CAIGG
CONSEJO DE AUDITORÍA INTERNA GENERAL DE GOBIERNO
Ministerio Secretaría General de la Presidencia

Guía de Auditoría, Seguridad de la Información y Ciberseguridad N°4

GESTIÓN DE ACCESOS E IDENTIDADES

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°4: Gestión de Accesos e Identidades.

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 2024.

Daniela Caldana Fulss
Auditora General de Gobierno

Capítulo 1

GESTIÓN DE IDENTIDAD Y ACCESOS

Al discutir las mejores prácticas en ciberseguridad, es esencial resaltar dos aspectos fundamentales relacionados con la autenticación segura: garantizar el acceso a las aplicaciones vitales y zonas protegidas, y administrar las contraseñas de manera segura. Atender adecuadamente estas áreas es vital para asegurar la ciberseguridad en cualquier negocio, puesto que cualquier debilidad podría llevar a brechas serias de seguridad, como el acceso no autorizado a datos confidenciales de la empresa.

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.

Ilustración n°1. Fuente: Elaboración Propia

Identidad Digital

Un importante concepto relacionado es "Identidad digital" se define como una representación única de un sujeto que participa en una transacción en línea. Esto contiene dos elementos que constituyen el papel de la identidad digital: representar a un sujeto y apoyar una transacción en línea. La "identidad" en sí misma se puede definir como un conjunto de atributos relacionados con una entidad.

Fuente: Enisa Digital Identity Standards

1.1 CARACTERÍSTICAS CLAVE DE LA GESTIÓN DE IDENTIDAD Y ACCESOS

Los sistemas de gestión de identidad y acceso (IAM por sus singlas en inglés) están diseñados para iniciar, registrar y administrar las identidades de los usuarios y sus permisos asociados con respecto a la información delicada de una empresa. Estos usuarios incluyen no solo a los trabajadores de la empresa, sino también a proveedores, clientes, dispositivos industriales, cuentas administrativas genéricas y tarjetas electrónicas de acceso. Las herramientas que la empresa emplea para gestionar las cuentas de usuario y establecer medidas de seguridad adecuadas para la protección de datos son el núcleo de la IAM.

Fuente: GTAG09 - Gestion de Identidades y accesos

Los aspectos fundamentales definidos por INCIBE para la gestión de acceso e identidades son:

01 **Política de Usuarios y Grupos**
Define los roles de usuarios y de grupos en función del tipo de información al que podrán acceder.

02 **Asignación de Permisos**
Asigna los permisos necesarios para que cada usuario o grupo de usuarios solo puedan realizar las acciones oportunas sobre la información a la que tienen acceso

03 **Creación, Modificación y Borrado de Cuentas de Usuario con Permisos**
Define y aplica un procedimiento para dar de alta/baja o modificar las cuentas de usuario.

04 **Cuentas de Administración**
Gestiona las cuentas de administración de sistemas y aplicaciones teniendo en cuenta su criticidad.

05 **Mecanismos de Autenticación**
Determina e implantas las técnicas de autenticación más apropiados para permitir el acceso a la información de tu empresa

06 **Registro de Eventos**
Establece los mecanismos necesarios para registrar todos los eventos relevantes en el manejo de la información de tu empresa.

07 **Revisión de Permisos**
Revisar cada cierto tiempo que los permisos concedidos a los usuarios son los adecuados.

08 **Revocación de Permisos y Eliminación de Cuentas**
Desactivar los permisos de acceso y eliminas las cuentas de usuario una vez finalizada la relación contractual.

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

La gestión de identidad y acceso juega un papel fundamental en la seguridad de la información, ya que garantiza que solo las personas y entidades autorizadas puedan acceder a recursos específicos dentro de una organización. *Esta función no solo se centra en identificar a los usuarios, sino también en establecer, gestionar y auditar sus permisos y roles. Mientras que algunos aspectos de IAM, como la creación de cuentas de usuario y la gestión de permisos, suelen ser responsabilidades de la función de TI, otros aspectos más críticos, como la definición de políticas de acceso, la supervisión de patrones de comportamiento anómalos y la revisión de registros de auditoría, caen bajo la responsabilidad de la función de seguridad de la información.* ***Esta colaboración entre TI y seguridad es esencial para mantener un equilibrio entre la operatividad y la protección de los datos y recursos de la organización.***

Fuente: Relevancia de la Gestión de Identidad y Acceso para el Cumplimiento de Objetivos Organizacionales

La gestión de identidad y acceso es esencial para alcanzar los objetivos organizacionales y controlar los ciber riesgos, y su relevancia puede entenderse a través de las siguientes razones:

01 Cumplimiento Regulatorio

Muchas organizaciones están sujetas a regulaciones que exigen la protección de datos y privacidad. El IAM ayuda a cumplir con estas normativas al garantizar que solo usuarios autorizados accedan a datos sensibles.

02 Eficiencia Operacional

Al administrar los roles y permisos adecuados, las organizaciones se aseguran de que los empleados tengan acceso estrictamente a las herramientas y datos que necesitan para desempeñar sus funciones. Esto optimiza las operaciones al eliminar redundancias y agilizarprocesos.

03 Control de Ciber Riesgos

IAM permite a las organizaciones establecer controles granulares sobre quién puede acceder a qué recursos, reduciendo así la superficie de ataque. Además, facilita la detección de comportamientos anómalos, como un usuario intentando acceder a recursos fuera de sus permisos habituales.

04 Protección Contra Amenazas Internas

No todas las amenazas provienen del exterior. Empleados descontentos o comprometidos pueden representar riesgos. Un IAM robusto puede limitar el potencial daño que un actor interno puede infligir al restringir el acceso basado en la necesidad de conocer y separación de funciones.

05 Auditoría y Rendición de Cuentas

El IAM proporciona registros detallados sobre quién accedió a qué recursos y cuándo. Esto no solo ayuda en investigaciones tras un incidente, sino que también es útil para auditorías internas y externas.

06 Adaptabilidad a Cambios Organizacionales

Las organizaciones están en constante evolución, con empleados uniéndose, cambiando roles o dejando la empresa. El IAM facilita la adaptación a estos cambios

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

Ilustrar la Importancia de IAM en la Ciberseguridad
Destacar cómo un IAM efectivo puede actuar como primera línea de defensa contra amenazas cibernéticas y Subrayar la relación entre una adecuada gestión de identidades y la reducción de la superficie de ataque en una organización.

Profundizar en las Normativas Relevantes
Describir las principales normas, regulaciones y marcos de referencia que rigen la gestión de identidad y acceso. Resaltar la importancia del cumplimiento de estas normativas para evitar sanciones y proteger la reputación de la organización.

