



**OZonE**  
CIBERSECURITY

# **Auditoría de Seguridad de la Información y Gobierno de TI: Implementación COBIT y Roles de Auditoría**

Ruben Apablaza Muñoz  
—OZonE—



## Introducción

Este documento aborda tanto la implementación como los beneficios de aplicar el marco COBIT para fortalecer el gobierno de TI y la ciberseguridad en el caso de la empresa Jaguar Tech Solutions, una empresa multinacional de desarrollo de software y servicios tecnológicos que experimenta un crecimiento acelerado y un aumento en las amenazas cibernéticas. Cabe destacar que este marco es recomendado para empresas que dependen de la tecnología para lograr sus objetivos comerciales.

En este documento se examinan los principios clave de COBIT y su aplicación práctica, así como el rol fundamental de las matrices RACI en la definición de roles y responsabilidades para optimizar la gestión de TI.

Asimismo, se profundizará en los objetivos y tipos de auditorías de seguridad, diferenciando entre auditorías internas y externas, y analizando los roles esenciales involucrados en el proceso de auditoría para asegurar el cumplimiento normativo y la mejora continua de los sistemas de seguridad de la información.

## CASO DE ESTUDIO

### 1. Desarrollo del caso estudio

Caso de Estudio: Jaguar Tech Solutions

#### 1.1. Contexto de la Empresa

Jaguar Tech Solutions es una empresa multinacional dedicada al desarrollo de software y servicios tecnológicos. Enfrenta desafíos relacionados con el gobierno de TI, la seguridad cibernética y la alineación estratégica de sus operaciones tecnológicas con los objetivos empresariales.

La empresa ha decidido implementar el marco COBIT para mejorar su gestión de TI y cumplir con las normativas de ciberseguridad.

#### 1.2. Enunciado del Caso

Jaguar Tech Solutions ha experimentado un crecimiento acelerado en los últimos años, lo que ha llevado a una expansión en su infraestructura tecnológica y un aumento en las amenazas cibernéticas. Para abordar estos desafíos, la empresa ha decidido adoptar el marco COBIT para fortalecer su gobierno de TI y mejorar la seguridad de sus sistemas.

La dirección ha identificado varias áreas clave para la mejora:

**1. Gobierno de TI:** Necesidad de establecer principios claros para gestionar las tecnologías de información.

**2. Estructura Organizacional:** Definir roles y responsabilidades claros en la gestión de TI.

**3. Seguridad Cibernética:** Cumplir con las normativas de ciberseguridad mediante auditorías efectivas.

**4. Tipos de Auditoría:** Diferenciar los tipos de auditoría para definir alcances y enfoques.

**5. Roles en Auditoría:** Describir roles clave en el proceso de auditoría.



## **INDICADOR 1: IDENTIFICACIÓN DE PRINCIPIOS CLAVE DE COBIT**

**Pregunta 1: Enumere y explique dos principios clave de COBIT que Jaguar Tech Solutions debería aplicar para mejorar su gobierno de TI.**

De los **5** principios **CLAVE** de **COBIT**

- Satisfacer las necesidades de las partes
- Cubrir la empresa de extremo a extremo
- Aplicar un marco único e integrado
- Facilitar un enfoque holístico
- Separar la gobernanza de la gestión

Se escogen los siguientes para la elaboración de la respuesta de cara a la segunda pregunta.

### **1. Satisfacer las necesidades de las partes interesadas**

Reconoce la importancia de identificar y SATISFACER las expectativas de TODAS las partes interesadas de la organización.

Básicamente este principio asegura que las decisiones de TI estén alineadas con los objetivos del negocio y las expectativas de clientes, reguladores, empleados y socios estratégicos.

