CAIGG

CONSEJO DE AUDITORÍA INTERNA GENERAL DE GOBIERNO

Ministerio Secretaría General de la Presidencia

Guía de Auditoría, Seguridad de la Información y Ciberseguridad N°2

GOBIERNO Y GESTIÓN DE LA CIBERSEGURIDAD

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 °2: Gobierno y Gestión de la Cibersegruidad.

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

INTRODUCCIÓN AL GOBIERNO DE LA CIBERSEGURIDAD

En el mundo cada vez más digitalizado, la ciberseguridad es una preocupación crítica para las organizaciones de todos los tamaños e industrias. A medida que el número y la sofisticación de las amenazas cibernéticas continúan aumentando, las organizaciones deben adoptar prácticas de gobierno efectivas para proteger sus activos digitales y mitigar los riesgos asociados con los ataques cibernéticos. Este documento proporciona una visión general de la gobernanza de la ciberseguridad, incluidos sus principales objetivos, características clave, roles, responsabilidades y riesgos asociados. En esta guía se presenta el papel del gobierno de la seguridad de la información en la protección de los activos de la organización y la mitigación de los riesgos cibernéticos, así como los principios clave y las mejores prácticas que deben seguirse al auditar una gobernanza efectiva de la ciberseguridad.

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.

El Gobierno de la Ciberseguridad

El Gobierno de la Ciberseguridad se refiere al liderazgo y definición de los sistema de procesos, políticas y controles establecidos por una organización para garantizar la continuidad del negocio, a través de la protección de la confidencialidad, integridad y disponibilidad de sus activos digitales.

El Gobierno de la Ciberseguridad abarca los aspectos estratégicos de la gestión del riesgo de ciberseguridad e incluye la asignación de recursos, el desarrollo de políticas y procedimientos, y el establecimiento de una cultura de conciencia y responsabilidad de ciberseguridad. Involucra también el asegurar la correcta gestión de las operaciones de ciberseguridad y sus proyectos a fin de que se encuentren alineados con las necesidades de la organización, su plan estratégico, su misión y su visión.

¿Gobierno de Ciberseguridad versus Gobierno Corporativo?

Es importante aclarar un punto desde el inicio: El Gobierno de la Ciberseguridad es una función del Gobierno Corporativo. En otras palabras, el Gobierno de la Ciberseguridad es una tarea del órgano de gobierno de la institución. Así como hablamos del Gobierno de Ciberseguridad, también podemos hablar del Gobierno de TI o Gobierno de Datos, cada uno con su matiz individual.

En este sentido, podemos definir los principales objetivos del Gobierno de la Ciberseguridad como:

- **Asegurar la entrega de valor de la organización, a través del alineamiento de los procesos, prácticas y controles con la estrategia corporativa de la organización.**
- **Promover una cultura de conciencia y responsabilidad de ciberseguridad en toda la organización.**
- **Mitigar los riesgos asociados con ataques cibernéticos, violaciones de datos y otros incidentes cibernéticos.**
- **Establecer un marco para monitorear, evaluar y mejorar continuamente la postura de ciberseguridad de la organización.**
- **Garantizar el cumplimiento de las leyes, regulaciones y estándares de la industria aplicables.**
- **Proteger los activos de información de la organización, incluidos sus datos, sistemas, redes y aplicaciones.**

En la sección "El Rol del Gobierno de la Ciberseguridad" se explora en mayor profundidad cómo materializar estos puntos.

¿Qué es el alineamiento?

El alineamiento entre la función de ciberseguridad y los objetivos corporativos contempla lo siguiente:

01 La dirección de la organización comprende el potencial y las restricciones de la función de ciberseguridad.

02 La función de ciberseguridad entiende los objetivos y las necesidades estratégicos de la organización.

03 Esta comprensión se aplica y se supervisa en toda la organización a través de una estructura de gobierno y responsabilidades apropiadas

1.1 CARACTERÍSTICAS CLAVE DE LA GOBERNANZA DE LA CIBERSEGURIDAD

El Gobierno de la Ciberseguridad tiene ciertas características propias, que pueden ser diferentes al ejercicio de gobernanza en otras funciones organizacionales. Si bien comparte algunas características comunes, como un enfoque en la rendición de cuentas, la gestión de riesgos y la alineación estratégica, también tiene varias características únicas:

- **La gobernanza de la ciberseguridad debe ser proactiva, lo que significa que busca asegurar que la organización cuenta con las capacidades para anticiparse y abordar posibles amenazas y vulnerabilidades antes de que puedan ser explotadas por actores maliciosos (o adversarios).**
- **Es dinámico, se adapta al panorama de amenazas en rápida evolución y a las necesidades y prioridades cambiantes de la organización.**
- **La gobernanza de la ciberseguridad es independiente de la tecnología, centrándose en la gestión efectiva de los riesgos de seguridad de la información en lugar de las herramientas y tecnologías específicas utilizadas para lograr el objetivo.**
- **Se basa en el riesgo y en la contribución de valor a los objetivos de la organización, priorizando la protección de los activos más criticos y necesarios para el cumplimiento de la misión organizacional**

¿Gobierno o Gobernanza?

El gobierno se refiere a la autoridad y control de un sistema o entidad, ya sea una empresa, organización o gobierno. *El gobierno se enfoca en establecer políticas, procedimientos y prácticas para guiar y controlar el comportamiento de la entidad. Por otro lado,* ***la gobernanza se refiere al acto de ejercer el gobierno.***

1.2 MARCOS, ESTÁNDARES Y BUENAS 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 gobernanza efectiva de la ciberseguridad. 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.**
ISO 38500 – Gobierno Corporativo de las Tecnologías de la Información	**Esta norma proporciona un marco de alto nivel para la gobernanza efectiva de las tecnologías de la información y establece principios de gobierno que aseguran el éxito en el ejercicio de la gobernanza.**
Guía Global de Auditoría Tecnológica (GTAG) 17	**Proporciona orientación sobre la auditoría de los procesos de gobernanza y gestión de riesgos de ciberseguridad.**
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.**
ISO 27001 :2022	**Establece los requisitos para la implementación del Sistema de Gestión de Seguridad de la Información, así como las mejores prácticas en su anexo, la norma ISO 27002.**

1.3 EL ROL DEL GOBIERNO DE LA CIBERSEGURIDAD

Previamente hemos definido que El Gobierno de la Ciberseguridad desempeña un papel crucial en la protección de los activos de la organización y la mitigación de los riesgos cibernéticos. Para que esto sea posible, es necesario que sea capaz de realizar ciertas tareas, lo que se denomina "el rol del Gobierno de la Ciberseguridad". Este rol consiste en:

01

Establecer una visión y estrategia claras para la ciberseguridad

La gobernanza efectiva de la ciberseguridad comienza con el desarrollo de un plan director de seguridad que describa los objetivos, prioridades y resultados deseados de la organización relacionados con la seguridad de la información. Este plan sirve como una hoja de ruta para los esfuerzos de la organización y garantiza que todas las actividades estén alineadas con sus metas y objetivos generales.

02

Definir roles y responsabilidades

Implica definir claramente los roles y responsabilidades de las diversas partes interesadas dentro de la organización, incluida la junta directiva, la alta gerencia, las responsabilidades específicas de ciberseguridad, el personal de TI y otros empleados. Esto ayuda a garantizar que todos entiendan su papel en los procesos y controles de ciberseguridad de la organización y sean responsables de sus acciones.

