridad de la información de la organización son adecuados y se adhieren a los estándares de la industria y las regulaciones legales.

Verificación de cumplimiento

Pueden verificar si la organización está cumpliendo con sus propias políticas y procedimientos, así como con las regulaciones externas. Esto podría implicar la revisión de registros de acceso, pruebas de penetración, evaluaciones de vulnerabilidad y más.

Identificación de riesgos

Los auditores internos están capacitados para identificar posibles riesgos y brechas en la seguridad de la información. Esto puede incluir un amplio espectro de actividades, desde amenazas físicas a la infraestructura de TI hasta riesgos de ciberseguridad por lo que los auditores internos deben contar con una correcta capacitación y entrenamiento en temas relacionados con las tecnologías y la seguridad de la información.

Educación y concienciación	A través de la implementación de acciones correctivas, los auditores pueden apoyar en la educación a la organización sobre la importancia de la seguridad de la información y promover una cultura de seguridad.
Recomendaciones de mejora	Basándose en sus hallazgos durante las auditorías, pueden recomendar mejoras para aumentar la seguridad de la información. Esto es especialmente útil si la organización ha experimentado recientemente una violación de seguridad o si se ha identificado un nuevo riesgo.
Seguimiento de las medidas correctivas	Una vez que se han identificado los problemas y se han recomendado las soluciones, los auditores internos también pueden tener la responsabilidad de garantizar que se implementen las medidas correctivas.
Informe a la alta dirección	Los auditores internos deben informar regularmente a la alta dirección sobre el estado de la seguridad de la información de la organización. Estos informes pueden ayudar a la dirección a tomar decisiones informadas sobre las prioridades de seguridad y la asignación de recursos.

3.2 CÓMO UTILIZAR LA GUÍA PARA LA AUDITORÍA INTERNA

Para que el auditor interno pueda aprovechar al máximo esta publicación, es conveniente que se refiera a los instrumentos complementarios: Las preguntas de auditoría temáticas y el modelo de madurez general. Cada GASIC se compone de tres componentes:

Guía de Auditoría de la Seguridad de la Información y Ciberseguridad (GASIC):
Este es el cuerpo teórico y consiste en el marco contextual necesario para que el auditor interno comprenda el alcance y del dominio de seguridad que está evaluando. Es un instrumento con los conceptos fundamentales recopilados de mejores prácticas.

Matríz de Controles
Recopila controles desde las mejores prácticas asociadas al tema central de Guía de Auditoría, organiza los controles en una propuesta de madurez y permite al auditor conocer los requisitos que debería evaluar.

Ejemplos de Preguntas de Auditoría:
Complementa el modelo de madurez a través de una serie de preguntas organizadas en varios documentos. Cada documento representa un control que pertenece a uno de los ejes temáticos definidos al interior de la Guía de Auditoría.

La ilustración a continuación presenta esta estructura documental:

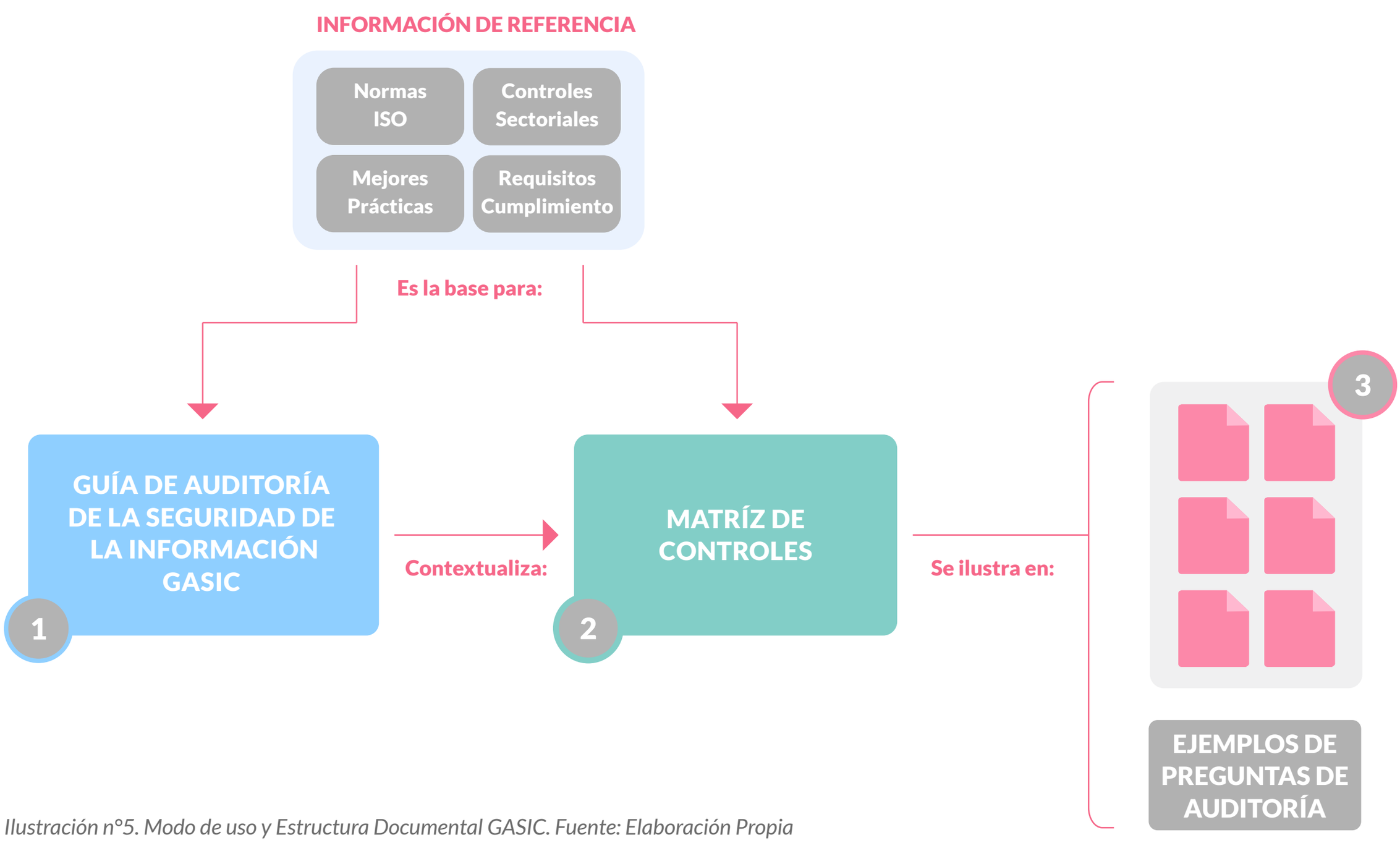


Ilustración n°5. Modo de uso y Estructura Documental GASIC. Fuente: Elaboración Propia

El método de trabajo sugerido es el siguiente:

01 **El auditor interno debe estudiar cada Guía de Auditoría para Seguridad de la Información y Ciberseguridad (GASIC) y su contexto para tener plena comprensión del tema a trabajar.**

02 **A continuación, puede utilizar el Modelo de Madurez para seleccionar los controles que sean apropiados para la organización. La selección de controles debe estar alineados con:**

a. **La estrategia de la organización.**
b. **Los resultados de la evaluación de riesgos.**
c. **Los requisitos de cumplimiento.**
d. **La estrategia de auditoría interna, expresada en el plan.**

03 **Por último, puede utilizar los documentos de ejemplo para la planificación de las preguntas y pruebas que fuese a realizar. El formato del programa, plan, instrumentos, pruebas y reportería debe ser aquel solicitado en el contexto de cada auditoría, que está fuera del alcance de esta guía.**

3.3 DESARROLLO DE UN PLAN DE AUDITORÍA PARA LA SEGURIDAD DE LA INFORMACIÓN EN EL PROCESO DE GESTIÓN DE PERSONAS

El instrumento de apoyo para la auditoría busca determinar si las actividades descritas en la guía se realizan de tal forma que permiten asegurar el logro de los objetivos de la función de seguridad de la información y ciberseguridad, apoyando de esta forma la continuidad operacional y habilitando la generación de valor de las organizaciones.