### **2. Facilitar un enfoque holístico**

Al adoptar un enfoque holístico, las organizaciones pueden comprender mejor el impacto de las decisiones de TI en toda la empresa y tomar decisiones informadas que beneficien a la organización en su conjunto. Esto ayuda a identificar interdependencias, mitigar riesgos y optimizar la asignación de recursos. <sup>i</sup>

**Pregunta 2: Proporcione 2 ejemplos específicos en los que estos principios podrían beneficiar a Jaguar Tech Solutions.**

**Ejemplo 1.**

***Satisfacer las necesidades de las partes interesadas:***

- **Situación:**

Jaguar Tech Solutions desarrolla software para clientes del sector financiero, que requieren altos estándares de seguridad y cumplimiento normativo.

- **Aplicación del principio:**

Implementar procesos de gobierno que aseguren que los requisitos regulatorios se integren desde el diseño del software.

Marcos regulatorios aplicados a este ejemplo:

- ✓ **ISO/IEC 27001** (Internacional).
- ✓ **NORMATIVA DE CARÁCTER GENERAL N° 454 de la CMF.**<sup>ii</sup>
- ✓ **LEY 21.663 LEY MARCO DE CIBERSEGURIDAD.**<sup>iii</sup>
- ✓ **LEY 21.719 REGULA LA PROTECCIÓN Y EL TRATAMIENTO DE LOS DATOS PERSONALES Y CREA LA AGENCIA DE PROTECCIÓN DE DATOS PERSONALES.**<sup>iv</sup>
- ✓ **Circulares emitidas por la CMF como por ejemplo la Circular n°2 entre otras.**<sup>v</sup>

- **Beneficio:**

Cumplir con este principio evita sanciones legales, mejora la reputación de la empresa y aumenta la confianza del cliente, ya que la seguridad está alineada con las necesidades del negocio.



## Ejemplo 2.

### *Facilitar un enfoque holístico*

- **Situación:**

El crecimiento acelerado ha provocado que distintos equipos (seguridad, desarrollo, soporte, infraestructura) trabajen sin una coordinación clara. Esto ha generado problemas como:

- ✓ Duplicación de esfuerzos en tareas de mantenimiento.
- ✓ Incidentes de seguridad mal gestionados por no saber quién es responsable de responder.
- ✓ Proyectos retrasados por falta de claridad en los roles.

- **Aplicación del principio:**

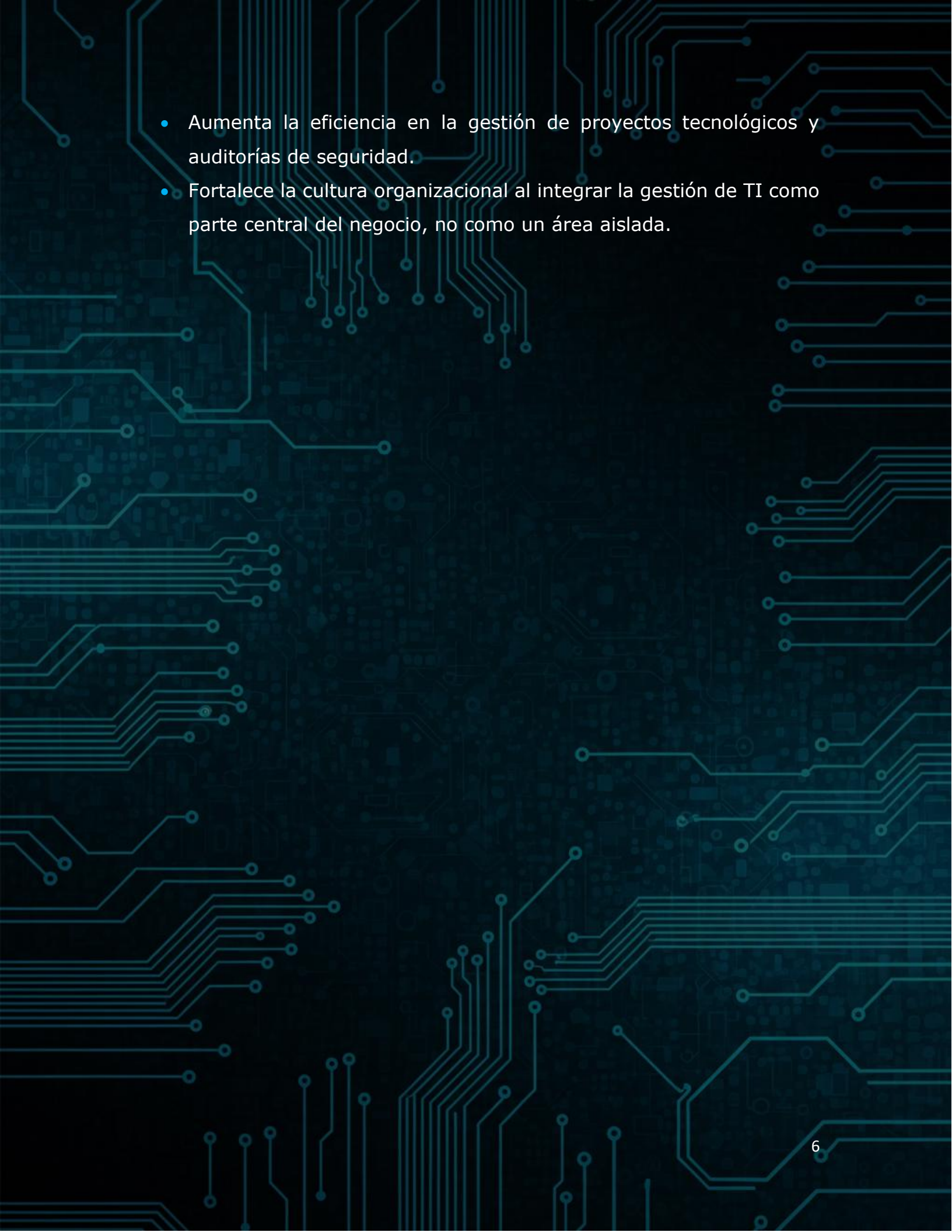
Se crea una matriz RACI para todos los procesos críticos de TI:

- ✓ Gestión de incidentes de seguridad.
- ✓ Actualizaciones de sistemas.
- ✓ Auditorías internas y externas.
- ✓ Implementación de nuevos servicios tecnológicos.

Además, revisa y alinea las estructuras organizativas, para que cada área conozca su rol, se comuniquen con las demás y todas las decisiones estén dentro del marco general de la empresa.

- **Beneficio:**

- Mejora la comunicación y colaboración entre equipos de TI y otras áreas (como legal o recursos humanos).
- Reduce errores y solapamientos al establecer responsables específicos para cada tarea.

- 
- Aumenta la eficiencia en la gestión de proyectos tecnológicos y auditorías de seguridad.
  - Fortalece la cultura organizacional al integrar la gestión de TI como parte central del negocio, no como un área aislada.



## INDICADOR 2: ESTRUCTURA CLARA DE RESPONSABILIDADES

**Pregunta 3: Describa cómo una matriz RACI podría ayudar a Jaguar Tech Solutions a definir roles y responsabilidades en su gestión de TI.**

Antes de responder directamente primero se debe entender aunque sea de forma breve **que es** una matriz **RACI**.

### Definición:

Herramienta de gestión de proyectos y procesos que se utiliza para definir y comunicar roles y responsabilidades dentro de una organización o equipo.

- **RESPONSABLE**
  - ✓ Responsables de realizar la tarea.
- **APROBADOR**
  - ✓ Quien toma la última decisión.
- **CONSULTADO**
  - ✓ Quien da información o asesoramiento de la tarea.
- **INFORMADO**
  - ✓ Reciben actualización o comunicación sobre el progreso, pero no tienen un rol activo en la ejecución.

En corto es una herramienta que comunica quien hace que dentro de un proceso y por lo tanto ayuda a romper el **síndrome de "no es mi trabajo"**.

En el caso de Jaguar Tech Solutions, la matriz RACI, **ordena su gestión de TI**, como se señala en la respuesta anterior, sobre todo debido al crecimiento acelerado de la empresa y pueden presentarse confusiones críticas como:

- ¿Quién es el/la responsable de responder a un incidente de seguridad?