03

Desarrollo de políticas

La gobernanza de la ciberseguridad requiere el desarrollo de un conjunto de políticas que describan las expectativas y requisitos de la organización relacionados con la ciberseguridad, los cuales deben ser evaluados periódicamente para reflejar los cambios en el entorno interno y externo de la organización, el panorama de amenazas, y las necesidades y prioridades de las partes interesadas clave de la organización.

04

Asignación de recursos

Asignar los recursos necesarios, incluidos el presupuesto, el personal y la tecnología para respaldar los esfuerzos de ciberseguridad de la organización. Esto garantiza que tenga las herramientas y capacidades para proteger sus activos de información críticos, responder a posibles amenazas y asegurar la continuidad operacional.

05

Establecer una cultura de conciencia de ciberseguridad

El gobierno de la ciberseguridad desempeña un papel fundamental en la promoción de una cultura de conciencia y responsabilidad en toda la organización. Para ello, debe proporcionar capacitación y educación continuas para los empleados, así como promover una cultura de apertura y colaboración cuando se trata de abordar los desafíos de ciberseguridad.

06

Implementación de mecanismos de monitoreo y supervisión

Establecer mecanismos de monitoreo y presentación de informes para rastrear el progreso de la organización en el logro de sus objetivos de ciberseguridad e identificar áreas donde se pueden necesitar mejoras.

Fuente: COBIT 2019.

1.4 MODELO DE GOBIERNO ISO 38500

El marco ISO 38500 proporciona una guía para la gobernanza de TI en las organizaciones, centrándose en los principios y componentes clave que permiten una gobernanza eficaz. A continuación, exploraremos una visión general de los principios y componentes del marco ISO 38500, específicamente en las funciones definidas: "Dirigir", "Evaluar" y "Monitorear". Se analizará cómo se llevan a cabo estas funciones en el contexto particular de la ciberseguridad, y su importancia para una gobernanza efectiva. Además, se examinarán las interacciones entre la gobernanza de la seguridad de la información de una organización y las presiones y necesidades del negocio.

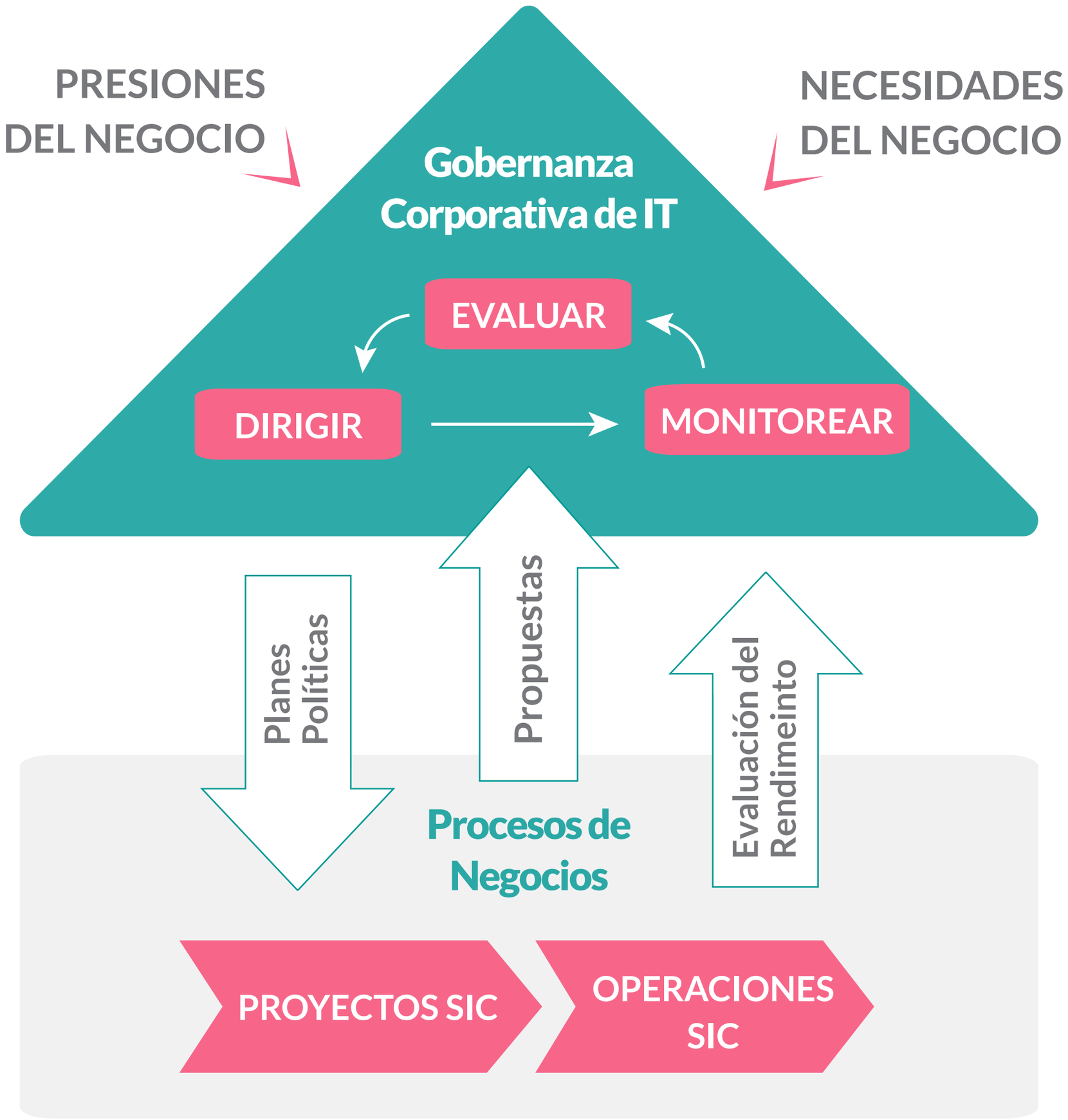


Ilustración n°1.

A pesar de que el marco ISO 38500 está enfocado en el Gobierno de las TI, sus principios y dinámicas son aplicables al contexto de Seguridad de la Información y Ciberseguridad. Mas adelante, veremos cómo se vinculan sus funciones con el contexto específico de ciber riesgos.

Funciones del Gobierno según ISO 38500

DIRIGIR

La función de dirigir implica que la alta dirección y el órgano de gobierno establezcan la dirección general y las prioridades de ciberseguridad en la organización. Esto incluye actividades como: La definición de políticas, la asignación de responsabilidades y la garantía de que se siguen las prácticas de gobernanza adecuadas. La función de dirigir ayuda a garantizar que la gobernanza de seguridad de la información esté alineada con la estrategia y los objetivos generales del negocio.

EVALUAR

La función de evaluar implica examinar de manera regular y sistemática los proyectos, inversiones y operaciones de ciberseguridad de la organización. Esto incluye actividades como: La evaluación de riesgos, el desempeño y la efectividad de las políticas y prácticas de gobernanza. La función de evaluar ayuda a garantizar que las inversiones en seguridad estén optimizadas para apoyar los resultados empresariales y que se gestionen de manera efectiva los ciber riesgos.

