**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

|  |  |
| --- | --- |
| PROGRAMA DE FORMACIÓN | Herramientas tecnológicas para la planeación estratégica, riesgo y cumplimiento |

|  |  |  |  |
| --- | --- | --- | --- |
| COMPETENCIA | 220601044  Monitorear sistemas de gestión de acuerdo con normativa y requerimientos técnicos | RESULTADOS DE APRENDIZAJE | 220601044-01 - Planificar los procesos de verificación del cumplimento según las estrategias de Gobierno Riesgo y Cumplimiento.  220601044-02 - Aplicar herramientas de evaluación y seguimiento acorde con procedimientos técnicos y normativa vigente.  220601044-03 - Analizar los hallazgos de la auditoría conforme a los resultados obtenidos de la herramienta tecnológica. |

|  |  |
| --- | --- |
| NÚMERO DEL COMPONENTE FORMATIVO | 09 |
| NOMBRE DEL COMPONENTE FORMATIVO | Verificación del cumplimiento según las estrategias de gobierno, riesgo y cumplimiento |
| BREVE DESCRIPCIÓN | El logro de objetivos organizacionales es posible en la medida en que se gestionen integralmente los riesgos dentro del cumplimiento de regulaciones nacionales y globales, y también en el marco de las buenas prácticas de gobierno corporativo. |
| PALABRAS CLAVE | Auditoría, cumplimiento de la regulación, estrategia empresarial, gestión de riesgos, gobierno corporativo, mejora continua, requisitos de norma, sistema de gestión. |

|  |  |
| --- | --- |
| ÁREA OCUPACIONAL | FINANZAS Y ADMINISTRACIÓN |
| IDIOMA | Español |

1. **TABLA DE CONTENIDOS**

**Introducción**

**1. Cultura de cumplimiento y gestión de riesgos.**

* 1. **Gobierno corporativo**
  2. **Gestión de riesgos**
  3. **Cumplimiento de la regulación**
  4. **Gobierno, Riesgo y Cumplimiento en la era digital**

**2. Auditoría de los sistemas de gestión según la ISO 19011**

**3. Sistema de Gestión de Cumplimiento según la ISO 37301**

1. **INTRODUCCIÓN**

En los últimos años, con la globalización y la complejidad de los mercados en la era digital, la incertidumbre ha aumentado significativamente para las organizaciones.

Los problemas éticos en grandes corporaciones, difundidos ampliamente por los medios de comunicación, como los de Enron (2001) y el banco BCCI (1986) de Estados Unidos, y la constructora Odebrecht (2015) en Latinoamérica, han causado perjuicios a los accionistas, a los trabajadores, proveedores, al medio ambiente, y a la sociedad en general. Ante tales escándalos corporativos, las regulaciones nacionales e internacionales han respondido con legislación para evitar se vuelvan a presentar tales delitos. También surgió la necesidad de desarrollar valores, vincularlos a una cultura organizacional de la ética, y así surge el concepto de gobierno corporativo.

Adicionalmente, nuevos elementos se han ido incorporando al panorama empresarial con los cambios en los modelos de negocios, que se aceleraron con motivo de la emergencia sanitaria global (2019); la llamada transformación digital, con el diseño de los productos y servicios centrados en las personas, hizo también que la gestión de gobierno, riesgo y cumplimiento cambiara de foco.

Video de Introducción

CF09\_0\_Video\_Introductorio

1. **DESARROLLO DE CONTENIDOS** 
   * + 1. **Cultura de cumplimiento y gestión de riesgos**

Tanto las personas como las organizaciones que deseen ser exitosas necesitan de valores y cumplimiento de normas. Los valores, la cultura y la integridad son los motores para el éxito sostenido de las empresas, bien sean privadas o estatales.

Se dice que una persona demuestra integridad cuando es honesta, actúa correctamente, sin afectar a otros. Los valores de las personas son los determinantes de la cultura de las organizaciones, y la cultura de la organización puede definir los riesgos en el logro de los objetivos.

Las organizaciones y las personas que deseen ser exitosas necesitan una cultura de cumplimiento evidente y genuina. Y los líderes de la organización, directores, gerentes, deberían predicar con el ejemplo, para que la cultura de cumplimiento sea adoptada por todos.

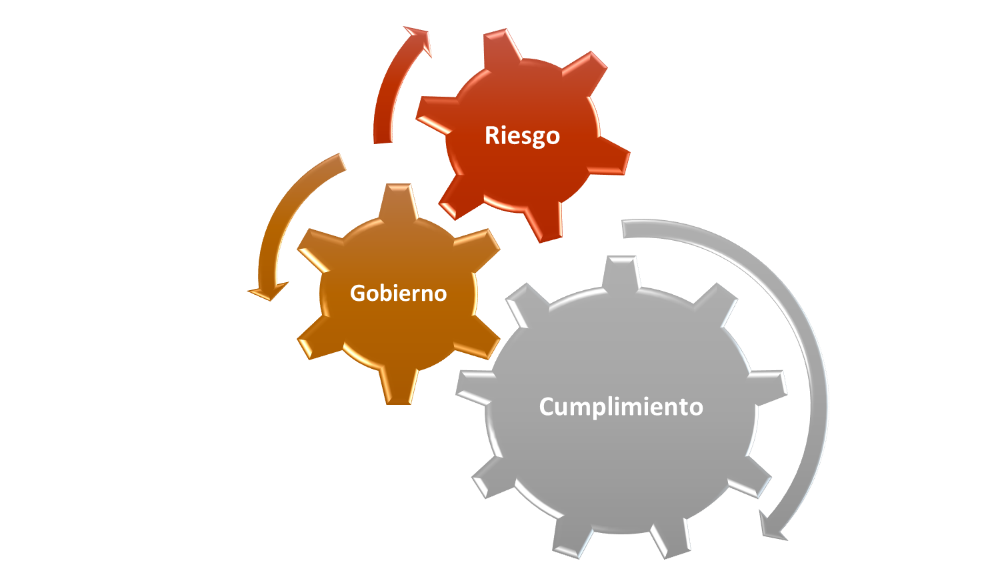
Tradicionalmente, las actividades de gestión de riesgo y el cumplimiento de la regulación se habían ejecutado como funciones independientes, y dado que las normas y los marcos de referencia tanto de gestión de riesgo como de cumplimiento comparten requerimientos comunes, se pueden presentar actividades redundantes y uso ineficiente de recursos.