- ¿Quién aprueba los cambios en los sistemas?
- ¿A quién deben informar los equipos en caso de un fallo crítico?

Estas dudas **generan ineficiencia, riesgos y retrasos.**

Por este motivo se utiliza una matriz RACI ya que se asignan e informan CLARAMENTE los roles para cada proceso como en el ejemplo siguiente:

Actividad	CISO	Equipo SOC	Equipo de operaciones de TI	Gerente de TI
Detectar y clasificar el incidente	I	R	C	C
Contener y remediar el incidente	A	R	C	I
Reportar a la dirección y documentar	R	C	I	A

Descripción breve de roles involucrados:

- **CISO:** *Chief Information Security Officer, responsable estratégico de la seguridad.*
- **Equipo SOC:** *Centro de operaciones de seguridad, encargado de la detección y respuesta.*
- **Equipo de Operaciones de TI:** *Gestiona la infraestructura técnica, sistemas y soporte.*
- **Gerente de TI:** *Supervisa y coordina las operaciones de TI desde un enfoque ejecutivo.*

Si bien la pregunta no lo solicita, prefiero dejar el registro siguiente que me parece relevante y atinente.

Así como utilizar una matriz RACI tiene sus ventajas, lo cierto es que también hay algunas desventajas que es bueno considerar:



- **Limitaciones en el alcance de los roles:**

El modelo RACI no proporciona detalles sobre el alcance de los roles.

- **Límites en los detalles y el alcance de las tareas:**

si bien una matriz RACI puede proporcionar una descripción general de quién es responsable de las diferentes tareas, no indicará qué se debe hacer.

Alternativas a RACI según las necesidades del proyecto:

- **RASCI** : agrega un rol de soporte a la estructura RACI tradicional, brindando asistencia adicional cuando sea necesario.
- **DACI** : El marco DACI<sup>vi</sup> se centra en la toma de decisiones mediante la identificación de tomadores de decisiones claros y responsables de los resultados finales.
- **RAPID** : Un marco de toma de decisiones que define quién recomienda, acuerda, ejecuta, aporta y decide sobre decisiones críticas.
- **Diagrama de Gantt** : proporciona una vista completa de quién hace qué y cuándo, combinando responsabilidades con cronogramas en un formato visual.
- **Estructura de desglose del trabajo** : desglosa todo el alcance del trabajo en un proyecto, ofreciendo una vista detallada de todas las tareas en una estructura jerárquica.
- **Panel de proyecto** : ofrece una supervisión dinámica y en tiempo real, manteniendo a los equipos informados con información actualizada sobre el progreso del proyecto, los roles y las responsabilidades.



Para revisar información que me parece relevante respecto de RACI sugiero visitar los siguientes enlaces:

<https://project-management.com/understanding-responsibility-assignment-matrix-raci-matrix/>

<https://www.pmi.cl/blog/de-matriz-raci-a-recia-redefiniendo-la-gobernanza-de-programas-proyectos-y-operaciones-en-entornos-complejos-22638>

<https://clickup.com/es-ES/blog/42483/ejemplos-de-matrices-de-raci>



**Pregunta 4: Indique dos ejemplos donde la claridad en roles haya mejorado la alineación con los objetivos estratégicos.**

**EJEMPLO 1. SpaceX** (si, la compañía de Elon Musk)

- Compañía aeroespacial que fabrica cohetes, y ofrece servicios de transporte.
- Asumiendo que una empresa de ese tamaño debe de tener una matriz RACI "GIGANTESCA", simplificando al máximo una matriz para uno de sus proyectos quedaría algo así.

RESPONSABLES	Ingenieros Eléctricos	Ingenieros Aeroespaciales	Ingenieros jefe	Elon Musk
Diseño del cohete	C	R	I	A
Suministros vitales	R	C	A	I
Protección térmica	C	R	A	I
Eficiencia del combustible	C	R	A	I

Elon Musk es el **Administrador** del "Diseño del Cohete".

- Eso es porque él, es el "Ingeniero Jefe" en SpaceX.