MONITOREAR

La función de monitorear implica supervisar de manera continua el desempeño y la conformidad de la organización con las políticas y prácticas de gobernanza de ciberseguridad. Esto incluye la identificación de áreas de mejora y la implementación de acciones correctivas según sea necesario. La función de monitorear ayuda a garantizar que el gobierno de ciberseguridad se mantenga efectivo y que se aborden de manera proactiva los problemas y desafíos que puedan surgir.

Fuente: ISO 38500 - Principios de Gobierno Corporativo de las TI

Interacción entre la Gobernanza de Ciberseguridad y las Necesidades del Negocio

El marco ISO 38500 reconoce que la gobernanza de TI (y por extensión, la función de ciberseguridad) no pueden abordarse de manera aislada, sino que deben estar integrada en la gobernanza general de la organización. Esto implica que las presiones y necesidades del negocio deben tenerse en cuenta al establecer y mantener la gobernanza de TI/ciberseguridad.

El marco ISO 38500 ayuda a abordar estos desafíos al proporcionar una guía para alinear la gobernanza de ciberseguridad con la estrategia y los objetivos empresariales generales, así como para garantizar que las inversiones en seguridad de la información estén optimizadas para apoyar los resultados empresariales.

Este estándar también reconoce que la gobernanza de ciberseguridad es un proceso continuo de mejora y adaptación, y que las organizaciones deben ser capaces de responder a los cambios en el entorno empresarial y tecnológico. Esto implica que la gobernanza de seguridad debe ser flexible y adaptable, y que las organizaciones deben estar preparadas para revisar y ajustar sus políticas y prácticas de gobernanza a medida que evolucionan sus necesidades y objetivos.

1.5 INTEGRACIÓN DEL MODELO ISO 38500 Y EL ROL DEL GOBIERNO DE CIBERSEGURIDAD

Para ejemplificar los conceptos revisados anteriormente, se entrega a continuación una tabla que relaciona las actividades contenidas en el rol del gobierno de ciberseguridad, la función del gobierno al que tributan y cómo se expresan en el contexto particular de la seguridad de la información.

ACTIVIDAD	FUNCIÓN DEL GOBIERNO	APLICACIÓN A CIBERSEGURIDAD	EJEMPLOS
Establecer una visión y estrategia claras para la ciberseguridad	Dirigir	La alta dirección y el consejo de administración definen la dirección y las prioridades en ciberseguridad alineadas con la estrategia del negocio.	Establecimiento de objetivos de ciberseguridad a corto, medio y largo plazo, identificación de las principales áreas de riesgo y priorización de iniciativas de ciberseguridad.
Definir roles y responsabilidades	Dirigir	Se asignan responsabilidades y autoridades específicas en relación con la ciberseguridad a individuos o equipos dentro de la organización.	Definición del rol del CISO, creación de un equipo de respuesta a incidentes de seguridad (CSIRT), asignación de responsabilidades en ciberseguridad a los líderes de departamento.
Desarrollo de políticas y procedimientos	Dirigir	Se desarrollan y establecen políticas y procedimientos formales de ciberseguridad que guían las acciones y decisiones de la organización.	Política de gestión de contraseñas, política de uso aceptable, procedimientos para la gestión de incidentes de seguridad.
Asignación de recursos	Dirigir	Se asignan recursos humanos, tecnológicos y financieros para implementar y mantener las políticas y procedimientos de ciberseguridad.	Contratación de personal de seguridad, adquisición de tecnologías de protección, asignación de presupuesto para capacitación en ciberseguridad.
Establecer una cultura de conciencia de ciberseguridad	Dirigir	Se fomenta una cultura organizacional en la que todos los empleados comprendan y valoren la importancia de la ciberseguridad.	Programas de capacitación y concientización en ciberseguridad, comunicación regular sobre temas de ciberseguridad, promoción de buenas prácticas de seguridad.
Implementación de mecanismos de monitoreo y presentación de informes	Evaluar y Monitorear	Se implementan sistemas de monitoreo y presentación de informes para evaluar y supervisar el desempeño de la organización en ciberseguridad.	Establecimiento de indicadores clave de rendimiento (KPIs) en ciberseguridad, implementación de herramientas de monitoreo, informes periódicos al

Fuente: Elaboración propia.

1.6 ROLES Y RESPONSABILIDADES EN EL GOBIERNO DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Una gobernanza de ciberseguridad eficaz requiere un claro entendimiento de los roles y responsabilidades de los diferentes actores dentro de una organización. En este punto ofrecemos una visión general de los principales roles y responsabilidades involucrados en el ejercicio de la gobernanza de ciberseguridad y la dinámica de su relación según el modelo de tres líneas de defensa.

Liderazgo Estratégico y el Consejo de Administración

El liderazgo estratégico, incluyendo al Consejo de Administración, juega un papel crucial en la gobernanza de ciberseguridad al establecer la dirección y estrategia generales para los esfuerzos de ciberseguridad de la organización. Son responsables de garantizar que la postura de ciberseguridad de la organización se alinee con su estrategia empresarial y objetivos generales, según lo recomendado por normas como ISO 38500 y COBIT.

Los roles y responsabilidades específicos del Consejo de Administración en la gestión de riesgos de ciberseguridad y garantizar una gobernanza de ciberseguridad eficaz incluyen:

01	**Definir el apetito y los niveles de tolerancia al riesgo de la organización en relación con los riesgos de ciberseguridad.**
02	**Aprobar la estrategia, políticas y presupuesto de ciberseguridad de la organización.**
03	**Asegurar que la organización cuente con los recursos necesarios, incluyendo personal y tecnología, para implementar su estrategia de ciberseguridad de manera efectiva.**
04	**Supervisar la postura de ciberseguridad y los esfuerzos de gestión de riesgos de la organización, asegurando que estén alineados con la estrategia y objetivos generales de la organización.**
05	**Definir las responsabilidades del CISO y otros actores relevantes sobre el desempeño en ciberseguridad de la organización.**

Fuente: COBIT 2019.

El Director de Seguridad de la Información (CISO)

El CISO es una figura clave en la gobernanza de ciberseguridad, responsable de supervisar los esfuerzos de ciberseguridad de la organización y asegurar que se alineen con su estrategia general y objetivos. Los roles y responsabilidades específicos del CISO incluyen:

01	**Desarrollar la estrategia, políticas y procedimientos de ciberseguridad de la organización, en colaboración con otros actores.**
02	**Asegurar que los esfuerzos de ciberseguridad de la organización estén alineados con su estrategia y objetivos generales, y que cumplan con el apetito y niveles de tolerancia al riesgo de la organización.**
03	**Supervisar la implementación de la estrategia de ciberseguridad de la organización, incluyendo la asignación de recursos**

Comités

Los comités estratégicos y ejecutivos de TI, así como el comité del SGSI (Sistema de Gestión de Seguridad de la Información), son estructuras de gobernanza que ayudan a una organización a gestionar y supervisar sus iniciativas de ciberseguridad y seguridad de la información.

Estos comités desempeñan un papel importante en la gobernanza y gestión de la ciberseguridad y la seguridad de la información, asegurando que las organizaciones adopten un enfoque estructurado y coherente para proteger sus activos digitales y reducir los riesgos asociados. Al trabajar juntos, estos comités pueden proporcionar una supervisión eficaz y garantizar la implementación adecuada de las iniciativas de ciberseguridad en toda la organización.