Para este fin, se han establecido 15 controles que provienen de las mejores prácticas (NIST CSF 1.1, ISO 22301:2021, ISO 27002:2022, COBIT 2019, CIS) apoyados por los principios establecidos en el Estatuto Administrativo y el Modelo de Gestión de Personas

Estos controles se han organizado en tres temas, que permiten su mejor comprensión, los cuales son:

- **Gestionar el Proceso de dotación estratégica**
- **Optimizar las capacidades de los recursos humanos**
- **Responsabilidades en la Seguridad de la Información y Ciberseguridad**

Apéndice

ANEXOS

Ejes Temáticos

I. Gestionar el proceso de Dotación Estratégica

El eje de Gestionar el Proceso de Dotación Estratégica busca hacerse cargo de los temas relacionados con la Gestión de Personas, excluyendo la Capacitación y Entrenamiento. En particular, se busca implementar mecanismos de control durante el ciclo de vida del personal en la organización, minimizando el riesgo de su interacción con los SI y la información relevante. Los controles que conforman este eje temático son:

	CONTROL	DESCRIPTOR
1	**Planificacion de la Dotación Estratégica**	**La organización se asegura de planificar y hacer seguimiento del uso de los recursos humanos del negocio y de TI.**
2	**Segregación de Funciones**	**La organización se asegura de identificar al personal clave de SIC mediante la segregación de funciones y según la importancia del cargo y funciones de las posiciones críticas.**
3	**Selección del Personal**	**La organización se asegura de adquirir una dotación de personal suficiente y adecuada, en línea con los requisitos de seguridad de la información, alineada con las políticas organizacionales y la legislación vigente.**
4	**Evaluación del Rendimiento Laboral**	**La organización asegura que evalúa y reconoce el rendimiento laboral de los empleados mediante criterios que fomenten una conducta apropiada que consolide el compromiso del personal con la seguridad de la información.**
5	**Proceso Disciplinario**	**La organización asegura que mantiene un proceso disciplinario adecuado para quienes hayan cometido violaciones a las políticas de seguridad de la información.**
6	**Terminación y Cambio de Empelo**	**La organización asegura que las responsabilidades y deberes de seguridad de la información sigan vigentes después de la terminación o cambio de empleo del personal para asegurar la confidencialidad, integridad y disponibilidad de la información.**
7	**Términos y Condiciones del Empelo**	**La organización se asegura de que los términos y condiciones de empleo establecidos dentro de los contratos de trabajo estén en línea con los requisitos de seguridad de la información, políticas y legislación vigente, y sean entendidos y aceptados por el personal.**

II. Optimizar las capacidades de los recursos humanos

Este eje temático busca abordar las habilidades generales que todo miembro de la organización debe demostrar y el dominio mínimo de los requisitos de seguridad y la higiene cibernética. Esto busca mejorar el perfil de riesgo de la organización y optimizar los recursos dedicados a la concientización y entrenamiento.
Por otro lado, este eje temático comprende las habilidades propias requeridas por la función de SIC.

Los controles que conforman este eje temático son:

CONTROL		DESCRIPTOR
1	**Concientización, Educación y Capacitación de Respuesta a Incidentes**	**La organización asegura que exista un programa de concientización y capacitación en el proceso de respuesta a incidentes, su responsabilidad y los impactos de sus acciones para todo el personal.**
2	**Concientización y Capacitación SIC**	**La organización se asegura que exista un programa de concientización y capacitación en seguridad de la información para todo el personal.**
3	**Habilidades y Competencias del Personal**	**La organización se asegura de poder garantizar que las habilidades y competencias del personal estén actualizadas y en línea con los requisitos de seguridad de la información, las políticas y la normativa vigente.**

II. Responsabilidades en Seguridad de la Información y Ciberseguridad.

Este eje temático aglutina los controles generales de seguridad que deben ser observados transversalmente en la gestión de personas.

Los controles que conforman este eje temático son:

	CONTROL	DESCRIPTOR
1	**Acceso a la Información del Personal**	**La organización asegura que mantiene acuerdos de acceso a información aplicados a las partes interesadas y al personal correspondiente, y que estos estén en línea con los requisitos de seguridad de la información, políticas y legislación vigente**
2	**Acuerdos de Confidencialidad**	**La organización asegura que mantiene acuerdos de confidencialidad o no divulgación aplicados a las partes interesadas y al personal correspondiente, y que estos estén en línea con los requisitos de seguridad de la información, políticas y legislación vigente**
3	**Gestión del Personal Externo**	**La organización se asegura de gestionar al personal externo o de carácter transitorio en el cumplimiento de sus funciones y en línea con los requisitos de seguridad de la información, las políticas y la normativa vigente**
4	**Manejo de los Incidentes**	**La organización asegura que existe un manejo adecuado en la respuesta de incidentes en seguridad de la información**
5	**Seguridad para el Teletrabajo**	**La organización asegura que existen las medidas de seguridad adecuadas para el personal que trabaja de forma remota, y que estas estén en línea con los requisitos de seguridad de la información, políticas y legislación vigente**