Entender los Riesgos Asociados a la Gestión de Identidad y Accesos
Identificar y analizar los principales riesgos que surgen de deficiencias o fallos en el proceso de IAM. Examinar escenarios potenciales y sus consecuencias derivadas de una inadecuada gestión de identidades y accesos.

Comprender el Rol del Auditor Interno
Detallar la función y responsabilidades del auditor interno en la revisión y evaluación de los sistemas de IAM, ofrecer pautas sobre cómo el auditor puede aportar valor, detectar deficiencias y proponer mejoras en el proceso de IAM. Abordar las mejores prácticas y herramientas que el auditor interno puede emplear para una revisión efectiva de IAM

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 identidades y accesos 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.

	CONTROL	DESCRIPTOR
1	**Marco de Protección de la Infraestructura Crítica NIST CSF Versión 1.1**	**Desarrollado por el Instituto Nacional de Estándares y Tecnología. 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**
2	**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**
3	**Sistema de Gestión de Seguridad de la Información ISO 27001**	**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. Abarca la implementación de controles y la mejora continua del SGSI ayudando a organizaciones a proteger sus datos y mantener la confianza de sus partes interesadas.**

	CONTROL	DESCRIPTOR
4	**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**
5	**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. Estos controles proveen un marco sólido para ayudar a las organizaciones a prevenir y responder efectivamente a amenazas cibernéticas, siguiendo estándares reconocidos en la industria.**
6	**Guía de Auditoría de Tecnología Global 09 Gestión de Acceso e Identidades**	**Las Guías de Auditoría de Tecnología Global (GTAG) preparadas por el Instituto de Auditores Internos (IIA) están escritas en un lenguaje directo de negocio para abordar en forma oportuna problemas relacionados con la gestión, el control y la seguridad de la tecnología de la información.** **La colección GTAG se utiliza como un recurso disponible para los directores ejecutivos de auditoría sobre los distintos riesgos asociados a la tecnología y las prácticas recomendadas**

1.3 GESTIÓN DE IDENTIDADES

La Guía de Auditoría General de Tecnología define los conceptos fundamentales de IAM a través del siguiente modelo y conceptos, que serán adoptados en esta guía metodológica instruccional y en posteriormente, en el planteamiento del plan de pruebas:

Identidad

Elemento o combinación de elementos utilizados para describir, de manera exclusiva, a una persona o máquina

Además de autenticarnos con una contraseña o con PIN, es decir con «Algo que sé», también podemos hacerlo con «Algo que tengo» (Token USB o una tarjeta de coordenadas) o con «Algo que soy» (La huella, el iris, la voz o el rostro) o bien con varios de estos elementos o factores. Algunos bancos llevan haciendo esto desde hace tiempo. La autenticación de dos (o más) factores, al comprobar dos veces mediante mecanismos diferentes, que somos quienes decimos ser, agrega una capa de seguridad a nuestros servicios, aplicaciones y sistemas. Cualquier intento de hacerse con nuestras llaves se complica.

Algunos métodos de autenticación de uso común no contienen ni comprenden secretos y, por lo tanto, no son aceptables para su uso como un único factor. Por ejemplo:

- La autenticación basada en conocimiento, en la que se pide al usuario responder a preguntas que presumiblemente sólo el (debería) conocer, no constituye un secreto aceptable para la autenticación digital. (Ej, preguntas secretas)
- Un factor biométrico tampoco constituye por sí mismo un secreto y no puede ser utilizado como autenticador.

Fuentes : Incibe Dos Mejor que Uno, Doble Factor de Autenticación - NIST SP 800-63

Accesos

Simbolizan los permisos concedidos a una entidad. Estos permisos se pueden asignar para que los individuos lleven a cabo acciones específicas en diferentes grados. Algunas de estas acciones incluyen copiar, transferir, añadir, modificar, eliminar, revisar, aprobar, leer y anular.

Habilitaciones

Grupo de derechos de acceso para realizar acciones específicas.

Es importante recordar que también existen cuentas de servicio, identidades de máquinas y otras identidades no humanas que se deben gestionar. La imposibilidad de controlar cualquiera de estas identidades y accesos puede ser perjudicial para el esquema de control general de la organización.