COMITÉ	DESCRIPCIÓN	RELACIÓN CON LA CIBERSEGURIDAD Y LA SEGURIDAD DE LA INFORMACIÓN
Comité Estratégico de TI	Este comité es responsable de la supervisión y dirección de las estrategias y políticas de TI a nivel organizacional.	Se encarga de asegurar que las estrategias y políticas de TI estén alineadas con los objetivos de ciberseguridad y seguridad de la información, y que se aborden los riesgos relacionados.
Comité Ejecutivo de TI	Este comité es responsable de la implementación y gestión de las iniciativas y proyectos de TI a nivel operacional.	Se encarga de garantizar que los proyectos y actividades de TI cumplan con los requisitos de ciberseguridad y seguridad de la información, y de monitorear y gestionar los riesgos relacionados.
Comité del SGSI	Este comité es responsable de la supervisión, dirección y mejora continua del Sistema de Gestión de Seguridad de la Información en la organización.	Se encarga de garantizar que el SGSI esté adecuadamente implementado y mantenido, y que las actividades de ciberseguridad y seguridad de la información estén en línea con los objetivos y requisitos del SGSI.

Fuentes: COBIT 2019 e ISO 27001 - Requisitos para la implementación de un SGSI.

Modelo de Tres Líneas de Defensa

Ilustración n°2.

Fuente: El IIA. Documento de posición. Las tres líneas de defensa en la gestión y el control efectivos de riesgos (Altamonte Springs, Florida, EE. UU, Instituto de Auditores Internos, 2013) Adaptado de ECIIA/FERMA Guidance on the 8th EU Company Law Directive, artículo 41.

El modelo de las tres líneas de defensa de la IIA (Instituto de Auditores Internos) es un enfoque ampliamente utilizado para la gestión de riesgos y el control interno en las organizaciones. En este modelo, se establecen tres líneas de defensa que interactúan entre sí para asegurar que los riesgos sean adecuadamente identificados, evaluados y gestionados.

● ***Primera línea de defensa:*** La primera línea de defensa está compuesta por la gestión y el personal operativo, que son responsables de la identificación y gestión de los riesgos en sus actividades diarias. Estos individuos son los que toman decisiones y ejecutan acciones para mantener y mejorar los controles internos. **La función de gobierno, en este caso, es establecer políticas y directrices claras, así como proporcionar recursos y apoyo para que la primera línea de defensa pueda llevar a cabo sus responsabilidades de manera efectiva.**

● ***Segunda línea de defensa:*** La segunda línea de defensa incluye funciones especializadas de monitoreo y supervisión, como la gestión de riesgos, la gestión de la calidad y la función de cumplimiento. Estas áreas son responsables de supervisar y asegurar que la primera línea de defensa esté cumpliendo con las políticas y directrices establecidas por el gobierno. **La función de gobierno en este nivel es garantizar que exista una estructura adecuada y recursos suficientes para llevar a cabo la supervisión y el monitoreo de la segunda línea de defensa.**

● ***Tercera línea de defensa:*** La tercera línea de defensa es la función de auditoría interna, que proporciona una evaluación independiente y objetiva de la eficacia de los controles internos, la gestión de riesgos y la gobernanza en la organización. **La función de gobierno en esta etapa es garantizar la independencia y objetividad de la auditoría interna, proporcionar apoyo y recursos adecuados y asegurar que las recomendaciones de la auditoría interna sean abordadas y aplicadas de manera oportuna.**

El Gobierno de Ciberseguridad en el modelo de las tres líneas de defensa interactúa con cada línea de defensa al establecer políticas y directrices claras, proporcionar apoyo y recursos y garantizar una supervisión y monitoreo adecuados. El gobierno también juega un papel fundamental en mantener la independencia y objetividad de la función de auditoría interna y en asegurar que las recomendaciones de la auditoría interna sean abordadas y aplicadas de manera oportuna. Esta interacción entre el gobierno y las líneas de defensa ayuda a las organizaciones a gestionar de manera efectiva los riesgos y a mantener un control interno sólido.

1.7 LOS PRINCIPIOS DE GOBIERNO

Por último, y no menos importante, la norma ISO38500 establece seis "principios de gobierno", que buscan establecer el buen gobierno corporativo de las TI, que es extensible en este caso para el gobierno de seguridad de la información y ciberseguridad. Estos principios son aplicables a la mayoría de las organizaciones y expresan el comportamiento deseado a la hora de tomar decisiones. El cumplimiento de estos principios es responsabilidad de la dirección de la organización.

A continuación se presentan los seis principios de gobierno, enfocándolos específicamente a Seguridad de la Información y Ciberseguridad:

01 Principio de Responsabilidad

Este principio establece que la alta dirección debe asumir la responsabilidad de garantizar que los procesos de seguridad de la información se utilicen de manera efectiva y eficiente. Esto implica establecer políticas, asignar responsabilidades y garantizar la supervisión de las actividades de ciberseguridad.

02 Principio de Estrategia

La organización debe alinear su estrategia de seguridad de la información con los objetivos y metas corporativos. Esto significa que la tecnología, procesos y controles de seguridad deben apoyar y mejorar los procesos comerciales, y no simplemente existir como una función separada.

03 Principio de Adquisición

La adquisición de tecnologías y recursos asociados a la seguridad de la información debe estar en línea con la estrategia de la organización, asegurando que los recursos y soluciones tecnológicas seleccionadas sean apropiados y rentables.

04 Principio de Desempeño

Las organizaciones deben medir y monitorear el desempeño de la función de ciberseguridad. Esto incluye la evaluación del rendimiento, la disponibilidad y la calidad de las soluciones tecnológicas, así como su impacto en los resultados comerciales.

05 Principio de Conformidad

Este principio destaca la importancia de cumplir con las leyes, regulaciones y políticas aplicables en relación con la gestión de seguridad de la información. Las organizaciones deben asegurarse de que sus prácticas de seguridad estén diseñadas y operadas de acuerdo con los requisitos legales y reglamentarios.

06 Principio de Comportamiento Humano

El último principio reconoce que las personas son fundamentales para el éxito de la función de seguridad de la información. Las organizaciones deben promover una cultura que valore y apoye el uso ético y responsable de la tecnología, además de proporcionar capacitación y recursos para garantizar que los empleados comprendan y sigan las políticas y procedimientos de ciberseguridad y seguridad de la información.

Se puede concluir entonces, que los Principios de Gobierno son lo que, últimamente se materializarán en las funciones del gobierno de ciberseguridad en la organización. Muchos de estos principios se pueden observar directamente en el rol del gobierno (ver punto 1.3), sin embargo, todos deben ser correctamente evaluados tanto a nivel de estrategia como su despliegue en niveles tácticos y en las acciones del día al día.

Fuente: COBIT 2019.