Sin embargo, los "Ingenieros Aeroespaciales" son los **Responsables** de diseñarlo. Estos **Consultan** a otros ingenieros como los "Ingenieros Eléctricos", pero finalmente ellos hacen los números y el diseño.

En el resto de las tareas desarrolladas en SpaceX, Elon Musk sólo es **Informado** o ligeramente Consultado.

Como se puede ver, aún si eres el Fundador y CEO de una Empresa, sólo serás **Responsable** de lo que estés directamente al cargo.

Por esto es tan importante esta Herramienta.



## Porque ayuda a evitar interferencias entre los diferentes departamentos y profesionales.

- Estas interferencias pueden acabar matando un proyecto:
  - Jefes entrometidos.
  - Responsabilidades que se desvanecen.
  - Retoques interminables.
  - etc.

### EJEMPLO 2. Empresa de diseño con “amigos”

Lo interesante de este ejemplo son las características de su contexto además de tratarse de un caso diametralmente distinto al anterior, lo que demuestra que la matriz RACI se puede aplicar no solo a organizaciones grandes sino que también a equipos pequeños.

- 4 diseñadores se unen para hacer una empresa de diseño.
  - Los 4 tienen la misma formación académica y similares habilidades.
- Por esto resulta difícil decidir quién debería hacer que.

La matriz RACI para este caso queda conformada de la siguiente forma:

RESPONSABLES	Juan	María	Raquel	Ruben
Imagen principal	R	C	A	I
Composición de color	I	R	C	A
Tipografía	A	I	R	C
Estructura final	C	A	I	R

En este caso todos han decidido alternar roles y definirlos claramente.

De esta forma se consigue un equilibrio perfecto en la carga de trabajo global que esta alineado con los objetivos estratégicos del proyecto.<sup>vii</sup>

Fuente:

### **INDICADOR 3: OBJETIVOS PRINCIPALES DE LA AUDITORÍA DE SEGURIDAD**

**Pregunta 5: Identifique dos objetivos principales que una auditoría de seguridad debería cumplir para Jaguar Tech Solutions.**

**Pregunta 6: Explique y sustente cómo estos objetivos contribuyen al cumplimiento normativo.**

**ACLARACION PREVIA:** Debido a que ambas preguntas apuntan hacia donde mismo, es que responderé a ambas en una sola respuesta.

Lo primero seria definir que es una auditoria de seguridad y cuáles serían los objetivos principales para poder seleccionar 2.

#### **Auditoria de seguridad**

Proceso sistemático para evaluar y mejorar la seguridad de la información.

#### **Objetivos**

- **Evaluación de controles**
  - ✓ Se verifica la efectividad de los controles de seguridad.
- **Detección de vulnerabilidades.**
  - ✓ Detectar y mitigar vulnerabilidades y riesgos de seguridad.
- **Cumplimiento normativo**
  - ✓ Verificar el cumplimiento de las políticas, regulaciones y estándares de seguridad tanto internos como externos, asegurándose que se cumple con leyes y regulaciones de la industria.
- **Documentación de auditoria**
  - ✓ Se documentan los hallazgos y recomendaciones resultantes, proporcionando una base para la mejora continua.



En relación a Jaguar Tech Solutions los dos objetivos principales debiesen ser:

### **1. Cumplimiento normativo**

Asegura que Jaguar Tech Solutions cumple con todas las leyes, normas y estándares aplicables en materia de ciberseguridad y protección de datos. Esto incluye normativas enumeradas y presentadas en el ejemplo de la pregunta 2 de este informe.

#### **¿Cómo contribuye al cumplimiento normativo?**

- ✓ Permite detectar incumplimientos antes de una auditoría externa o una fiscalización.
- ✓ Ayuda a documentar evidencias de cumplimiento, lo que es exigido por muchas regulaciones.
- ✓ Asegura que las políticas, procedimientos y controles estén alineados con el marco legal vigente.