De la necesidad de manejar las redundancias e ineficiencias surge el programa de GRC, con una visión integral denominada Gobierno, Riesgo y Cumplimento (*Governance, Risk and Compliance - GRC*), con el cual se deben identificar las correlaciones entre diferentes tipos de riesgos, elementos internos y entes regulatorios, considerando que el entorno es dinámico y tanto los riesgos como los requerimientos de cumplimiento están evolucionando permanentemente.

La siguiente figura ilustra la estrecha relación existente entre Gobierno, Riesgo y Cumplimiento GRC:

**Figura 1**

*Gobierno, Riesgo y Cumplimiento GRC*



* 1. **Gobierno corporativo**

El gobierno corporativo es el conjunto de normas, principios y procedimientos que regulan la estructura y el funcionamiento de los órganos de gobierno de una empresa. En concreto, establece las relaciones entre la junta directiva, el consejo de administración, los accionistas y el resto de las partes interesadas, y estipula las reglas por las que se rige el proceso de toma de decisiones sobre la compañía para la generación de valor (Deloitte, 2022).

El gobierno corporativo responde a las exigencias no solo por parte de inversores, sino también de los consumidores y de la sociedad que requieren saber cómo las organizaciones logran los resultados. Es por esto que cada vez adquiere mayor relevancia que las organizaciones sean gestionadas con transparencia, buenas prácticas y comportamiento responsable, para lograr mayores niveles de confianza y haciéndolas más atractivas, competitivas y sostenibles en el tiempo.

Por el contrario, la falta de buen gobierno corporativo es la causa de reportes de falsos registros contables, contratación sin criterios profesionales, aceptación de sobornos, desvío de dineros a cuentas personales, e innumerables situaciones que se han presentado en organizaciones. El tipo de gobierno corporativo depende del tipo de empresa; por ejemplo, las que cotizan en bolsa son presionadas a tener un gobierno corporativo sólido, requisito de normas de las comisiones de valores de cada jurisdicción.

Sin embargo, las prácticas de gobierno corporativo pueden y deben ser aplicadas a todas las empresas, sin importar el tamaño, porque, como se mencionaba al comienzo, cada vez es más fácil que se divulguen las faltas y sean de conocimiento de clientes y sociedad en general, a través de medios de comunicación y redes sociales, lo que también constituye riesgos reputacionales.

Las normas de gobierno corporativo articulan los componentes siguientes:

* Toma de decisiones y políticas corporativas.
* Mecanismos de control sobre el desempeño de la dirección ejecutiva.
* Cumplimiento del marco normativo.
* Relaciones entre órganos de gobierno, derechos y deberes de: consejo de administración, junta directiva y accionistas.

En cuanto a empresas del Estado, los principios de buen gobierno, la metodología de gestión del riesgo y el cumplimiento de normas son similares al sector privado, la diferencia principal es que el objetivo no es necesariamente maximizar el valor de los accionistas, sino proveer servicios y productos de acuerdo con los intereses y prioridades definidas por el Estado. Según se describe en DNP (s.f.), la práctica del buen gobierno busca mejores organizaciones, eficiencia de los recursos públicos y procesos de gestión, atracción y promoción de talento humano con excelencia para el servicio público, y mayor transparencia. También se mencionan los principios orientadores del ejercicio del buen gobierno:

* Transparencia y rendición de cuentas.
* Gestión pública efectiva.
* Participación y servicio al ciudadano.
* Vocación por el servicio público.
* Estrategias de lucha contra la corrupción.
  1. **Gestión de Riesgos**

Los estándares internacionales definen los riesgos como eventos que impiden el logro de los objetivos de las organizaciones. Y la gestión de riesgo es el conjunto de actividades que la organización realiza para entender y reducir los efectos de la incertidumbre en el logro de los objetivos. Por lo tanto, el primer paso en una gestión de riesgo es entender los objetivos de la organización en particular.

En el proceso de gestión de riesgos se identifican, analizan, mitigan y controlan los riesgos, hasta dejarlos en un nivel residual que sea aceptable por la organización.

La gestión de riesgo tradicionalmente se asocia al análisis cuantitativo, y exige conocimientos de probabilidades, finanzas, estadística y matemáticas. Pero también, por tener elementos de comportamiento humano, la gestión de riesgo requiere del componente psicológico, de habilidades de imaginación y persuasión para comunicar a las partes interesadas.

En la actividad de identificación de los riesgos, estos se pueden agrupar en categorías, que según la función se pueden clasificar de la siguiente manera:

Slide de Diapositivas

CF09\_1.0\_clasificacion\_riesgos\_funcion

* 1. **Cumplimiento de la regulación**

El “*compliance”* hace relación a los esfuerzos de las organizaciones por mitigar el riesgo legal. El cumplimiento puede tener una parte de obligaciones de cumplimiento **mandatorias** y otra parte de obligaciones de cumplimiento **voluntarias**.

Las obligaciones de cumplimiento mandatorias se refieren a las leyes que deben cumplir las empresas, pueden ser ambientales, laborales, leyes de lavado de activos, etc. Y las obligaciones de cumplimiento voluntarias están relacionadas con cumplimiento de obligaciones adquiridas por acuerdos con empleados, por ejemplo, obligaciones contractuales, requisitos de norma ISO, directrices, y también relacionadas con mitigar penas por delitos como el cohecho o la colusión, contienen elementos de autorregulación y se refuerzan con códigos internos de conducta (Cascón, 2021).

Cada organización debe cumplir regulaciones según el sector al que pertenece, e históricamente, los servicios financieros han sido de los más exigidos por las regulaciones en todos los países, junto con los de salud, alimentos, minería y transporte.