Capítulo 2

RIESGOS ASOCIADOS AL GOBIERNO DE LA SEGURIDAD DE LA INFORMACIÓN

Capítulo 2

RIESGOS ASOCIADOS AL GOBIERNO DE LA SEGURIDAD DE LA INFORMACIÓN

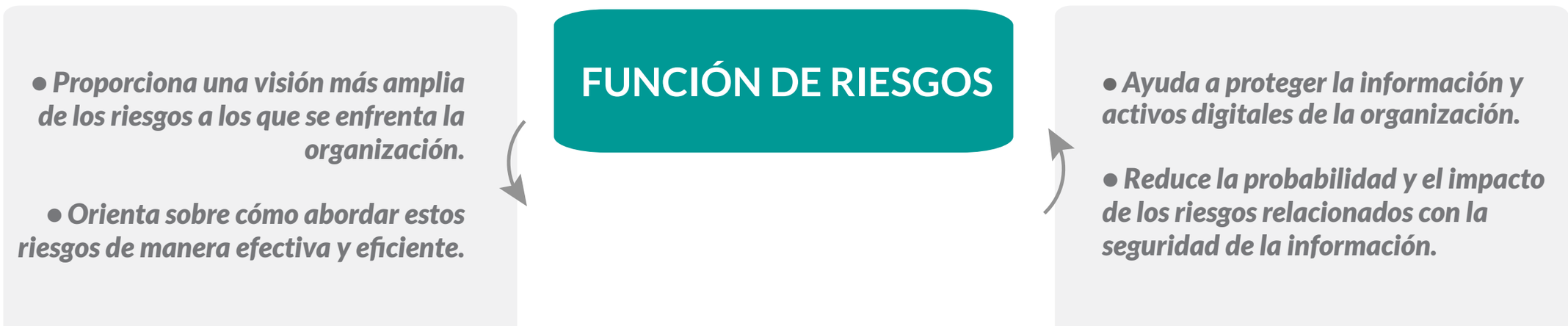
La función de riesgos guarda estrecha relación con el gobierno de la ciberseguridad; este ultimo debe proveer los recursos y los lineamientos necesarios para que riesgos sea capaz de proveer un nivel de confianza adecuado en la continuidad de las operaciones del negocio.

Función de Riesgos en las organizaciones

La función de riesgos es responsable de la identificación, evaluación y gestión de los riesgos que pueden afectar a la organización en su conjunto. Esto incluye riesgos financieros, operativos, regulatorios, reputacionales y de cumplimiento. Una parte fundamental de la gestión de riesgos es establecer un marco adecuado para evaluar y priorizar los riesgos, así como diseñar e implementar estrategias de tratamiento.

Seguridad de la Información y su importancia en la Función de Riesgos

La seguridad de la información es el conjunto de prácticas, procesos y tecnologías diseñadas para proteger la información y los sistemas de TI de las amenazas. Los incidentes de seguridad pueden tener graves consecuencias para la empresa, incluyendo la pérdida de ingresos, la interrupción del negocio (continuidad del negocio), el daño a la reputación y las sanciones legales.



Fuentes: ISO 27005 - Gestión de Riesgos para el SGSI y COSO.

Colaboración entre la función de Riesgos y la Ciberseguridad

Para que las funciones de riesgos y ciberseguridad trabajen juntas de manera efectiva, es importante establecer mecanismos de comunicación y colaboración sólidas entre ambas áreas. Esto puede incluir la creación de comités de riesgos y ciberseguridad, la participación en ejercicios de evaluación de riesgos y la implementación de políticas y procedimientos comunes.

Como se ha revisado hemos revisado en el capítulo anterior, es responsabilidad del gobierno de la organización (y en particular, del ejercicio del gobierno de ciberseguridad) el proveer de los mecanismos y recursos necesarios para asegurar que exista una colaboración real y efectiva entre ambas funciones.

Ilustración n°3: Ejemplo de Integración.

2.1 EXTERNALIZACIÓN DE LA FUNCIÓN DE CIBERSEGURIDAD

La externalización de la función de ciberseguridad se refiere a la contratación de terceros para que proporcionen servicios de ciberseguridad en nombre de una organización. Esta opción puede ofrecer beneficios significativos, como la reducción de costos, la mejora de la experiencia y habilidades de los profesionales de ciberseguridad, y la ampliación de la capacidad de respuesta a las amenazas y vulnerabilidades. Sin embargo, también puede presentar algunos riesgos importantes que deben ser considerados cuidadosamente antes de tomar una decisión.

Riesgos de la externalización de la función de ciberseguridad:

01 Pérdida de Control

Externalizar la función de ciberseguridad puede resultar en una pérdida de control sobre los datos y sistemas de la organización, que se puede materializar en incidentes de seguridad que afecten la privacidad.

02 Falta de Transparencia

No establecer adecuados acuerdos y contratos, puede haber una falta de transparencia en la gestión de la ciberseguridad que deriva a dificultades en la identificación y gestión de ciber riesgos.

03 Dependencia Excesiva

La externalización de la función de ciberseguridad puede dar lugar a una dependencia excesiva del proveedor externo, lo que puede hacer que la organización pierda la capacidad de tomar decisiones críticas sobre la seguridad de la información y ciberseguridad.

04 Falta de Adaptabilidad

Si el proveedor externo de servicios de ciberseguridad no es lo suficientemente flexible, puede haber dificultades para adaptarse a los cambios en los requisitos de la organización.

Fuente: COSO.

El rol del Gobierno de Ciberseguridad en la Externalización de la Ciberseguridad

Es importante que la alta dirección supervise de cerca el proceso de externalización y establezca políticas claras y procesos de gestión de riesgos para garantizar que se identifiquen y gestionen adecuadamente los riesgos asociados con ella. Además, se deben establecer acuerdos y contratos claros y detallados con el proveedor externo de servicios de ciberseguridad para garantizar la transparencia y la efectividad de la gestión de la ciberseguridad. Finalmente, se debe realizar un monitoreo constante y una evaluación regular de la efectividad de los servicios de ciberseguridad proporcionados por el proveedor externo.

2.2 RIESGOS Y CUMPLIMIENTO

Los riesgos de cumplimiento son aquellos que pueden surgir de la no conformidad con leyes, regulaciones y normativas que rigen la seguridad de la información en una organización. Por ejemplo, la violación de la GDPR (Reglamento General de Protección de Datos) en Europa puede resultar en multas significativas, que pueden alcanzar hasta el 4% del volumen de negocios global anual de una empresa.

Cuando hablamos de ***"Requisitos de Cumplimiento"*** *no solo hacemos referencia a lo que estamos obligados de hacer por ley. Además de la ley,* ***constituyen requisitos de cumplimiento todas aquellas responsabilidades que hemos aceptado voluntariamente para con terceras personas y que ahora, se deben cumplir.***

Fuente: ISO 37301 - Sistema de Gestión de Compliance.

Además de las multas monetarias, el incumplimiento puede llevar a sanciones no monetarias, como la pérdida de la reputación de la empresa, la pérdida de la confianza del cliente, e incluso la pérdida de la capacidad de hacer negocios en ciertas jurisdicciones.

Algunos de los riesgos de cumplimiento más comunes son:

Incumplimiento de leyes y regulaciones

Las organizaciones deben cumplir con las leyes y regulaciones de los países y jurisdicciones en las que operan. Estas pueden incluir leyes como la GDPR en Europa, la Ley de Protección de Datos o la CCPA en Estados Unidos. En Chile, existe una incipiente regulación que debe ser considerada, tanto en términos generales como para sectores específicos. El CSIRT de Gobierno mantiene un registro de los decretos de ciberseguridad relevantes, que se encuentran listados al término de este capítulo. El incumplimiento de estas leyes puede resultar en multas y sanciones significativas, así como en daños a la reputación de la organización.