### **2. Evaluación de controles**

Comprueba que los mecanismos de seguridad existentes (firewalls, antivirus, autenticación, monitoreo, políticas internas, etc.) funcionan correctamente y están alineados con los objetivos estratégicos de la empresa y es fundamental para demostrar que los controles exigidos por la ley o estándares están operativos y son efectivos. No basta con declarar que existen políticas; se debe probar que los controles funcionan adecuadamente.

## ¿Cómo contribuye al cumplimiento normativo?

- ✓ Asegura que los controles documentados (como cifrado, autenticación, respaldo, etc.) están activos y funcionando, lo cual es requerido por normas como las mencionadas previamente en la pregunta 2 de este informe.
- ✓ Demuestra un enfoque proactivo de la gestión del riesgo, lo que muchas normas valoran y en algunos casos exigen.
- ✓ Permite ajustar o mejorar controles ineficientes, reduciendo el riesgo de incumplimientos futuros.



## INDICADOR 4: DIFERENCIACIÓN ENTRE TIPOS DE AUDITORÍA

**Pregunta 7: Diferencie entre auditorías internas y externas, y explique cuál sería más beneficiosa para Jaguar Tech Solutions.**

### Tipo de auditoria 1. INTERNA

- ✓ Realizada por personal interno.
- ✓ Su **objetivo** es evaluar y mejorar políticas y procedimientos internos de seguridad, identificar riesgos, asegurar cumplimiento y eficiencia operativa.
- ✓ Su **frecuencia** puede ser regular o continua (trimestral, semestral, anual, etc).
- ✓ Su **alcance** es flexible y definido por la organización.
- ✓ Su **enfoque** es preventivo, de mejora continua.
- ✓ Por su naturaleza interna su **grado de independencia** puede ser limitado aunque puede ser objetiva si hay separación de funciones.

### Tipo de auditoria 2. EXTERNA

- ✓ Por auditores externos independientes.
- ✓ Su **objetivo** es verificar el cumplimiento normativo y la confiabilidad de la información para terceros.
- ✓ Su **frecuencia** es generalmente anual o según requerimientos regulatorios o contractuales.
- ✓ Su **alcance** es fijo, según normas específicas o requerimientos legales.
- ✓ Su **enfoque** es netamente evaluador, con enfoque en cumplimiento y validación externa.
- ✓ Su **grado de independencia** es alta debido a que el auditor externo no tiene relación directa con la empresa.

### Tipo de auditoria 3. DE CUMPLIMIENTO

#### CUMPLIMIENTO<sup>viii</sup>

- ✓ Puede ser realizada por personal interno o externo, dependiendo del contexto.
- ✓ Su **objetivo** es verificar si la empresa cumple con leyes, normativas, estándares o políticas internas específicas relacionadas con seguridad, privacidad y operaciones.
- ✓ Su **frecuencia** depende de exigencias legales, regulatorias o internas (por ejemplo, anualmente, semestral o por evento).
- ✓ Su **alcance** está enfocado en normativas específicas como las ya citadas en la pregunta 2.
- ✓ Su **enfoque** es asegurar conformidad con marcos legales y contractuales, y evitar sanciones o incumplimientos.
- ✓ Su **grado de independencia** depende de quién la realiza: si es interna puede ser limitada, si es externa es alta.



## ¿Cuál sería más beneficiosa para Jaguar Tech?

Debido a que la empresa se encuentra en un proceso de fortalecimiento del gobierno de TI, la auditoría interna es la más beneficiosa.

Le permite identificar debilidades, adaptar procesos a COBIT y prepararse para futuras auditorías externas sin exponer riesgos prematuramente.

A continuación se enumeran algunas razones para sustentar la respuesta:

### **1. Apoya directamente la implementación de COBIT**

Una auditoría interna permite evaluar si los procesos de TI, roles, controles y estructuras están **alineados con los principios de COBIT**. Sirve como herramienta para ajustar y mejorar el sistema de gobierno de TI desde adentro, antes de una evaluación externa.

### **2. Detecta fallas antes de que escalen**

La auditoría interna actúa como una defensa **preventiva**, ayudando a Jaguar a identificar brechas en seguridad, cumplimiento y operación sin exponer públicamente sus debilidades.