El riesgo legal se basa en reglas y, por tanto, es manejable con una estrategia de cumplimiento sólida y la implementación de un Sistema de Gestión de Cumplimiento (SGC); las pérdidas financieras por multas y los daños de reputación son evitables. Debido a la aprobación de leyes de responsabilidad penal para las personas jurídicas, en los últimos años, puede ser un mitigante del riesgo legal para las organizaciones tener implementado un SGC.

En términos generales, son elementos clave del programa de cumplimiento:

* El rol del oficial de cumplimiento.
* El mapa de riesgos.
* El plan de comunicación.
* Los códigos internos de conducta.
  1. **Gobierno, Riesgo y Cumplimiento en la era digital**

Hoy por hoy, las compañías se transformaron y se adaptaron a las nuevas condiciones, desarrollando nuevos productos y servicios basados en datos y explotando tecnologías emergentes con aplicaciones de *blockchain*, *Big data,* IoT, Inteligencia Artificial.

Debido al nuevo contexto, la gestión de riesgos debe incluir riesgos emergentes con estas características (SENA, 2020):

* Alta incertidumbre y falta de conocimiento sobre impacto e interacciones.
* Incremento de complejidad, interacciones emergentes y dependencias sistemáticas.
* Cambios en el contexto: político, económico, social, tecnológico y legal.

Se requiere entender el riesgo en el contexto digital, con las características de incertidumbre y complejidad, y aprender de los eventos para el desarrollo de la capacidad de resiliencia. La resiliencia de una organización se desarrolla con la combinación de factores estratégicos y operativos.

“La resiliencia organizacional es la capacidad de una organización para absorber y adaptarse en un entorno cambiante para permitirle cumplir sus objetivos y sobrevivir y prosperar. Las organizaciones más resilientes pueden anticipar y responder a amenazas y oportunidades, que surgen de cambios repentinos o graduales en su contexto interno y externo. Mejorar la resiliencia puede ser un objetivo estratégico de la organización y es el resultado de una buena práctica empresarial y una gestión eficaz del riesgo” (ISO, 2017).

Para generar la confianza digital, las organizaciones, entonces, ahora deben además de contar con el proceso de gestión de seguridad para garantizar la continuidad del negocio, también desarrollar capacidades de resiliencia para lograr mantener la operación del negocio a pesar de haber sido impactados por eventos de ciberseguridad.

**Marcos de referencia y estándares internacionales para el GRC**

El uso de marcos de referencia y estándares permite impulsar programas de Gobierno, Riesgo y Cumplimiento apropiados para cada organización. A continuación, se presentan algunos de los principales relacionados con este programa que se pueden adoptar de manera integral en las organizaciones:

Slide de Diapositivas

CF09\_1.1\_Marcos\_GRC

De acuerdo con la información anterior, son varias las organizaciones de profesionales que han trabajado en los últimos años en el desarrollo y madurez de normas y marcos de referencia. Estas organizaciones, además, ofrecen permanente formación a los asociados y profesionales interesados en adquirir las habilidades y competencias, también ofrecen exámenes de certificación en dichos marcos y normas, con el fin de que los profesionales demuestren su idoneidad para desempeñarse como consultores de los temas de riesgo y cumplimiento.

**2. Auditoría de los sistemas de gestiones según la ISO 19011**

Las auditorías son un proceso sistemático, independiente y documentado para obtener evidencias objetivas y evaluarlas de manera objetiva, con el fin de determinar el grado en que se cumplen los criterios de auditoría.

En esta sección, se hace referencia a la norma ISO 19011:2018 (ISO, 2018), que contiene las orientaciones sobre la auditoría de los sistemas de gestión, incluyendo los principios de la auditoría, la gestión de un programa de auditoría y la realización de auditorías de sistemas de gestión, y es aplicable a todas las organizaciones que necesitan planificar y realizar auditorías internas o externas de sistemas de gestión, o gestionar un programa de auditoría.

* **Tipos de auditoria**

Con base en la relación con el auditor y el auditado, existen tres tipos de auditoria:

Slide de Diapositivas

CF09\_2.0\_tipos\_auditoria

La norma ISO 19011:2018 hace referencia a las auditorías de primera y segunda parte. En algunos casos, se auditan varios sistemas de gestión de distintas disciplinas, por ejemplo: Sistema de Gestión de Calidad- SGC, de Seguridad de la Información- SI, de Gestión Ambiental- SGA, de Seguridad y Salud en el Trabajo- SSST, etc. En esos casos, se le denomina auditoría **combinada.** También se puede presentar la situación de auditar Sistemas Integrados en un único Sistema de Gestión; los principios y procesos de auditoría son los mismos que para una auditoría combinada, a veces llamada auditoría integrada.

* **Principios de la auditoría**

Los **principios** de la auditoria son declaraciones de filosofía, reglas o códigos de conducta, en este caso, relacionados con las auditorías:

Slide de Diapositivas

CF09\_2.1\_principio\_auditoria

Los 7 principios de auditoría ayudan a hacer del proceso una herramienta eficaz y fiable en apoyo de las políticas y controles de gestión. Es un requisito para el equipo de auditores adherirse a estos principios para proporcionar conclusiones pertinentes y suficientes de la auditoría realizada.