Incumplimiento de normas y estándares de la industria

Las organizaciones pueden estar sujetas a estándares específicos de la industria, como el Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS) para las empresas que procesan pagos con tarjeta de crédito. El incumplimiento de estos estándares puede resultar en multas, sanciones y pérdida de acceso a ciertos mercados o clientes.

Violaciones de contratos y acuerdos de nivel de servicio (SLA)

Las organizaciones pueden tener acuerdos contractuales con sus clientes y proveedores que incluyen requisitos de seguridad de la información y protección de datos. La violación de estos acuerdos puede resultar en consecuencias legales y financieras, así como en la pérdida de confianza de los clientes.

Exposición a litigios

Si una organización no cumple con las leyes y regulaciones de protección de datos o experimenta una violación de datos, puede enfrentar demandas legales de clientes, empleados, socios comerciales y otras partes afectadas. Estos litigios pueden resultar en costos legales significativos, así como en indemnizaciones y daños a la reputación.

RESPONSABILIDAD DE LOS DIRECTIVOS

Los directivos y miembros del consejo de administración de una organización pueden ser considerados personalmente responsables en caso de incumplimiento de las leyes y regulaciones de ciberseguridad.
Esto puede resultar en responsabilidad financiera y legal, así como en daños a la reputación personal.

El rol del Gobierno de Ciberseguridad en los Riesgos de Cumplimiento

Las buenas prácticas de gobierno de la ciberseguridad que hemos revisado continuamente en los puntos anteriores de esta guía desempeñan un papel fundamental en la reducción de la exposición a los riesgos de cumplimiento. Podemos observar como estas prácticas tributan en el siguiente diagrama:

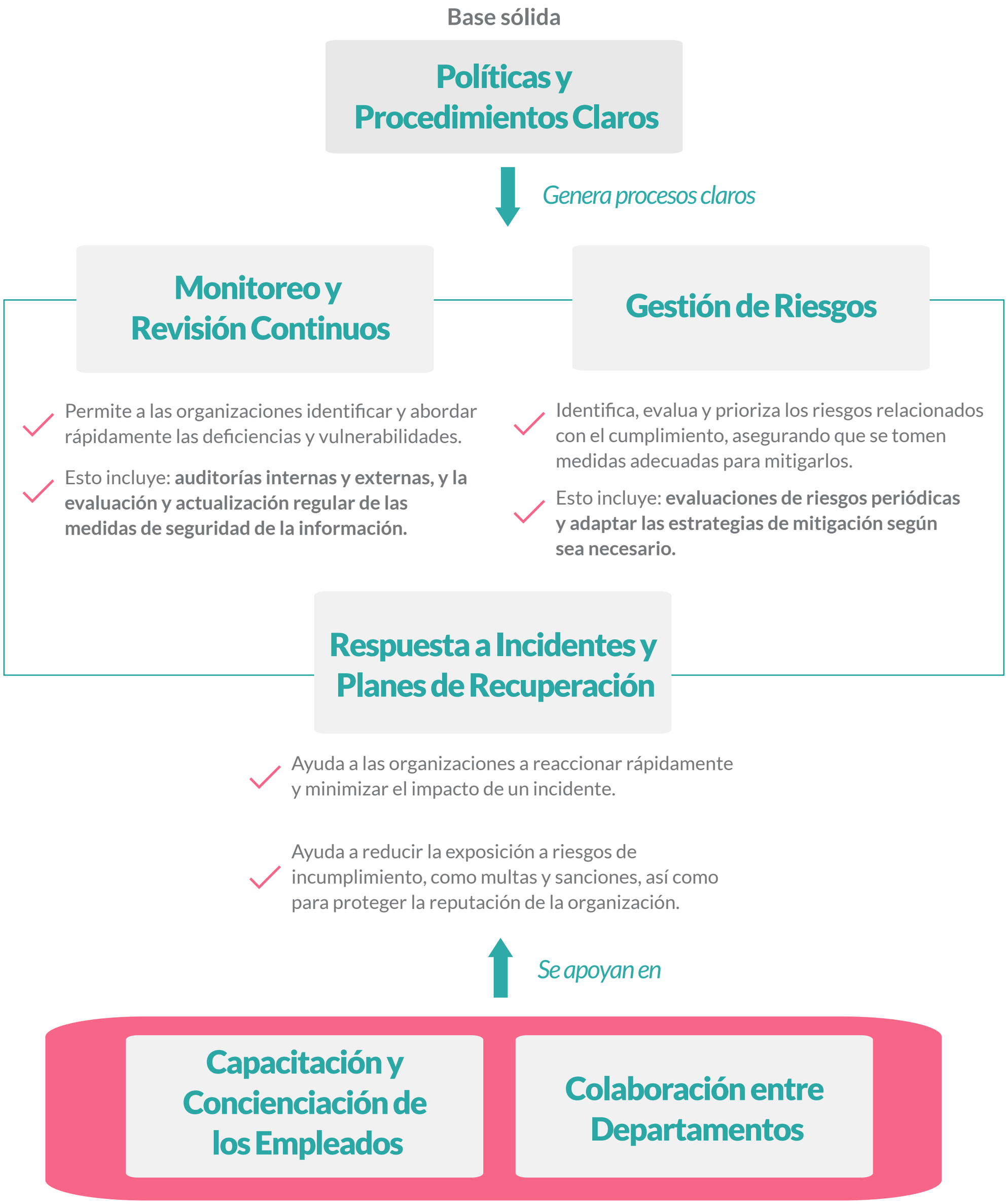


Ilustración n°4.

Capítulo 3

ROL DEL AUDITOR INTERNO EN EL GOBIERNO DE LA SEGURIDAD DE LA INFORMACIÓN

Capítulo 3

ROL DEL AUDITOR INTERNO EN EL GOBIERNO DE LA SEGURIDAD DE LA INFORMACIÓN

El papel del auditor interno es esencial, es este el profesional que proporciona una capa de control y supervisión para garantizar que la organización esté gobernando de manera efectiva su 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 Gobierno de la Ciberseguridad son:

- **Determinar si la función de seguridad de la información se alinea con y comprende los objetivos y estrategias de la organización.**
- **Determinar la eficacia de la gestión de recursos y de los recursos y el rendimiento de ciberseguridad.**
- **Evaluar si el gobierno organizacional entrega los recursos y se compromete de la forma que la organización requiere para mantener una culta de seguridad y un sistema de gestion de seguridad de la información robusto.**

3.1 EL ROL DEL AUDITOR INTERNO

En ningún caso el auditor interno tendrá las facultades para definir ni implementar estructuras organizacionales, procesos, metodologías, políticas ni cualquier otro elemento de la arquitectura empresarial. 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:

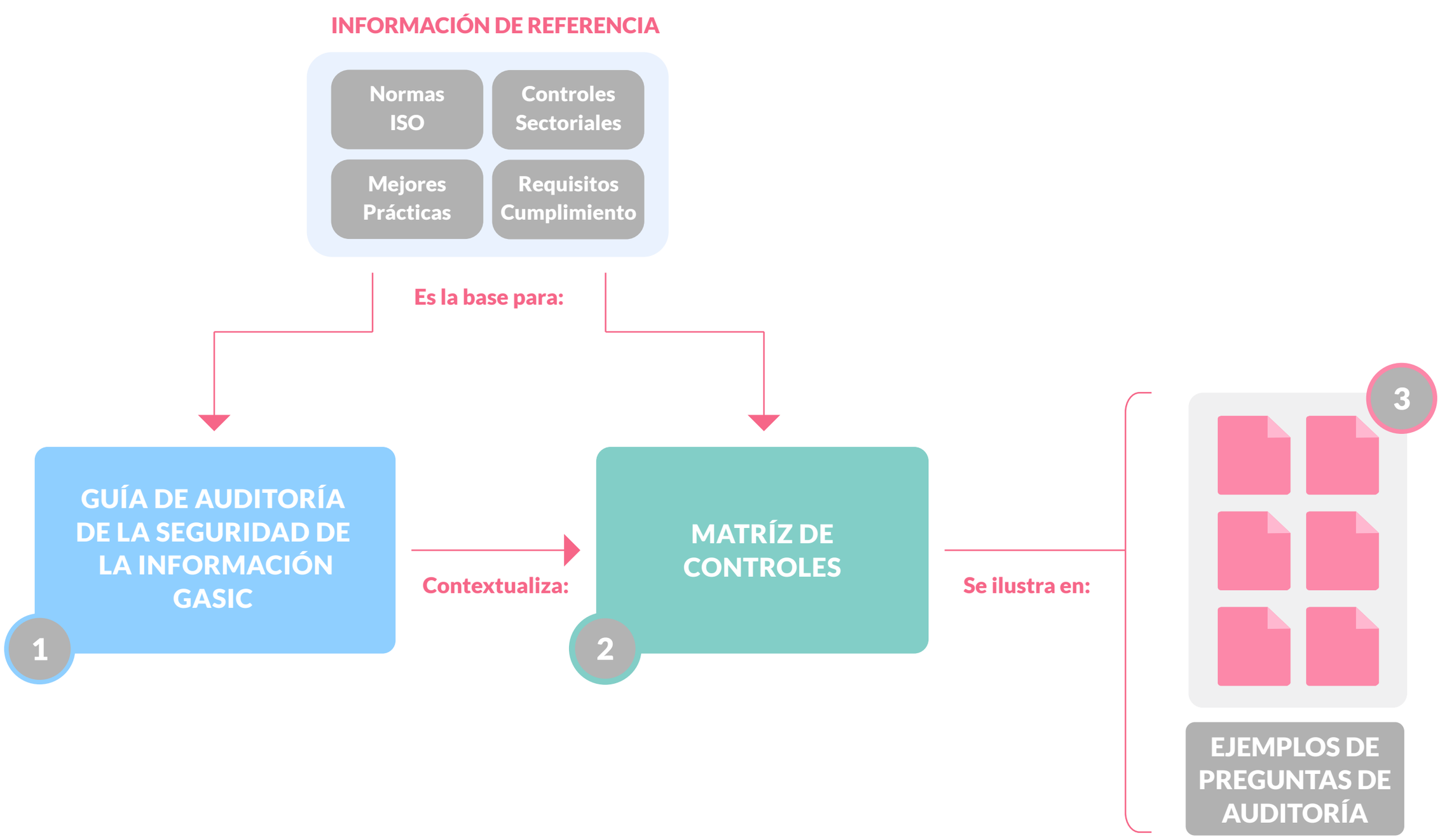


Ilustración n°5. Modo de uso y Estructura Documental GASIC. Fuente: Elaboración Propia

El método de trabajo sugerido es el siguiente:

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

02 A continuación, puede utilizar la Matriz de Controles GASIC 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 Ejemplos de Preguntas de Auditoria GASIC 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.

3.3 DESARROLLO DE UN PLAN DE AUDITORÍA PARA EL GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN

El instrumento de apoyo para la auditoría busca determinar si las actividades descritas en la guía metodológica de Gobierno de la Ciberseguridad 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 21 controles que provienen de las mejores prácticas (NIST CSF 1.1, ISO 22301:2021, ISO 27002:2022, COBIT 2019) apoyados por los principios de gobierno contenidos en la ISO 38500 y considerando las recomendaciones de GTAG 17.
Estos controles se han organizado en cuatro ejes temáticos, que permiten su mejor comprensión, los cuales son:

- **Dirección Estratégica de Riesgos**
- **Dirección de la Inversión y Garantización del Valor**
- **Dirección de Riesgos**
- **Dirección con las Partes Interesadas**

Ejes Temáticos
I. Sistema de Gobierno

El eje de Dirección de Sistema de Gobierno aborda las temáticas relacionadas con la dirección de los procesos de SIC. Este eje vela por resguardar el alineamiento estratégico, que los instrumentos de dirección se han desarrollado de la mejor forma posible en concordancia con las mejores prácticas y que se habilitan instancias para la mejora del sistema de gobierno en sí mismo.
Los controles que conforman este eje temático son:

	CONTROL	DESCRIPTOR
1	**Dirigir el Sistema de Gobierno**	**La dirección debe asegurar que el marco de gobierno de SIC se ajuste a los objetivos empresariales, alineado con las estrategias y planes de la organización.**
2	**Establecer la Política de SIC**	**La dirección debe asegurar que se han definido y comunicado políticas para la gestión de la seguridad de la información.**
3	**Establecer Roles y Responsabilidades**	**La dirección debe asegurar los roles y responsabilidades relacionados con la ciberseguridad están correctamente definidos, coordinados y alineados adecuadamente con los roles internos y los socios externos de la organización.**
4	**Asegurar el Cumplimiento de los Requerimientos Legales y Regulatorios**	**La dirección debe asegurar qué se han identificado y se cumplen las leyes y regulaciones aplicables.**
5	**Monitorear el Sistema de Gobierno**	**La dirección debe asegurar que se establezcan y mantengan procesos de monitoreo efectivos para el sistema de gobierno de SIC.**
6	**Evaluar el Sistema de Gobierno**	**La dirección debe asegurar que se realice una evaluación del sistema de gobierno de SIC para determinar su efectividad en el cumplimiento de los objetivos empresariales y que se identifiquen las áreas que requieren mejoras o cambios.**

II. Dirección de la Inversión y Garantizar el Valor

Es responsabilidad de la dirección el proveer los recursos necesarios para llevar a cabo las actividades en los procesos de SIC. Esto implica que las inversiones en seguridad deben aportar al cumplimiento de los objetivos estratégicos y no herir la rentabilidad general de la organización. A través de este eje temático busca comprobar que la dirección gestiona de forma adecuada los recursos de la organización.