### **3. Flexibilidad en el alcance**

Puede enfocarse específicamente en áreas críticas (como gestión de incidentes, control de accesos o cumplimiento de políticas internas), **adaptándose** al crecimiento y madurez tecnológica de la empresa.

### **4. Fomenta la mejora continua**

Permite realizar ciclos de revisión frecuentes y seguimiento de planes de acción **correctivos**, algo esencial en una empresa que está en proceso de madurar su gobernanza de TI.

**Pregunta 8: Proporcione 2 ejemplos donde cada tipo de auditoría podría ser aplicada dentro de la empresa.**

### **Auditoría Interna**

- **Ejemplo 1:**

*Evaluación del proceso de gestión de incidentes de ciberseguridad.*

- Verificar si los incidentes son detectados, registrados, priorizados y resueltos según el procedimiento interno.

- **Ejemplo 2:**

*Auditoría interna sobre el control de accesos a sistemas críticos.*

- Revisar si los accesos están correctamente asignados, actualizados y revocados cuando corresponde (por ejemplo, cuando un empleado deja la empresa).

### **Auditoría Externa**

- **Ejemplo 1:**

*Auditoría externa de cumplimiento con la norma ISO/IEC 27001.*

- Revisar si la empresa tiene un Sistema de Gestión de Seguridad de la Información (SGSI) bien implementado.

- **Ejemplo 2:**

*Auditoría de cliente externo (sector financiero).*

- Una entidad bancaria que contrata a Jaguar exige revisar la seguridad de la plataforma que se le está desarrollando, como parte de sus controles de terceros.



## **Auditoría de Cumplimiento (o de Conformidad)**

- **Ejemplo 1:**

*Auditoría de cumplimiento con la Ley de Protección de Datos Personales del país.*

- Verificar si Jaguar trata, almacena y protege la información personal de empleados y clientes conforme a la ley.

- **Ejemplo 2:**

*Auditoría de cumplimiento con políticas internas de uso aceptable de tecnología.*

- Revisar si los empleados cumplen con las normas internas sobre uso de correo corporativo, navegación segura y almacenamiento en la nube.

## INDICADOR 5: ROLES Y RESPONSABILIDADES EN AUDITORÍA

**Pregunta 9: Describa los roles clave que deben estar presentes en una auditoría de seguridad en Jaguar Tech Solutions.**

**Pregunta 10: Explique cómo cada rol contribuye al éxito del proceso de auditoría.**

**ACLARACION PREVIA:** Al igual que en el indicador 3, debido a que ambas preguntas apuntan hacia donde mismo, es que responderé a ambas en una sola respuesta.

### 1. Auditor Líder

Es el que **dirige la auditoría**, define el plan, asegura el cumplimiento del alcance y valida los resultados.

- **Ejemplo 1:**

El auditor líder planifica una auditoría enfocada en el control de accesos privilegiados, define los criterios de evaluación y asigna tareas al equipo auditor.

- **Ejemplo 2:**

Durante la reunión de cierre, el auditor líder presenta los hallazgos a la gerencia de Jaguar Tech Solutions y propone un plan de mejora con prioridades.

### 2. Equipo Auditor

Ejecuta las **tareas técnicas** de la auditoría (revisión de registros, entrevistas, pruebas, análisis de evidencia).



- **Ejemplo 1:**

Un miembro del equipo revisa los logs de autenticación para detectar intentos de acceso fallidos y verifica si los umbrales de bloqueo están configurados correctamente.

- **Ejemplo 2:**

Otro auditor técnico entrevista al encargado de backups y revisa si las copias están cifradas, actualizadas y almacenadas fuera del sitio.

### **3. Auditados**

Corresponde al **personal que es evaluado**. Proporcionan información, responden preguntas y entregan evidencia.

- **Ejemplo 1:**

Un técnico de soporte entrega al equipo auditor el procedimiento que siguen para dar de baja cuentas de usuarios que salen de la empresa.

- **Ejemplo 2:**

Un usuario de un área de negocio muestra cómo accede al sistema ERP y qué controles hay para evitar filtraciones de información sensible.