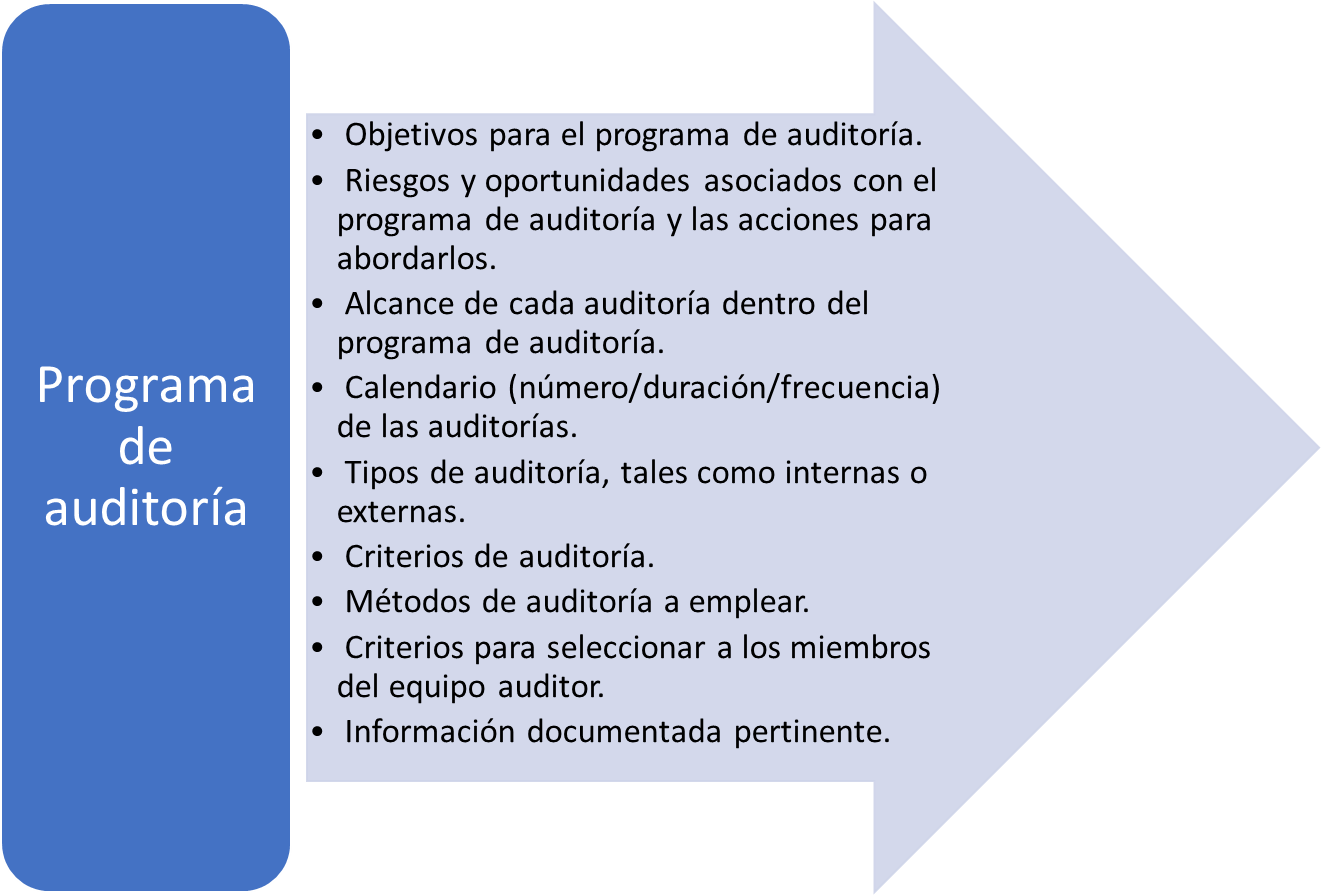
* **Programa de la auditoria**

El programa de auditorías hace referencia a un conjunto de auditorías planificadas para un periodo de tiempo determinado y dirigidas hacia un propósito específico. El programa depende del contexto del auditado, de los objetivos organizacionales, de las necesidades y expectativas de las partes interesadas, de los requisitos de seguridad y confidencialidad de la información.

La información que debe incluir el programa de auditoría se muestra a continuación.

**Figura 2.**

*Elementos del programa de auditoría*



* **Método establecido en la auditoría**

Elmétodo de auditoríaseleccionado depende de los objetivos de la auditoría, el alcance y los criterios definidos, así como de la duración y la ubicación. También la manera, el lugar y el momento en que se accede a la información de auditoría pueden determinar los métodos de auditoría y, según las circunstancias de la auditoría, pueden mezclar métodos o necesitar cambiarlos durante el proceso.

Según la auditoría se realice en las instalaciones del auditado, in situ, o a distancia, con o sin interacción entre personal auditado y equipo auditor, los métodos de auditoría pueden ser diferentes:

Slide de Diapositivas

CF09\_2.2\_Métodos

Las actividades de auditoría sin interacción humana con las personas que representan al auditado implican la interacción con los equipos, las instalaciones y la documentación, por ejemplo, revisión de registros, análisis de datos y muestrear productos.

La viabilidad de las actividades de auditoría a distancia puede depender del nivel de riesgo para el logro de los objetivos de la auditoría, el nivel de confianza que existe entre el auditor y el personal del auditado, y los requisitos reglamentarios. En las auditorías a distancia, se utilizan medios de comunicación interactivos para realizar las entrevistas, observar el trabajo realizado, completar cuestionarios y listas de verificación junto con el auditado.

* **Ciclo PHVA**

Planificar-Hacer-Verificar-Actuar, ciclo PHVA, es una estrategia de mejora continua en 4 pasos, también conocida como ciclo *Deming*.

El ciclo PHVA es una estrategia interactiva de resolución de problemas para mejorar procesos e implementar cambios en las organizaciones, ofrece un alto nivel de flexibilidad y mejora iterativa.

En las normas ISO, se destaca el “enfoque a procesos” y se sugiere el uso de esta metodología como una herramienta de mejora continua. Los auditores deben comprender que auditar un sistema de gestión es auditar los procesos de una organización y sus interacciones con una o más normas de sistemas de gestión.

Cuando las actividades se comprenden y se gestionan como procesos interrelacionados que funcionan como un sistema coherente, se logran resultados coherentes y predecibles de manera más eficaz y eficiente.

* **Gestión de un programa de auditoría**

En la gestión del Programa de Auditoría (PA), se cumple el ciclo de la mejora continua PHVA. En el capítulo 5 de la norma ISO 19011, en los numerales 5.2 a 5.7, se describen las actividades que deben seguir las personas responsables de gestionar el programa de auditoría (ISO, 2018).

El capítulo 6 de la norma ISO 19011 (ISO, 2018) comprende desde la preparación y realización de una auditoría, como parte de un programa de auditoría, hasta su seguimiento.