Los controles que conforman este eje temático son:

	CONTROL	DESCRIPTOR
7	**Establecer el Objetivo de Inversión en SIC**	**La dirección debe asegurar que se establezca un objetivo claro para la mezcla de inversión en SIC que sea consistente con los objetivos empresariales, y que se refleje en la estrategia de inversión en TI de la organización** **Las inversiones propuestas en SIC deben evaluarse en cuanto a sus beneficios empresariales y la adquisición de activos de TI debe ser dirigida de acuerdo con las estrategias y políticas establecidas.**
8	**Dirigir la Gestión de Recursos**	**La dirección debe asegurar que los recursos asignados a la función de SIC se gestionen adecuadamente y se utilicen de manera efectiva para alcanzar los objetivos empresariales y de seguridad.**
9	**Dirigir la Optimización del Valor**	**La dirección debe asegurar que se realice una evaluación regular del desempeño del portafolio de inversiones en SIC para identificar oportunidades de optimización del valor.**
10	**Evaluar la Optimización del Valor**	**La dirección debe asegurar que se realice una evaluación regular de la optimización del valor de los servicios de entregados por la función de SIC a la organización.**
11	**Evaluar la Gestión de Recursos**	**La dirección debe asegurar que se realice una evaluación de la gestión de recursos asignados a la función de SIC para determinar su efectividad en el cumplimiento de los objetivos empresariales y de seguridad, y que se identifiquen las áreas que requieren mejoras o cambios.**
12	**Monitorizar la Optimización de Valor**	**La dirección debe asegurar que se establezcan y mantengan procesos y sistemas de monitoreo efectivos para evaluar la optimización del valor de los activos y recursos de asignados a la función de SIC en relación con los objetivos empresariales y de seguridad.**
13	**Monitorear la Gestión de Recursos**	**La dirección debe asegurar que se realice una monitorización regular y documentada de la gestión de recursos asignados a la función de SIC para asegurar que los recursos estén siendo utilizados de manera efectiva y eficiente, y que se estén cumpliendo los objetivos de la empresa y de seguridad.**

III. Dirección de Riesgos

El eje "Dirección de Riesgos" contiene las actividades que son responsabilidad del órgano de gobierno en materia de definición de riesgos, tales como: la definición de la postura de riesgos de la organización, el reconocimiento de la relevancia de infraestructura crítica, la supervisión de las actividades de gestión de riesgo y la mejora continua del proceso.

Los controles que conforman este eje temático son:

	CONTROL	DESCRIPTOR
14	**Reconocer la Infraestructura Crítica**	**La dirección reconoce el rol de la organización como parte de la infraestructura crítica, o su relación con entidades categorizadas como infraestructura crítica y utiliza ese conocimiento para planificar sus procesos de gestión de riesgos, incidentes y continuidad.**
15	**Establecer las Dependencias y Funciones Críticas**	**La dirección asegura que se hayan establecido las dependencias y funciones críticas para la entrega de servicios críticos.**
16	**Definir la Tolerancia al Riesgo**	**La dirección asegura que la tolerancia al riesgo organizacional haya sido determinada y expresada claramente.**
17	**Dirigir la Gestión de Riesgos**	**La dirección debe asegurar que se establezca y mantenga un proceso formal y documentado de gestión de riesgos de SIC que esté alineado con los objetivos empresariales y de seguridad.**
18	**Evaluar la Gestión de Riesgos**	**La dirección debe asegurar que se realice una evaluación de la gestión de riesgos de SIC para determinar su efectividad en la identificación, evaluación, tratamiento y monitoreo de los riesgos de TI de la organización.**
19	**Monitorear la Gestión de Riesgos**	**La dirección debe asegurar que se establezca y mantenga un proceso formal y documentado para la monitorización de la gestión de riesgos de TI, con el fin de evaluar la eficacia de los controles de riesgos y la implementación de planes de acción para la mitigación de riesgos identificados.**

IV. Dirección de las Partes Interesadas

Este eje temático guarda relación con todas aquellas actividades que la dirección debe realizar para asegurar que su relación con las partes interesadas es óptima, que aporta a la consecución de sus objetivos estratégicos y a los objetivos de seguridad de la información y ciberseguridad.

Los controles que conforman este eje temático son:

CONTROL		DESCRIPTOR
20	**Dirigir el Compromiso, Comunicación y Reporte de las Partes Interesadas**	**La dirección debe asegurar que se establezcan y mantengan procesos y mecanismos de compromiso, comunicación y reporte efectivos con las partes interesadas relevantes para la función de SIC, incluyendo a la dirección ejecutiva, los empleados, los proveedores de servicios de TI, los clientes y los reguladores.**
21	**Rol en la Cadena de Suministro**	**La dirección asegura que se identifica y se comunica la función de la organización en la cadena de suministro.**
22	**Evaluar el Compromiso y los Requisitos de las Partes Interesadas.**	**La dirección debe asegurar que se evalúe regularmente el compromiso y los requisitos de reportes de las partes interesadas con relación a la gestión de SIC.**
23	**Monitorizar el Compromiso de las Partes Interesadas**	**La dirección debe asegurar que se establezcan y mantengan mecanismos de monitoreo efectivos para el compromiso de las partes interesadas en el marco de gobierno de SIC.**

Apéndice

ANEXOS

Anexos:

DECRETOS DE CIBERSEGURIDAD

Instructivo Presidencial N°1 de 2018	Imparte instrucciones sobre uso de servicios en la nube a los órganos de la Administración del Estado – Presidencia de la República.
Instructivo Presidencial N°8 de 2018	Imparte instrucciones urgentes en materia de ciberseguridad a los órganos de la administración del Estado – Presidencia de la República.
Ley N°21.180: Transformación Digital del Estado	Tiene por objeto efectuar una transformación digital del Estado, incorporando el soporte y la tramitación electrónica en los procedimientos administrativos del Estado y la gestión documental. De esta forma, se pretende digitalizar trámites ante servicios públicos, simplificar y eliminar trámites que las personas realizan ante el Estado. Además, se crea un Archivo Nacional digital que registrará de forma mucho más eficiente toda la información de los servicios públicos.
Ley N°21.459: Establece Normas sobre Delitos Informáticos	Deroga la Ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest.
Decreto Supremo N°5.996, de 1999	Crea Red Interna (INTRANET) del Estado y entrega su implementación, puesta en marcha, administración, coordinación y supervisión al Ministerio del Interior y Seguridad Pública.
Decreto Supremo N°1.299, de 2005	Establece nuevas normas que regulan la Red de Conectividad del Estado que administra el Ministerio del Interior y fija los procedimientos, requisitos y estándares tecnológicos para la incorporación a dicha red de instituciones públicas.
Decreto Supremo N°83, de 2005	Aprueba norma técnica para los órganos de la administración del estado, sobre seguridad y confidencialidad de los documentos electrónicos.

Decreto Supremo N°93, de 2006	Aprueba norma técnica para la adopción de medidas destinadas a minimizar los efectos perjudiciales de los mensajes electrónicos masivos no solicitados, recibidos en las casillas electrónicas de los órganos de la administración del Estado y de sus funcionarios.
Decreto Supremo N°14, de 2014	Modifica decreto n°181, de 2002, que aprueba reglamento de la ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, y deroga los decretos que indica.
Decreto Supremo N°1, de 2015	Aprueba norma técnica sobre sistemas y sitios web de los Órganos de la Administración del Estado.
Decreto N°83 de 2017	Convenio sobre la ciberdelincuencia.
Decreto N°4 de 2020	Regula la forma en que los procedimientos administrativos deberán expresarse a través de medios electrónicos.
Decreto N°273 de 2022	Establece obligación de reportar incidentes de ciberseguridad.
Ley 27663 de 2024	Ley Marco de Ciberseguridad, establece criterios de protección para la infraestructura crítica.