### **4. Dueño del proceso (responsable del área auditada)**

Es el **encargado directo del proceso** o sistema que está siendo auditado. Tiene responsabilidad y autoridad para aplicar cambios.

- **Ejemplo 1:**

El CISO, como dueño del proceso de gestión de incidentes, responde por los tiempos de respuesta ante alertas y coordina planes de mejora.

- **Ejemplo 2:**

El jefe de infraestructura, como responsable del proceso de respaldo, acepta el hallazgo de que las copias no se prueban mensualmente y se compromete a implementar pruebas regulares.

**Resumen de los 4 roles clave:**

<b>Rol</b>	<b>Función principal</b>	<b>Ejemplo en Jaguar Tech Solutions</b>
<b>Auditor líder</b>	Planifica, dirige y supervisa la auditoría.	Auditor interno o externo a cargo del proceso.
<b>Equipo auditor</b>	Ejecuta las actividades: revisión técnica, entrevistas, análisis.	Especialistas en seguridad, consultores o analistas.
<b>Auditados</b>	Colaboran con la auditoría respondiendo y entregando evidencias.	Usuarios, técnicos, personal de soporte.
<b>Dueño del proceso</b>	Responsable directo del área o proceso auditado.	CISO, jefe de infraestructura, jefe de desarrollo, etc.



## Conclusión

La investigación realizada para la elaboración de este informe ha sido crucial para comprender conceptos relacionados al marco COBIT y la importancia de las auditorías de seguridad.

Una de las principales enseñanzas tiene que ver con los beneficios que traen los procesos de auditoría y si bien muchas veces parecen intrusivos lo cierto es que apuntan a mejorar sustancialmente los procesos de las organizaciones y su reflejo a nivel comercial al cumplir tanto con la normativa interna y externa, reforzando la confianza tanto de clientes como de socios estratégicos.

Entre las cosas que me gusta destacar es el hecho de todos los tipos de auditorías que existen, si bien en este documento se informa respecto de tres: Auditorías internas, externas y de cumplimiento, lo cierto es que hay varias de otro tipo que están englobadas dentro de las 2 primeras como son las auditorías financieras, operativas, de sistemas, forenses, etc. De este modo queda la puerta abierta para seguir investigando al respecto y no han sido incluidas en este documento para no alargarlo más allá de lo estrictamente necesario.

## Bibliografía

<sup>i</sup> COBIT: Key principles, and Aspects of Governance

<https://www.itamq.com/cobit/>

<sup>ii</sup> NORMA DE CARACTER GENERAL Nº 454

[https://www.cmfchile.cl/normativa/ncq\\_454\\_2021.pdf](https://www.cmfchile.cl/normativa/ncq_454_2021.pdf)

<sup>iii</sup> LEY 21.663 LEY MARCO DE CIBERSEGURIDAD.

<https://www.bcn.cl/leychile/navegar?i=1202434>

<sup>iv</sup> LEY 21.719 REGULA LA PROTECCIÓN Y EL TRATAMIENTO DE LOS DATOS PERSONALES Y CREA LA AGENCIA DE PROTECCIÓN DE DATOS PERSONALES

<https://www.bcn.cl/leychile/navegar?idNorma=1209272>

<sup>v</sup> Circulares emitidas por la CMF como por ejemplo la Circular n°2 entre otras

[https://www.cmfchile.cl/portal/principal/613/articles-30170\\_doc\\_pdf.pdf](https://www.cmfchile.cl/portal/principal/613/articles-30170_doc_pdf.pdf)

<sup>vi</sup> DACI Decision-Making Framework: Everything You Need to Know

<https://project-management.com/daci-model/>

<sup>vii</sup> Matriz RACI explicada paso a paso

<https://www.consuunt.es/matriz-raci/>

<sup>viii</sup> *Principales diferencias entre auditoría interna y externa*

<https://www.globalsuitesolutions.com/es/principales-diferencias-entre-auditoria-interna-y-auditoria-externa/>