A continuación, se ilustra el **Ciclo PHVA**, incluyendo una breve descripción de los numerales correspondientes a la gestión de un programa y la realización de auditorías:

Pestañas verticales

CF09\_2.3\_Ciclo\_PHVA

**3. Sistema de Gestión de Cumplimiento según la ISO 37301**



Un SGC comprende: las políticas, los objetivos, y los procesos de “*compliance*”.

En la implementación de un SGC, como se especifica en la norma ISO 37301:2021 (ISO, 2021), se recorrerán de manera interactiva las fases del ciclo PHVA.

Las normas ISO tienen una estructura común y los numerales de la norma cubren todo el ciclo de la mejora continua, como se muestra en la siguiente figura, los numerales de ISO 37301. Requerimientos y guía de uso para el SGC:

**Figura 3.**

*Numerales norma ISO 37301 SGC*

En la figura se tiene:
ACTUAR 
10 Mejora.
PLANIFICAR
4 Contexto de la organización
5 Liderazgo
6 Planificación.
HACER
7 Apoyo
8 Operación.
VERIFICAR
9 Evaluación del desempeño.

Para cada numeral de la norma que contiene requisitos (cláusulas 4 al 10), existe una serie de actividades para desarrollar con el equipo de cumplimiento y representantes de los procesos que se abordan. También se realizan capacitaciones en todos los niveles, con el fin de desarrollar la cultura de cumplimiento, porque la responsabilidad del logro de los objetivos de cumplimientos es de todos, no solamente del oficial encargado o quien haga la función.

La implementación del SGC permite a la organización:

* La demostración eficaz, comprobable del cumplimiento de las obligaciones. Por ejemplo, leyes, reglamentos, acuerdos, contratos, código, directrices.
* La buena reputación de la organización.
* **Evaluación del desempeño**

Una vez implementados los procesos, realizadas las capacitaciones, que estén funcionando los mecanismos para la prevención, la detección y respuesta a situaciones de cumplimiento eventual o real, llega el momento de evaluar el desempeño en función del cumplimiento de los requisitos de la norma ISO 37301.

El desempeño corresponde a los resultados medibles, y se puede relacionar con la gestión de actividades, procesos, productos, servicios, sistemas u organizaciones.

En el numeral 9 de la norma 37301:2021, se describe la evaluación del desempeño del SGC, que corresponde a la fase Verificar (V) del ciclo PHVA.

A continuación, se describen los frentes de la evaluación de desempeño del SGC:

* **Realizar el seguimiento, medición, análisis y evaluación del sistema de gestión.**

Es necesario obtener valores para saber si se están logrando los objetivos de cumplimiento que estableció la organización en la fase anterior.

Para ello, se identifican las fuentes de retroalimentación del desempeño, se desarrollan indicadores, se elaboran informes, se mantienen registros.

Se puede decir que se hace seguimiento del sistema de gestión cuando se realizan verificaciones, supervisión y observaciones en forma crítica. Se debe definir a qué hacer seguimiento, cuándo y con cuáles métodos. Asimismo, determinar qué medir, cuándo, y con cuál método.

Se identifican las **fuentes** de información, clientes, proveedores, autoridades, empleados, leyes, auditorías internas, revisiones por la dirección, etc. Y las herramientas para obtener la información pueden ser encuestas de percepción, canales de denuncia, quejas, entre otras.

También se deben desarrollar **indicadores** de gestión apropiados para determinar si se están logrando los objetivos y para evaluar el desempeño en términos de cumplimiento. Los indicadores deben ser claros y comprensibles para todas las personas.

Cada organización puede organizar los indicadores según su conveniencia, su realidad, su contexto, e incluso, su nivel de conocimiento, lo importante es que tales indicadores soporten la toma de decisiones para mejorar el desempeño del SGC. Son ejemplo de indicadores: número de incidentes de protección de datos, tiempo para la investigación de denuncias, número de no conformidades de cumplimiento abiertas, entre otros.

El **informe** de cumplimiento que elabora periódicamente el oficial encargado o el equipo que tenga la función, sobre la base de criterios definidos, lo entrega al órgano de gobierno y a la alta dirección. La gestión eficaz del informe respectivo podría evitar que un problema de no cumplimiento se propague por la organización.

Algunas características del informe son:

* Debe detallar la obligación y cumplimiento correspondiente y los no cumplimientos que se produjeron.
* Mencionar los requisitos de las partes interesadas.
* Señalar las acciones correctivas implementadas y su eficacia.
* Mostrar los cambios eventuales en las obligaciones de cumplimiento y en el sistema de comunicaciones a utilizar, además de señalar antecedentes de auditorías y realizar monitoreo de los planes de acción para la mejora.

Los **registros** son parte de la información documentada del sistema de gestión, demuestran seguimientos y mediciones de los procesos. Corresponden a actas de revisión por la dirección, análisis de indicadores de gestión, seguimiento a las acciones correctivas, y los mismos informes de cumplimiento.

* **Auditorías internas**

La auditoría se trata de un proceso planeado, con objetivo establecido y enfocada en procesos. La auditoría debe ser transparente y hacer parte de un plan de auditoría.

En las auditorías, se revisa qué tan confiable es la organización, si respeta los pactos, cumple las promesas organizacionales y las normas.

La ejecución de la auditoría está a cargo del equipo auditor, con base en los conocimientos de los criterios de “*compliance*”, los requisitos y el contexto del auditado.

Los auditores deben tener habilidades y competencias para realizar la auditoría y una conducta profesional acorde con su rol, que garantice un ambiente de confianza.