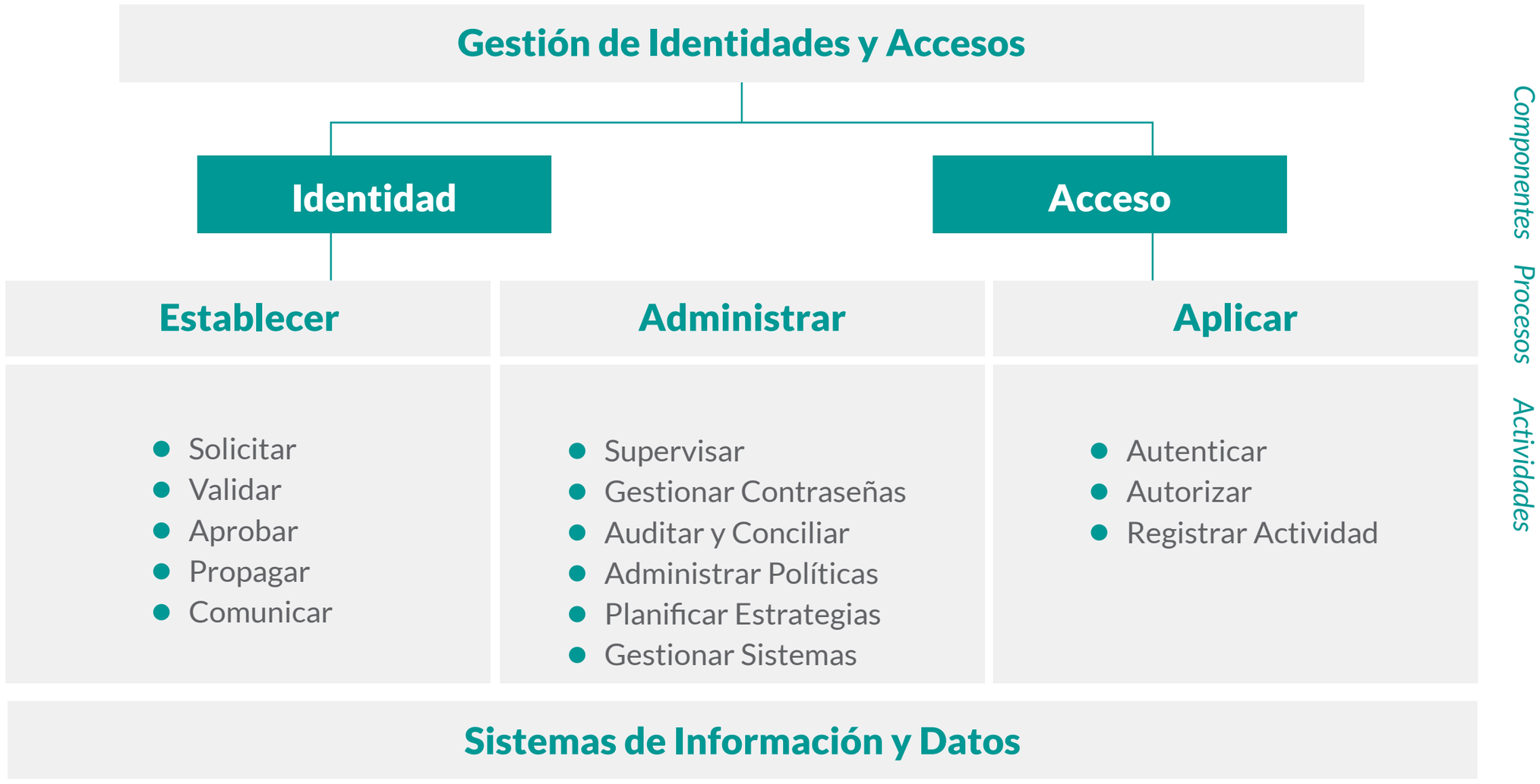


Ilustración n°2. Relaciones Entre los Componentes de IAM y los Conceptos Claves

El proceso de gestión de los accesos e identidades es el siguiente:

01 **Establecimiento**
Se refiere a la creación, cambio, extinción, validación, aprobación, propagación y comunicación de una identidad. Este proceso debe estar regido por una declaración de política específica de la organización, de aplicación universal, que redacta y mantiene el departamento de TI o SIC con aportes de otras unidades de negocio.

02 **Gestión de Identidad**
Debe formar parte de las actividades continuas de la organización. Incluye el establecimiento de una estrategia de IAM, la administración de los cambios en la declaración de política de IAM, el establecimiento de parámetros de identidades y contraseñas, la gestión de sistemas y procesos de IAM manuales o automatizados y las actividades periódicas de supervisión, auditoría, conciliación y preparación de informes respecto de los sistemas de IAM.

03 **Puesta en Marcha**
La puesta en marcha incluye la autenticación, la autorización y el registro de las identidades como se utilizan dentro de los sistemas de TI de la organización. La puesta en vigor de los derechos de acceso principalmente se realiza a través de procesos o mecanismos automatizados

Fuente: GTAG09 - Gestion de Identidades y accesos

1.4 TIPOS DE IDENTIDADES Y SUS RIESGOS

Las identidades y accesos no corresponden únicamente a humanos, si no que diferentes entidades de diversas naturalezas requieren acceder e interactuar con los sistemas de información (SI). Cada una de estas interacciones presenta características particular y escenarios de riesgos que la función de SIC deberá comprender y gestionar. Los tipos de identidades más frecuentes son:

TIPO DE IDENTIDAD	DESCRIPCIÓN	RIESGO DE NO CONTROLAR
Identidades Humanas	**Usuarios individuales, como empleados, contratistas, socios y clientes.**	**Acceso no autorizado a información confidencial, fraude, pérdida de datos y posibles violaciones de cumplimiento.**
Cuentas de Servicio	**Cuentas utilizadas por aplicaciones o sistemas para interactuar entre sí.**	**Cuentas utilizadas por aplicaciones o sistemas para interactuar entre sí.**
Identidades de Máquinas	**Dispositivos como servidores, computadoras, dispositivos móviles y otros dispositivos conectados.**	**Ataques a la infraestructura, propagación de malware y posibles interrupciones en la operación.**
Identidades No Humanas	**Otros tipos de identidades que no son ni humanas ni máquinas, como APIs, tokens y certificados.**	**Acceso no autorizado a sistemas y datos, interrupción de flujos de trabajo automatizados y posibles violaciones de**
Identidades Temporales	**Se otorgan por un período limitado, como para contratistas o visitantes temporales.**	**Acceso prolongado más allá del período requerido, acceso no autorizado a áreas restringidas y potencial exposición de información confidencial.**
Identidades Privilegiadas	**Usuarios con niveles elevados de acceso, como administradores de sistemas o bases de datos**	**Cambios no autorizados en sistemas y configuraciones, acceso no autorizado a datos sensibles y potencial para causar daños significativos.**

1.5 CAMBIOS DE ROLES Y ACCESO: EL VÍNCULO CON LA GESTIÓN DE PERSONAS

Los cambios en las habilitaciones de acceso e identidades están estrechamente vinculados con el proceso de gestión de personas. A medida que las personas se unen, se mueven dentro o abandonan una organización, sus necesidades de acceso a la información y a los sistemas cambian. Es esencial que las habilitaciones de acceso se actualicen adecuadamente para reflejar estos cambios y garantizar la seguridad y el cumplimiento.

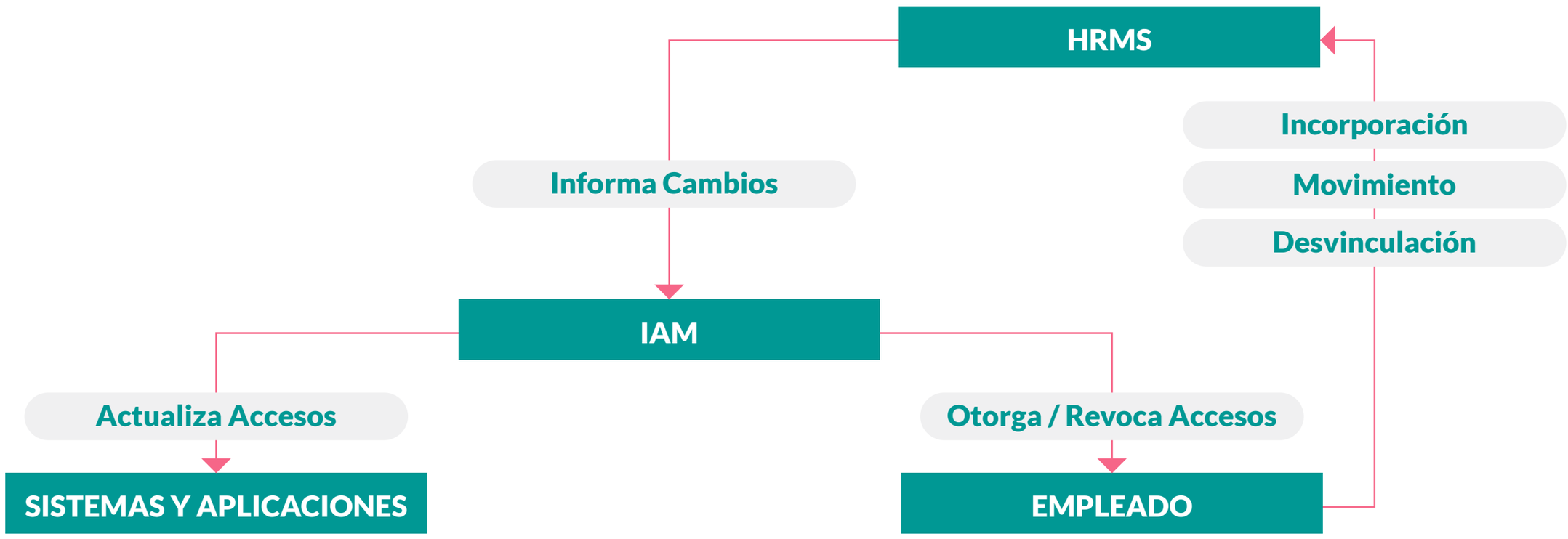


Ilustración n°3. Vínculo con la Gestión de Personas. Fuente: Elaboración Propia

Incorporación

Cuando un nuevo empleado se une a la organización, necesita acceso a ciertos sistemas y datos para realizar su trabajo. El proceso de gestión de personas debe comunicar la incorporación de este nuevo empleado al sistema de gestión de identidades y accesos (IAM) para que se le otorguen las habilitaciones adecuadas.

Movimiento Interno

Si un empleado cambia de rol o departamento, sus necesidades de acceso también pueden cambiar. Por ejemplo, un empleado que se traslada del departamento de ventas al departamento de finanzas necesitará acceso a diferentes sistemas.

Desvinculación

Cuando un empleado abandona la organización, es crucial que su acceso a todos los sistemas y datos de la empresa se revoque inmediatamente para prevenir posibles amenazas de seguridad.

Interfaces de Comunicación Comunes:

01 **Sistema de Gestión de Recursos Humanos (HRMS)**
Principal fuente de verdad para el estado de empleo de una persona. Debe comunicarse con el sistema IAM para informar sobre las incorporaciones, movimientos y desvinculaciones.

02 **Sistema de Gestión de Identidades y Accesos (IAM)**
Recibe información del sistema HRMS y realiza los cambios necesarios en las habilitaciones de acceso de un individuo.

03 **Sistemas y Aplicaciones de la Organización**
Estos sistemas deben estar integrados con el sistema IAM para recibir actualizaciones sobre quién debe tener acceso a qué información y sistemas.

Es importante comprender en profundidad el proceso de Gestión de Personas.
Te recomendamos leer la Guía Metodológica N°3 “Seguridad en Recursos Humanos”.

Capítulo 2

ALCANCES DE LA GESTIÓN DE ACCESO E IDENTIDADES

2.1 GOBERNANZA DE LA GESTIÓN DE ACCESOS E IDENTIDADES

La gobernanza de la identidades, credenciales y accesos es un proceso complejo que va mucho más allá de la función de gobernanza. Implica el compromiso y trabajo en conjunto de la dirección estratégica, la gestión de personas, el personal de TI, control de gestión, función de riesgos, función de cumplimiento, entre otras. Sin embargo, es importante que el auditor conozca el valor habilitante que tiene IAM cuando es trabajado a nivel de práctica de gobierno.

¿Por qué es importante elevar IAM a una práctica de gobierno?

Las organizaciones que dependen de datos y son sensibles a interrupciones en sus sistemas de información, por lo general, han distribuido responsabilidades en diferentes oficiales de alto nivel (CDO, CISO, CFO, Comité de Inversión, Oficiales de Seguridad de la Información, Oficiales de Privacidad, Personal de Seguridad, etc.). ***Al observar IAM como un elemento fundamental en la arquitectura organizacional y como práctica de gobierno, se asegura que las inversiones en proyectos de esta naturaleza se alinean apoyan a los objetivos estratégicos. Por otro lado, es un mecanismo de aprovechar el máximo el potencial de IAM para la minimización de riesgos y la optimización de los procesos de aprovisionamiento de credenciales y permisos.***