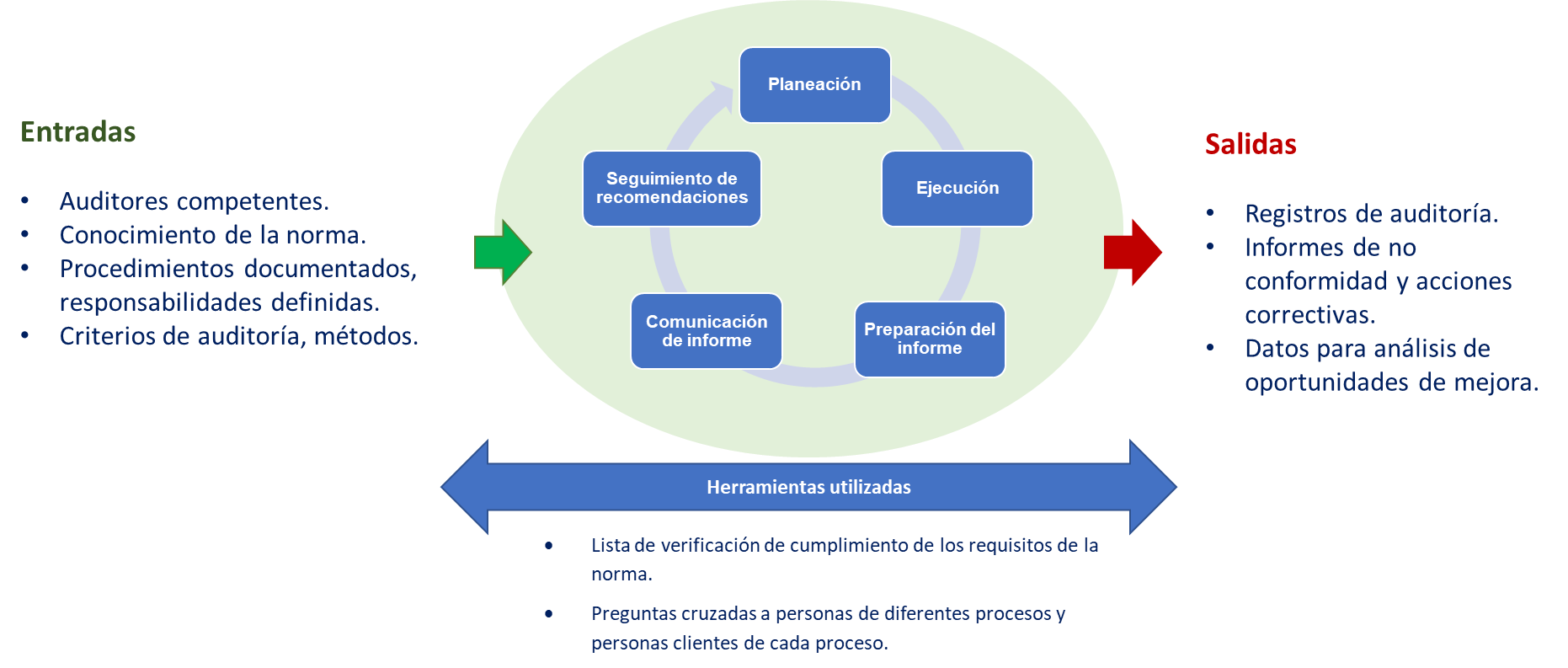
La auditoría no debe ser solo un ejercicio burocrático sin sentido, debe ser bien ejecutada, a la vez que entrega valor a la organización con la presentación de acciones apropiadas contenidas en el informe de auditoría. Este informe, es una entrada importante para las decisiones de la alta dirección, que potencialmente influyen en la gestión estratégica de la organización. El documento escrito debe demostrar el logro de los objetivos de auditoría, debe demostrar la eficacia del SGC, y debe identificar las no conformidades en el sistema de gestión y también las oportunidades de mejora.

Después de la auditoría interna, sigue la implementación de acciones correctivas para cerrar las no conformidades detectadas, lo cual es una oportunidad de aprendizaje para la organización (Thaller y Bravo, 2021).

La siguiente figura ilustra tanto el proceso como los elementos de entrada y salida de una auditoría:

**Figura 4.**

*Proceso de auditoría*



* **Revisiones por la Dirección**

La revisión por la dirección es un proceso liderado por la alta dirección y el órgano de gobierno, donde se toman las decisiones relacionadas con las oportunidades de mejora y aplicación de cambios, con el objetivo de mejorar el SGC.

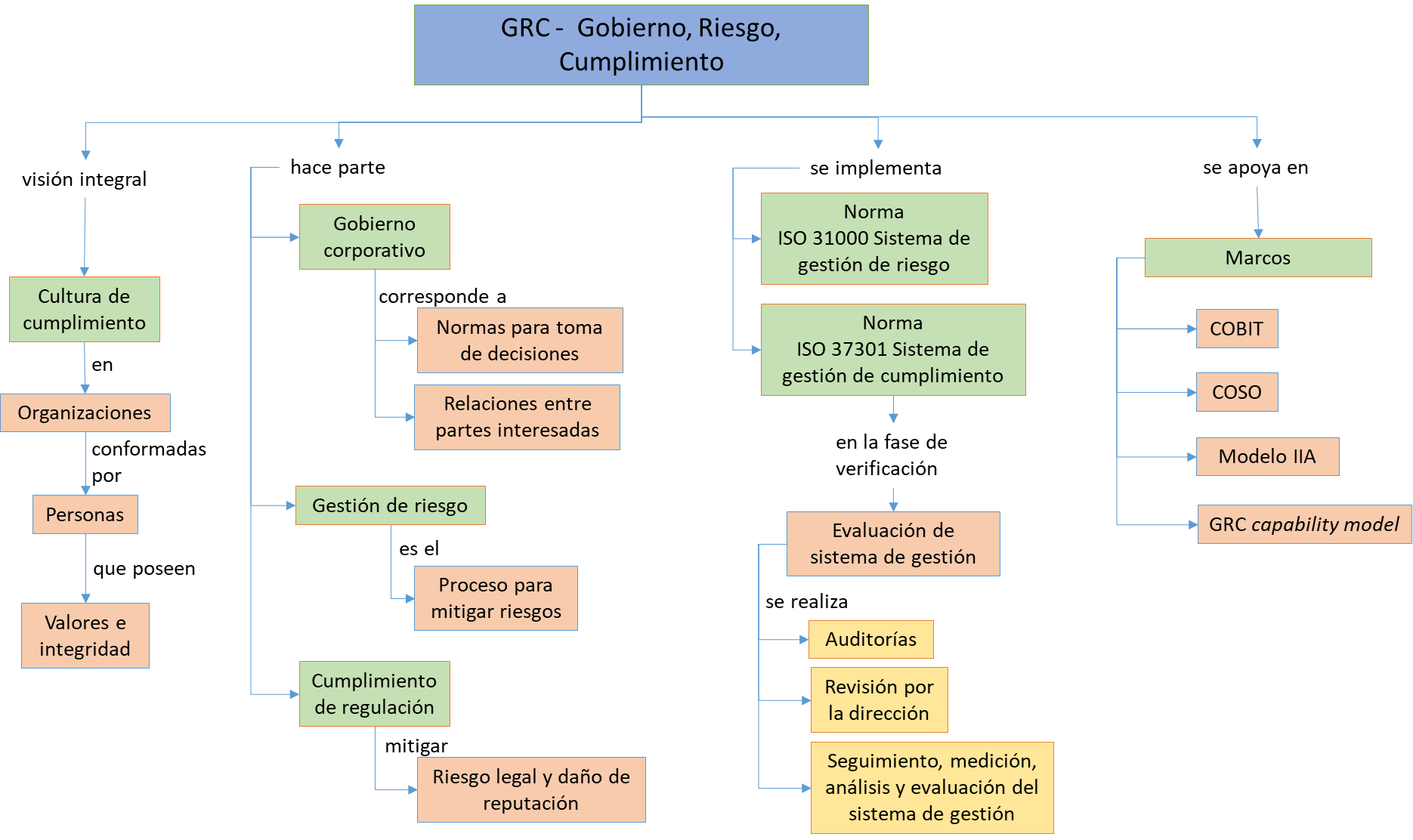
En la revisión por la dirección, se reconoce:

* Si las personas entienden la política de cumplimiento.
* Si se tomaron en cuenta los resultados de auditoría.
* Si las no conformidades fueron resueltas y cuáles acciones correctivas fueron implementadas.
* Se revisa la eficacia de los controles.
* Se toman en cuenta todos los registros frente a la violación de obligaciones de cumplimiento.
* Se evalúa si fueron suficientes los recursos asignados al SGC.

1. **SÍNTESIS**

El logro de los objetivos organizacionales es posible en la medida en que se desarrolle una cultura de cumplimiento y se gestionen integralmente los riesgos, dentro del marco de las buenas prácticas de gobierno corporativo. La implementación del sistema de gestión basado en la norma ISO 37301 se puede apoyar de buenas prácticas de los marcos de referencia relacionados con la gestión de riesgo, de gobierno TI y gobierno corporativo. En la evaluación del SGC, se realizan actividades de seguimiento, medición, análisis y evaluación, así como auditorías internas y la revisión por la dirección.

A continuación, se presenta una síntesis de las temáticas vistas en el componente formativo, a través del siguiente mapa conceptual:



1. **ACTIVIDADES DIDÁCTICAS**

|  |  |
| --- | --- |
| Nombre de la Actividad | Cuestionario Gobierno, Riesgo y Cumplimiento GRC |
| Objetivo de la actividad | Identificar los elementos relacionados con Gobierno, Riesgo y Cumplimiento GRC, para la implementación en las organizaciones. |
| Tipo de actividad sugerida | Cuestionario Selección múltiple |
| Archivo de la actividad | CF09\_ActividadDidactica\_cuestionario |

1. **MATERIAL COMPLEMENTARIO**

|  |  |  |  |
| --- | --- | --- | --- |
| Tema | Referencia APA del Material | Tipo de material | Enlace del Recurso o  Archivo del documento o material |
| 1. Cultura de cumplimiento y gestión de riesgos. | SENA. (2020). *Aplicabilidad de Caso Práctico en Gobierno, Riesgo y Cumplimiento - GRC - SENA* (Video). YouTube. | Video | <https://www.youtube.com/watch?v=yguzJDDvjDA> |
| 2. Auditoría de los sistemas de gestión según la ISO 19011 | ISO Expertos. (2016). *Los 11 secretos para realizar una auditoría que agregue valor* (Video). YouTube. | Video | <https://www.youtube.com/watch?v=fN5nC7uGNFc> |

1. **GLOSARIO**

|  |  |
| --- | --- |
| TÉRMINO | SIGNIFICADO |
| Arquitectura | Conjunto de elementos, sus interrelaciones y factores externos que gobiernan su diseño, su comportamiento y su evolución. |
| *BiSL- Business Information Services Library* | Marco utilizado para la gestión de la información regida por la Fundación *ASL BiSL* (anteriormente, *ASL Foundation*). |
| *CIO – Chief Information Officer* | Director de tecnologías de la información y las comunicaciones, es el ejecutivo que se encarga de que la organización logre el mejor rendimiento posible a través del uso de tecnologías de la información (TI). |
| *CISO -Chief Information Security Officer* | Rol desempeñado a nivel ejecutivo, corresponde al director de seguridad de la información. |
| Cibernética | Permite conceptualizar la comunicación como una ciencia de relaciones y mediaciones socio técnicas entre seres humanos y objetos de diferente naturaleza. |
| Cohecho | Este delito consiste en el soborno a un funcionario público, nacional o extranjero. |
| Colusión | Es el delito de ponerse de acuerdo para defraudar al Estado. |
| Eficacia | Grado en el que se realizan las actividades planificadas y se logran los resultados planificados. |
| ISO- Organización Internacional de Normalización | Federación mundial de organismos nacionales de normalización, que, a través de comités técnicos de ISO, elabora Normas Internacionales. |
| Marcos de referencia | Conjunto de métodos, herramientas y lenguaje común. |
| Mandatorio/a | Del inglés “*mandatory*”, y este del lat. tardío “*mandatorius*”, relativo a un mandato o encargo. Sinónimos: obligatorio, forzoso. |
| Resiliencia | Capacidad de absorber y adaptarse en un entorno cambiante. (ISO, 2017) |
| Riesgos cibernéticos | Los ciberriesgos son riesgos que tienen al menos tres características claves: son sistémicos (tienen efecto en cascada), emergentes (surgen como fruto del nivel de acoplamiento e interacción de diversos componentes) y disruptivos (generan efectos inesperados sobre la dinámica del sistema), los cuales están presentes en el entorno ciberfísico, lo que se traduce en una convergencia entre lo físico, lo lógico y lo biológico, como fundamento de la dinámica de la Cuarta Revolución Industrial. (Cano, 2019) |
| Gobierno, Riesgo y Cumplimento -GRC | OCEG (2022) [define a GRC](https://www.oceg.org/about/what-is-grc/) como "la colección integrada de capacidades que permiten a una organización alcanzar objetivos de manera confiable, abordar la incertidumbre y actuar con integridad". |
| Transformación Digital | Es la adaptación continua de los negocios a las exigencias del entorno cambiante. Es un enfoque centrado en el cliente que utiliza tecnologías digitales para aprovechar los datos e impulsar flujos de trabajo inteligentes. Entre las tecnologías utilizadas actualmente y en el futuro cercano, tenemos la Inteligencia Artificial, la automatización, IoT, nube híbrida, *Blockchain* y Microservicios.  El objetivo de la transformación digital es construir una base técnica y operativa para evolucionar y responder de la mejor manera posible a las expectativas impredecibles y cambiantes de los clientes, las condiciones del mercado y los eventos locales o globales. |
| Tráfico de influencias | Es el intercambio de un bien por la promesa de interceder en el ámbito judicial. |