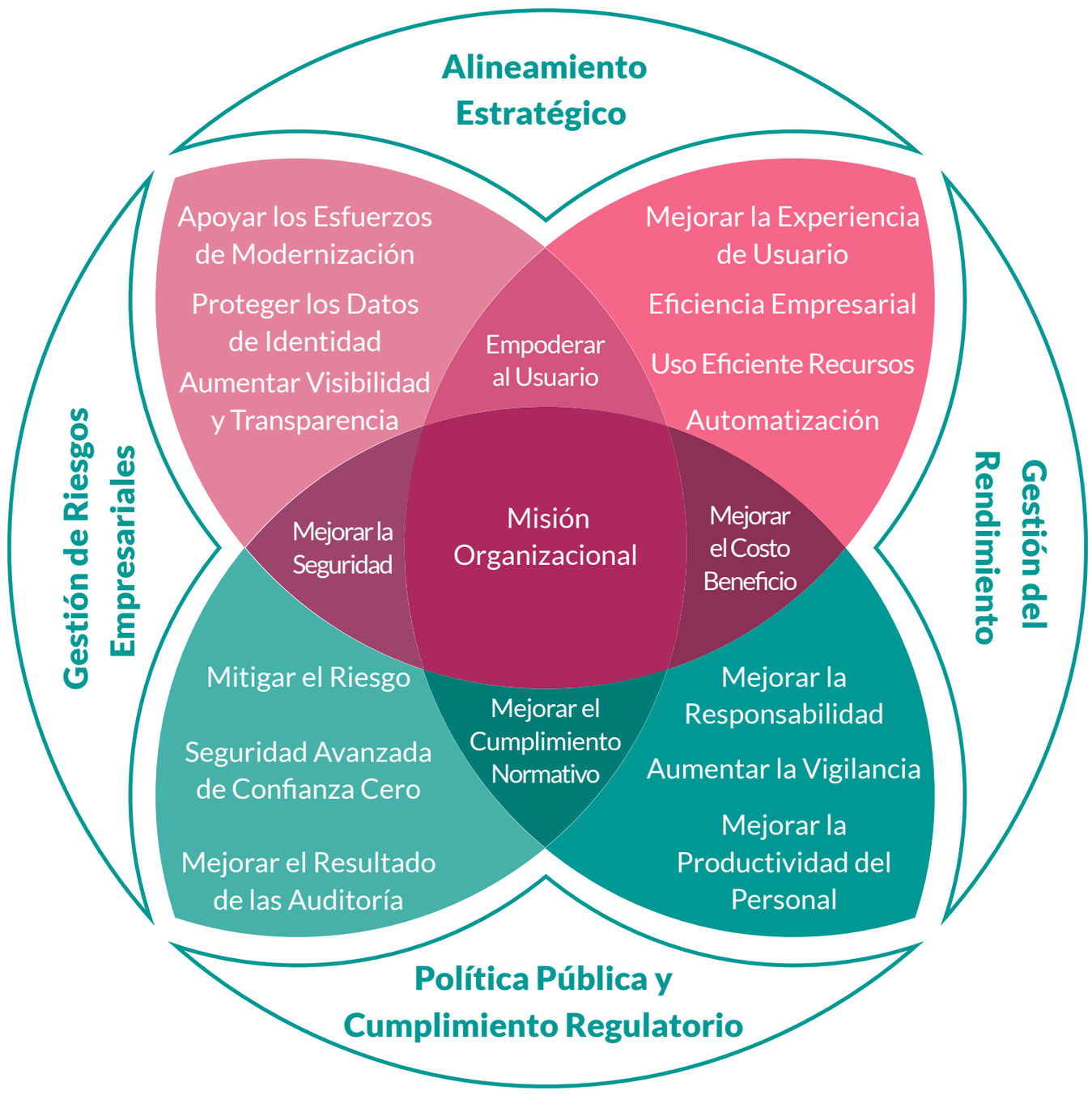


Ilustración n°4. Governance Core Components and Benefits. Fuente: ICAM

Prácticas Relevantes del Auditor Interno:

PRÁCTICAS RELEVANTES	EJEMPLOS DE APLICACIÓN
Revisión de Políticas y Procedimientos	• Asegurarse de que existen políticas y procedimientos escritos y actualizados relacionados con la gestión de identidades y accesos. • Verificar que estas políticas se comunican y se capacita a todo el personal relevante.
Evaluación de Roles y Responsabilidades	• Confirmar que los roles y responsabilidades relacionados con la gestión de accesos e identidades están claramente definidos y asignados.
* **Revisión de Procesos Onboarding y Offboarding**	• Evaluar el proceso de incorporación (Onboarding) para asegurar que los nuevos empleados reciben accesos adecuados basados en su rol. • Revisar el proceso de desvinculación (Offboarding) para confirmar que los accesos se revocan de manera oportuna cuando un empleado deja la organización .
Evaluación de Revisiones Periódicas	• Verificar que se realizan revisiones periódicas de los derechos de acceso para asegurarse de que siguen siendo apropiados para el rol del usuario.
Evaluación de Integración con Terceros	• Si la organización utiliza proveedores externos o soluciones en la nube, asegurarse de que existen controles adecuados para gestionar los accesos e identidades en estos entornos.

* ESTE TEMA SE ENCUENTRA DESARROLLADO EN PROFUNDIDAD EN LA GASIC N°3 "SEGURIDAD EN LOS RECURSOS HUMANOS"

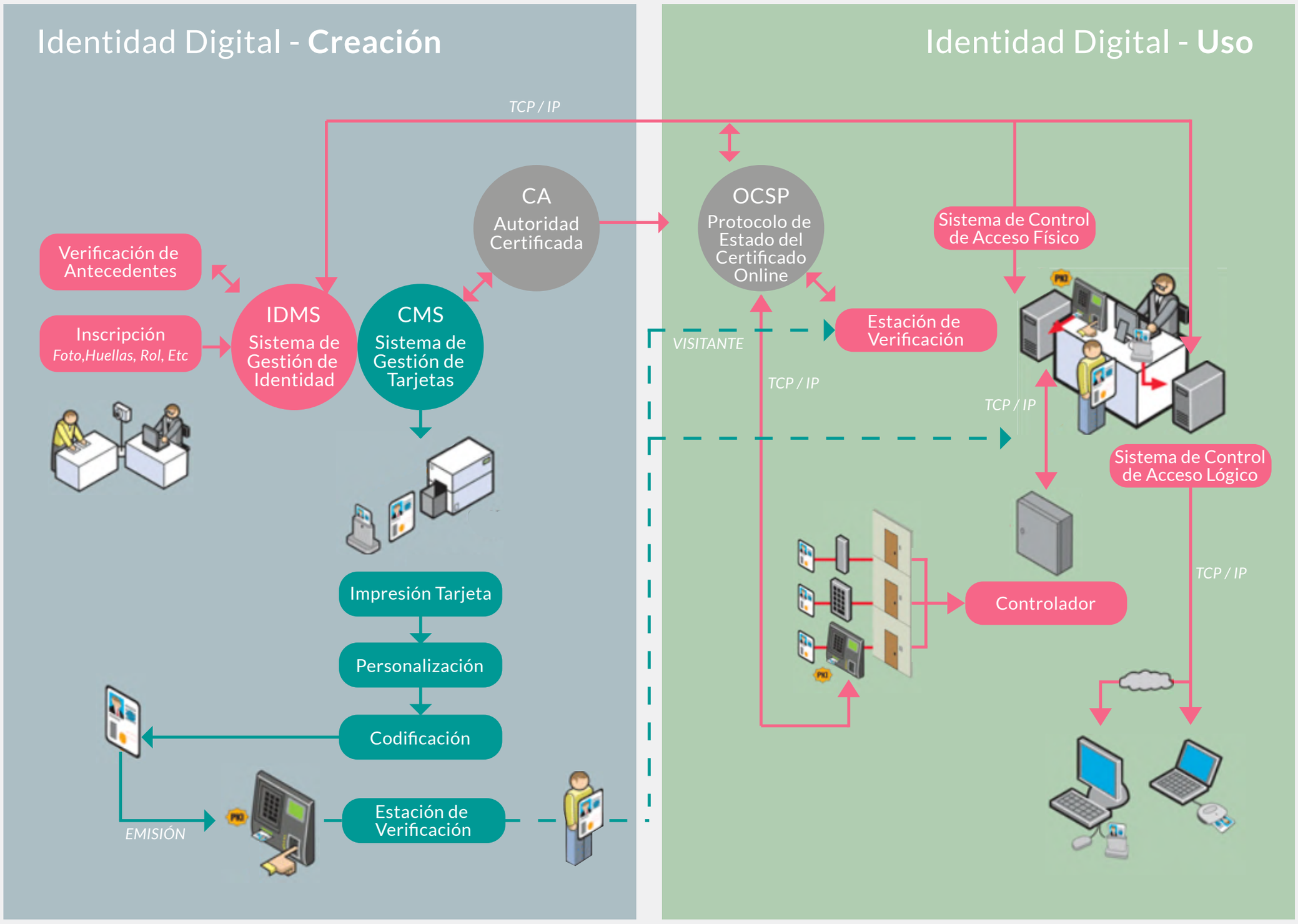
2.2 GESTIÓN DEL ACCESO FÍSICO (PACS)

Un sistema de control de acceso físico (PACS) otorga acceso a los empleados y contratistas que trabajan o visitan un sitio mediante la autenticación electrónica de sus credenciales. Aunque los PACS son sistemas de tecnología de la información, deben diseñarse, implementarse y operarse en cooperación con los equipos de seguridad física para satisfacer con éxito las necesidades de la misión de la agencia.

Fuente: FICAM ID Government

Protección Contra Amenazas Físicas	Evita el acceso no autorizado a instalaciones, centros de datos y áreas restringidas donde se almacena información sensible.
Protección De Robos y Daños	Los dispositivos físicos como servidores, computadoras y medios de almacenamiento pueden ser robados o dañados si no están adecuadamente protegidos.
Integridad de la Información	Asegura que la información no sea alterada o destruida por personal no autorizado.

Ejemplo de un Despliegue de PACS



Tips para el Auditor:

- ***Protocolos de Seguridad:*** *Asegurarse de que existan procedimientos claros para el ingreso y salida de personal y visitantes.*
- ***Sistemas de Monitoreo:*** *Verificar la existencia y funcionamiento de cámaras de seguridad y sistemas de alarma.*
- ***Control de acceso biométrico:*** *Evaluar la implementación de sistemas biométricos como huellas dactilares o reconocimiento facial.*

La siguiente tabla define los componentes PACS comunes:

	COMPONENTE	DESCRIPTOR
1	**Punto de Acceso**	Entrada o barrera física donde un empleado interactúa con el PACS. Ejemplos de puntos de acceso incluyen torniquetes, portones y puertas cerradura.
2	**Credencial PIV**	Los empleados federales utilizan credenciales de Verificación de Identidad Personal (PIV) para acceder físicamente a instalaciones federales y acceder lógicamente a los sistemas de información.
3	**Lector de Credenciales y Teclado**	El lector proporciona energía y lee datos de una credencial PIV. El lector también envía estos datos a un panel de control para autenticar la credencial PIV y solicitar autorización de acceso. Es posible que los empleados y contratistas necesiten ingresar un PIN en el teclado y agregar un dato biométrico, según la clasificación de seguridad y los niveles de riesgo de la instalación.
4	**Lector Biométrico**	Captura datos biométricos (por ejemplo, huellas dactilares o escaneo de iris) y los verifica con los datos biométricos de la credencial PIV.
5	**Panel de Control**	Recibe los datos de las credenciales enviadas por el lector y verifica su presencia en el repositorio de datos del titular de las credenciales. Luego decide y transmite los datos de autorización al servidor de control de acceso y al punto de acceso.
6	**Servidor de Control de Acceso**	Otorga autorización al empleado que solicita acceso (Por ejemplo: Presenta una credencial PIV a un lector). También registra e inscribe a empleados e inscribe y valida credenciales y registra eventos del sistema.
7	**Repositorio de Datos del Titular**	Contiene datos de empleados y privilegios de acceso físico. Los paneles de control utilizan estos datos autorizados para validar los datos de credenciales.
8	**Sistemas Auxiliares**	Las agencias pueden integrar el PACS con sistemas de monitoreo de instalaciones adicionales, como sistemas de vigilancia, sistemas de alarma contra incendios y sistemas de evacuación.

2.3 CONTROL DE ACCESO REMOTO

La forma clásica de realizar pruebas de identidad es que el solicitante proporcione evidencia de su identidad, como presentar un documento de identificación durante una reunión física con un operador del proveedor de servicios.

Es importante subrayar que la prueba de identidad a distancia se produce un paso antes de la identificación y la autenticación, ya que se ocupa de la creación de identidades en un conjunto de circunstancias muy específicas y restrictivas, en particular que la identidad debe estar inequívocamente vinculada a una persona física, lo que no es un requisito para la mayoría de los sistemas de información.

En un mundo físico, el solicitante y el operador deben estar en el mismo lugar al mismo tiempo, un proceso que puede ser complicado, lento y además, la prueba de la validación de la evidencia podría no registrarse adecuadamente, el operador podría no estar debidamente capacitado para realizar la verificación correcta de todos los diferentes tipos de evidencia aceptable, o podría ser manipulado psicológicamente, amenazado, sobornado o convencido de otra manera para validar indebidamente una identidad falsa.

Los métodos para probar la identidad de forma remota proporcionan los medios para identificar a una persona que elimina la necesidad de una presencia física, mejorando así la experiencia del usuario, reduciendo los costos del proveedor de servicios, apoyando el desarrollo de servicios transfronterizos y evitando riesgos innecesarios para la salud.

Fuente: ENISA Remote Identity Proofing

NIST 800-63

El control de acceso remoto es un proceso de prueba de identidad remoto que emplea medidas físicas, técnicas y de procedimiento que brindan suficiente confianza de que la sesión remota puede considerarse equivalente a un proceso de prueba de identidad físico en persona.

Ejemplo de un Mecanismo de Acceso Remoto: VPN

Un claro ejemplo de un mecanismo de acceso remoto, muy utilizado a propósito del contexto de teletrabajo son las VPN. *Las VPN se utilizan para transmitir datos de forma segura y anónima a través de redes públicas. Su funcionamiento consiste en ocultar las direcciones IP de los usuarios y cifrar los datos para que nadie que no esté autorizado a recibirlos pueda leerlos.*

Fuente: AWS Amazon Web Services

- ***Acceso Seguro Desde Cualquier Lugar:*** *Las VPN permiten a los empleados acceder de forma segura a la red corporativa desde ubicaciones remotas.*
- ***Protección Contra Interceptaciones:*** *Las VPN cifran el tráfico, lo que dificulta que los ciberdelincuentes intercepten y descifren la información transmitida.*
- ***Autenticación de Usuarios:*** *Asegura que solo el personal autorizado pueda acceder a la red corporativa de forma remota.*

El acceso remoto seguro no es una tecnología única, sino un grupo de herramientas que, en conjunto, brindan la seguridad que la Entidad necesita cuando los usuarios trabajan desde casa u otras ubicaciones remotas. Entre estos recursos se incluyen:

- **Red Privada Virtual (VPN)**
  Es una red virtual, un túnel seguro construido sobre redes físicas existentes, que proporciona un mecanismo de comunicaciones seguras para los datos e información transmitida entre dos puntos finales. La VPN da acceso al trabajador remoto a diferentes recursos corporativos tales como aplicaciones, servidores de archivos e impresoras.