1. **REFERENCIAS BIBLIOGRÁFICAS**

Cano, J. (2019). Ciberriesgo. Aprendizaje de un riesgo sistémico, emergente y disruptivo. *Revista SISTEMAS. Asociación Colombiana de Ingenieros de Sistemas*, (151), p. 63-73. <https://doi.org/10.29236/sistemas.n151a5>

Cascón, J. (2021). *GRC Gobierno Corporativo, Riesgo y Cumplimiento*. <https://www.researchgate.net/profile/Javier-Ismodes-2/publication/348280507_GRC_JIC_v70/links/5ff6225e45851553a02626da/GRC-JIC-v70.pdf>

Deloitte. (s. f.). *¿Qué es el gobierno corporativo? Transparencia y confianza*. <https://www2.deloitte.com/es/es/pages/governance-risk-and-compliance/articles/que-es-el-gobierno-corporativo.html>

Departamento Nacional de Planeación [DNP]. (s. f.). Rutas especializadas para la formulación de los Planes de Desarrollo Territoriales. *Buen Gobierno.* <https://www.funcionpublica.gov.co/documents/418537/28834001/Rutas+Especializadas+Buen+Gobierno.pdf/3eb8f83c-dec8-3d4e-461b-84f68a836591>

Fundación Latinoamericana de Auditores Internos [FLAI]. (2020). *El Modelo de las Tres Líneas del IIA 2020*. <https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-spanish.pdf>

ISACA. (s. f.). *COBIT. An ISACA Framework*. <https://www.isaca.org/resources/cobit>

ISO Expertos. (2018). *Los 11 secretos para realizar una auditoría que agregue valor* (Video). YouTube. <https://www.youtube.com/watch?v=fN5nC7uGNFc>

OCEG. (s. f.). *What Is GRC?* <https://www.oceg.org/about/what-is-grc/>

Organización Internacional de Normalización [ISO]. (2017). *Security and resilience — Organizational resilience — Principles and attributes* (ISO 22316). <https://www.iso.org/obp/ui#iso:std:iso:22316:ed-1:v1:en>

Organización Internacional de Normalización [ISO]. (2018a). *Directrices para la auditoría de los sistemas de gestión* (ISO 19011). <https://www.iso.org/obp/ui#iso:std:iso:19011:ed-3:v1:es>

Organización Internacional de Normalización [ISO]. (2018b). *Gestión del riesgo – Directrices* (ISO 31000)*.* <https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es>

Organización Internacional de Normalización [ISO]. (2021). *Compliance management systems — Requirements with guidance for use* (ISO 37301)*.* <https://www.iso.org/obp/ui/#iso:std:iso:37301:ed-1:v1:es>

SENA. (2020). *Aplicabilidad de Caso Práctico en Gobierno, Riesgo y Cumplimiento - GRC - SENA* (Video). YouTube. <https://www.youtube.com/watch?v=yguzJDDvjDA>

Thaller, E. y Bravo, J. (2021). *Beyond Compliance: Aplicación de la Norma ISO 37301 en cualquier organización interesada en el compliance.* Paton Professional. <https://books.google.com.co/books?id=-dxCEAAAQBAJ&pg=PT60&hl=es&source=gbs_selected_pages&cad=2#v=onepage&q&f=false>

1. **CONTROL DEL DOCUMENTO**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Nombre | Cargo | Dependencia | Fecha |
| Autor(es) | Dolly Stella Carrillo Vega | Experta Temática | Regional Norte de Santander - Centro de la Industria, la Empresa y los Servicios | Noviembre 2022 |
| Gustavo Santis Mancipe | Diseñador Instruccional | Regional Distrito Capital – Centro de Gestión Industrial | Noviembre 2022 |
| Silvia Milena Sequeda Cárdenas | Asesora Pedagógica y Metodológica | Regional Distrito Capital – Centro de Diseño y Metrología | Diciembre de 2022 |
| Rafael Neftalí Lizcano Reyes | Responsable Equipo Desarrollo Curricular | Regional Santander - Centro Industrial del Diseño y la Manufactura | Diciembre de 2022 |
| Darío González | Corrector de Estilo | Regional Distrito Capital – Centro de Diseño y Metrología | Diciembre de 2022 |

1. **CONTROL DE CAMBIOS**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Nombre | Cargo | Dependencia | Fecha | Razón del cambio |
| Autor(es) | Humberto Arias Díaz | Diseñador Instruccional | Regional Tolima – Centro de Comercio y Servicio | Octubre 2023 | Revisión y actualización. |
| María Inés Machado López | Revisora metodológica | Regional Tolima.  Centro de Servicios y Comercio | Noviembre 2023 | Revisión de cambios 2023, revisión metodológica. |