- **VPN de Sitio a Sitio**
  Es un puente virtual entre las redes de oficinas geográficamente distantes, que les permite conectarse a través de internet para mantener una comunicación segura y privada entre las redes.

- **RPD**
  Es un protocolo desarrollado por Microsoft que permite la comunicación entre una terminal y un servidor Windows en la ejecución de aplicaciones, es decir, permite acceder de forma remota a ordenadores y equipos sin estar físicamente.

- **Firewall**
  Es la parte de un sistema informático o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

- **Encriptación End to End**
  Permite que todo el tráfico de información desde un origen hasta un destino esté totalmente cifrado y autenticado, para que, si alguien captura dicho tráfico, no pueda leer la información que hay en su interior.

- **Inicio de Sesión Único (SSO)**
  Es una forma de iniciar sesión en diferentes aplicaciones usar solo un conjunto de credenciales de inicio de sesión para acceder cómodamente.

- **El acceso a la red de confianza cero (ZTNA)**
  conocido como perímetro definido por software (SDP), es un conjunto de tecnologías y funcionalidades que permiten el acceso seguro de los usuarios remotos a las aplicaciones internas. Funciona con un modelo de confianza adaptable en el que la confianza nunca es implícita y el acceso se concede en función de la necesidad de saber y del acceso menos privilegiado, definido por políticas granulares.

Tips para el auditor:

- ***Revisar Políticas de Acceso Remoto:*** *Asegurarse de que existan políticas claras sobre quién puede acceder de forma remota y qué recursos pueden acceder.*
- ***Evaluar Protocolos de Cifrado:*** *Verificar que se utilicen protocolos de cifrado robustos y actualizados.*
- ***Autenticación de Dos Factores:*** *Recomendar la implementación de la autenticación de dos factores para el acceso remoto.*
- ***Revisar el Estado de los Componentes de Seguridad (Antes Descritos):*** *Verificar su correcto funcionamiento, elementos configurables, procedimientos de revisión y trazabilidad.*

Capítulo 3

ROL DEL AUDITOR INTERNO EN EL PROCESO DE GESTIÓN DE IDENTIDAD Y ACCESOS

3.1 ROL DEL AUDITOR INTERNO

El papel del auditor interno es esencial, es este el profesional que se encuentra en la tercera lína 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 Identidad y acceso son:

Verificar la Existencia de Políticas y Procedimientos
Asegurarse de que existen políticas y procedimientos documentados y actualizados relacionados con la gestión de accesos e identidades. Estos deben ser coherentes con los objetivos y requisitos de seguridad de la organización.

Evaluación de la Implementación de Controles
Revisar si los controles de acceso e identidad están implementados adecuadamente y si son efectivos en la prevención de accesos no autorizados.

Revisión de Roles y Responsabilidades
Asegurarse de que los roles y responsabilidades relacionados con la gestión de accesos e identidades estén claramente definidos y asignados.

Verificación de la Autenticación y Autorización
Evaluar los mecanismos de autenticación y autorización para garantizar que sean robustos y adecuados para el nivel de riesgo asociado.

Revisión de Registros y Monitoreo
Analizar los registros de acceso para detectar cualquier actividad inusual o no autorizada y asegurarse de que existen mecanismos de monitoreo en tiempo real.

Evaluación de la Gestión de Credenciales
Verificar cómo se crean, distribuyen, renuevan y revocan las credenciales. Esto incluye contraseñas, tokens y otros medios de autenticación.

Verificar la Existencia de Políticas y Procedimientos
Asegurarse de que existen políticas y procedimientos documentados y actualizados relacionados con la gestión de accesos e identidades. Estos deben ser coherentes con los objetivos y requisitos de seguridad de la organización.

Evaluación de la Implementación de Controles
Revisar si los controles de acceso e identidad están implementados adecuadamente y si son efectivos en la prevención de accesos no autorizados.

Revisión de Roles y Responsabilidades
Asegurarse de que los roles y responsabilidades relacionados con la gestión de accesos e identidades estén claramente definidos y asignados.

Verificación de la Autenticación y Autorización
Evaluar los mecanismos de autenticación y autorización para garantizar que sean robustos y adecuados para el nivel de riesgo asociado.

Revisión de Registros y Monitoreo
Analizar los registros de acceso para detectar cualquier actividad inusual o no autorizada y asegurarse de que existen mecanismos de monitoreo en tiempo real.

Evaluación de la Gestión de Credenciales
Verificar cómo se crean, distribuyen, renuevan y revocan las credenciales. Esto incluye contraseñas, tokens y otros medios de autenticación.

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.

Modelo de Madurez:
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:

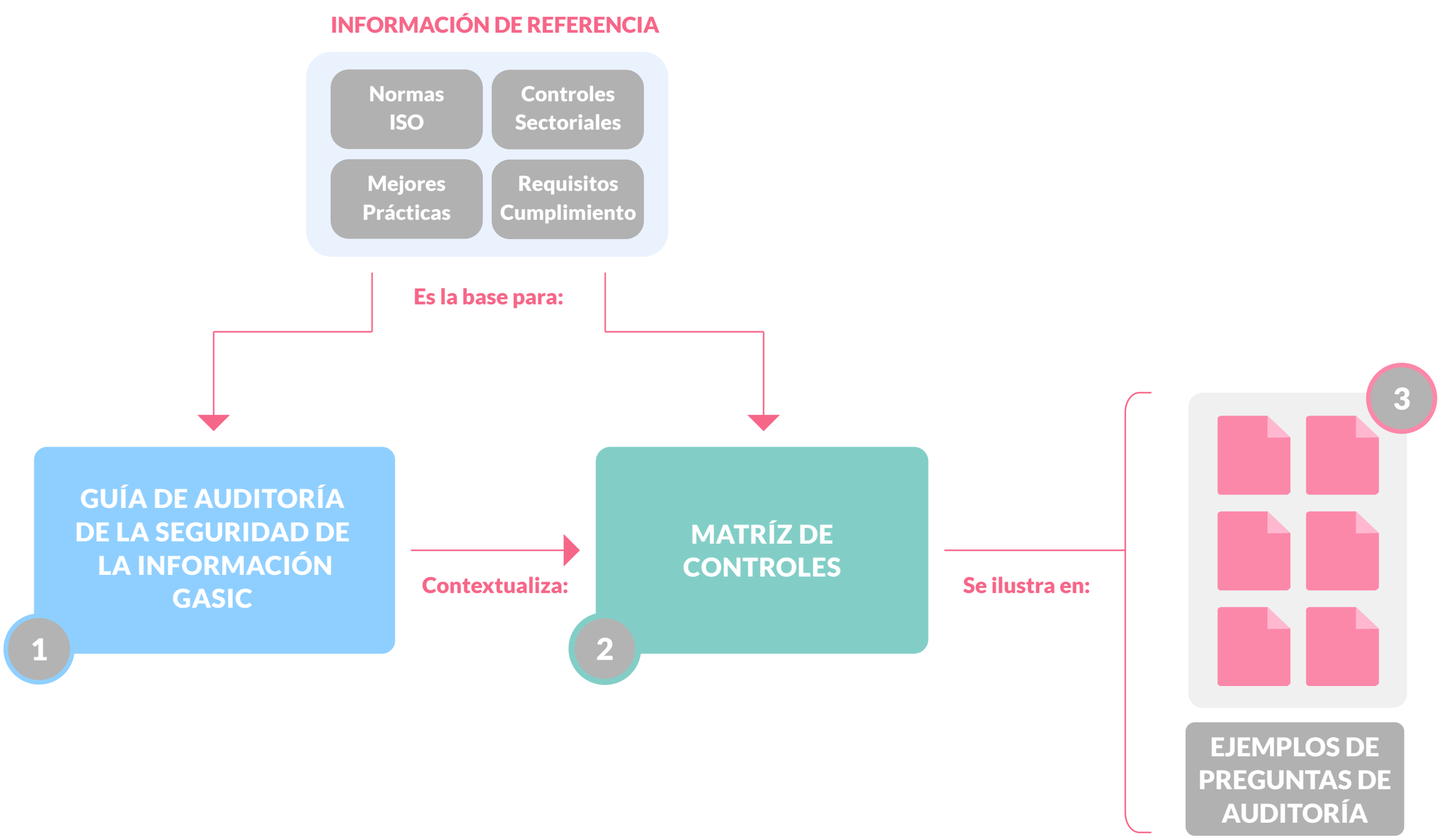


Ilustración n°5. Modo de uso y Estructura Documental GASIC. Fuente: Elaboración Propia

El método de trabajo sugerido es el siguiente:

01 **El auditor interno debe estudiar cada Guía de Auditoría 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.**

NOTA

Los ejemplos de pruebas tienen como propósito ilustrar la forma en la que los requisitos de los marcos que se encuentran en el matriz de controles. El auditor puede elegir utilizar un conjunto de estos ejemplos o diseñar sus propias pruebas para evaluar el nivel de cumplimiento de cada control.

En ningun caso, los ejemplos pretenden ser una lista completa; recuerde, debe contextualizar el ejercicio a la realidad de su organización.

Ejes temáticos

1. Gestión de Identidades y Accesos: Se centra en garantizar el control efectivo de los derechos de acceso y la autenticación segura dentro de una organización. Esto incluye la administración del acceso al código fuente, la gestión de cuentas y credenciales, la implementación de controles para el uso de aplicaciones y programas de utilidad, y el aseguramiento del acceso privilegiado.

	CONTROL	DESCRIPTOR
1	**Acceso a Código Fuente**	**Administrar y Gestionar el acceso a codigo fuente de todas las aplicaciones de la organización.**
2	**Cuentas y Credenciales**	**Establecer controles adecuados y medidas de verificación para garantizar el cumplimiento de los objetivos específicos del sistema.**
3	**Uso de Programas de Utilidad y Controles de Aplicaciones**	**Garantizar que el uso de programas de utilidad no dañe el sistema y los controles de aplicaciones para la seguridad de la información.**
4	**Derecho de Acceso y Acceso Privilegiado**	**La organización asegura que los derechos de acceso mínimo y accesos privilegiados a la información y otros activos asociados son restringidos, administrados, proporcionados, revisados, modificados y eliminados de acuerdo con la política específica de la organización y las normas de control de acceso.**
5	**Notificaciones y Bloqueos de Sesión**	**La organización establece notificaciones y controles de bloqueos automáticos de sesión en base eventos predeterminados.**
6	**Mecanismos de Autenticación Segura**	**La organización implementa, gestiona y mantiene mecanismos de autenticación segura.**

2. Políticas y Gobernanza de IAM: se enfoca en establecer un marco sólido para la gestión de acceso e identidad mediante políticas claras y planes de seguridad que reflejen las actividades y procesos relevantes de la organización. Esto incluye garantizar que se desarrollen, documenten y difundan controles de acceso efectivos, así como proporcionar, establecer y revisar atributos de seguridad y privacidad para mantener un entorno seguro y confiable.

	CONTROL	DESCRIPTOR
1	**Politicas de Control de Acceso e Identidad**	**La organización asegura que ha desarrollado, documentado y difundido los controles de acceso e identidad y autenticación a través de políticas o planes de seguridad y que reflejen los procesos y actividades relevantes en la organización.**
2	**Atributos de Seguridad y Privacidad**	**Proporcionar, Establecer y Revisar atributos de Seguridad y Privacidad.**

3. Seguridad Operacional, Control y Seguridad de Accesos: Aborda la implementación de medidas para proteger y gestionar de manera efectiva el acceso a los recursos de la organización. Esto incluye el control de accesos inalámbricos, físicos y remotos, la gestión de la seguridad en los servicios de red, y la supervisión de los controles de acceso a sistemas.

	CONTROL	DESCRIPTOR
1	**Acceso Inalámbrico**	**Administrar y controlar lo accesos inalambricos, dispositivos moviles, sistemas externos e Intercambio de Información.**
2	**Acceso Fisico**	**La organización administra, controla, monitorea y administra el acceso físico a los activos de información.**
3	**Acceso Remoto**	**La organización establece un procedimiento y controles para gestionar el Acceso Remoto.**
4	**Uso de los Servicios de Red**	**La organización garantiza la seguridad en el uso de los servicios de red.**
5	**Control de Acceso a Sistemas**	**La organización implementa, gestiona y mantiene controles de acceso a los sistemas.**