

Técnicas de comunicación, evaluación, seguridad y confidencialidad

**Breve descripción:**

Este componente se centra en identificar las técnicas de comunicación, evaluación de la seguridad y confidencialidad de la información según la norma ISO 27000, requisitos y aplicación. Así mismo como implementar la verificación del sistema de auditoría.

**Octubre 2023**

Tabla de contenido

[Introducción 1](#_Toc147857684)

[1. Técnicas de comunicación 3](#_Toc147857685)

[1.1. Revisión del proceso 15](#_Toc147857686)

[1.2. Verificación del sistema 23](#_Toc147857687)

[2. Seguridad y confidencialidad de la información 26](#_Toc147857688)

[2.1. ISO 27000 30](#_Toc147857689)

[2.2. Requisitos aplicables según la norma 36](#_Toc147857690)

[Síntesis 40](#_Toc147857691)

[Material complementario 42](#_Toc147857692)

[Glosario 44](#_Toc147857693)

[Referencias bibliográficas 45](#_Toc147857694)

[Créditos 47](#_Toc147857695)

Introducción

La comunicación es un proceso de transmisión de información técnica por diferentes medios entre los que se identifica el oral y el escrito con el objetivo de informar frente alguna situación y que esta sirva para tomar decisiones. Es importante que se maneje correctamente en las organizaciones y su funcionalidad en los planes de auditoría donde se verifican criterios, requisitos y cumplimiento de normas.

Es por esto, que en este componente formativo se conocerá la importancia de implementar técnicas de comunicación, sus elementos, tipos de información y el proceso de recopilación de información en una auditoría. También implementar herramientas de control mediante listas de verificación en los procesos de auditoría, se invita a explorar el video que se presenta a continuación que da una introducción temática:

1. Técnicas de comunicación, evaluación. Seguridad y confidencialidad



[**Enlace de reproducción del video**](https://youtu.be/P2Uzg0Wx2No)

|  |
| --- |
| **Síntesis del video: Técnicas de comunicación, evaluación, Seguridad y confidencialidad** |
| Se ofrece información detallada acerca de los diversos instrumentos y métodos utilizados para verificar y evaluar los criterios de seguridad en un sistema de gestión, este enfoque se centra en dotar a los participantes de las habilidades necesarias para evaluar la efectividad de las medidas de seguridad implementadas en un contexto organizacional; además se abordan los criterios relacionados, con la comunicación y el manejo de la información empleados en varios programas de auditoria, el objetivo es adquirir competencias fundamentales en la gestión y la comunicación efectiva de los hallazgos y resultados de las auditorías a las partes interesadas. |

## Técnicas de comunicación

Cuando se habla de técnicas de comunicación, es fundamental comprender primero el significado de la comunicación. La comunicación es el medio a través del cual una persona establece contacto con otra, dando lugar a un intercambio de información y creando una comprensión mutua al transmitir un mensaje entre el emisor y el receptor. La comunicación es la manera en que las personas se comprenden entre sí y consta de cuatro elementos esenciales, los cuales se mencionan en el siguiente video:

1. Elementos de la comunicación



[**Enlace de reproducción del video**](https://youtu.be/uyfkdAMQAI8)

|  |
| --- |
| **Síntesis del video: Elementos de la comunicación** |
| Los procesos de comunicación son dinámicos y se encuentran en constante cambio, por el simple hecho que el ser humano está asociado y es un actor principal en ellos, dentro de esta dinámica, es posible detener el proceso un momento para identificar los elementos que componen la comunicación. |

Estos elementos permiten que la comunicación sea parte fundamental de nuestra vida diaria. Una comunicación eficaz requiere el dominio de buenas técnicas para interactuar con los demás, ya que la forma en que expresamos un mensaje puede influir en cómo se interpreta y se comprende. Es importante tener en cuenta que no se aplican las mismas reglas de comunicación al hablar con un amigo que al redactar un trabajo para la clase. Reconocer las diferencias entre estos dos contextos ayudará a lograr una comunicación exitosa en todas las circunstancias. A continuación, se definen los tipos de comunicación que se utilizan en las empresas:

La comunicación oral es una forma de expresión de los seres humanos que implica el uso de palabras habladas. Esta comunicación puede variar en tono, volumen, velocidad y claridad. Se produce cuando dos o más personas que comparten el mismo idioma interactúan y se transmite a través del aire o, en algunos casos, mediante dispositivos electrónicos.

La comunicación escrita se lleva a cabo a través de palabras y códigos escritos. En este tipo de comunicación, tanto el emisor como el receptor deben compartir el conocimiento del código utilizado para lograr una comunicación efectiva. La buena ortografía y la comprensión lectora son fundamentales para transmitir el mensaje con éxito según lo previsto.

Es importante tener en cuenta las siguientes técnicas a la hora de querer comunicar.

1. **Preparar el mensaje**

Es necesario tener muy claro lo que se piensa decir, trasmitir e influir por medio de lo que estás hablando por eso tener un buen mensaje estructurado permite la fluidez y la comunicación clara y precisa entre el emisor y el receptor.

1. **Mirar y practicar**

En la mayoría de los casos todos tenemos un factor en contra y nos juega una mala pasada a la hora de comunicarnos, haciendo que tengamos nervios y nos enredemos a la hora de dar el mensaje, es por eso que es muy importante detectar nuestros defectos y poder ir mejorando poco a poco, de este modo, poder tener una buena oratoria a la hora de expresarse ante los demás.

1. **Ser preciso y claro con el mensaje**

Es necesario tener un mensaje preciso y claro sobre la idea que se quiere decir, sin alargar tanto el mensaje con solo palabras de rellenos que no conducen al mensaje directo y hace que el receptor se incomode o moleste.

1. **Tener confianza**

La confianza es algo muy importante a la hora de expresarnos, si no confiamos en nosotros mismos no podremos ser fluidos en la comunicación, ya que seremos muy tímidos a la hora de expresarnos.

1. **Escuchar al receptor**

El saber escuchar es algo muy importante a la hora de comunicarnos, ya que, si la persona no es capaz de respetar el espacio del emisor a la hora de comunicarse o dar el mensaje, posiblemente nunca vaya a entender nada y ocurran desacuerdos por falta de compresión.

1. **Dominar gestos**

Muchas veces no nos damos cuenta de los gestos que realizamos a la hora de hablar, por lo cual estos gestos son mal vistos por el receptor o los receptores, es por eso que debemos tener un control de nuestros propios gestos que inconscientemente hacemos.

**La información en una organización**

La información es un grupo de datos que al ser organizados tienen la posibilidad de generar un mensaje con base en hechos. La información es el mensaje que un emisor busca transmitir a través de un conjunto de datos que conforman un reporte pretendiendo ser llegado al receptor, la información siempre se da por medio de un canal entre el emisor y el receptor.

En una organización la información juega un papel muy importante ya que permite que las personas requieran de conocimientos previos para la toma de decisiones. Para que la información pueda ser de gran utilidad es necesario que tenga:

* Exactitud
* Oportunidad
* Pertinencia
* Integridad
* Frecuencia
* Margen de tiempo
* Alcance
* Origen
* Presentación

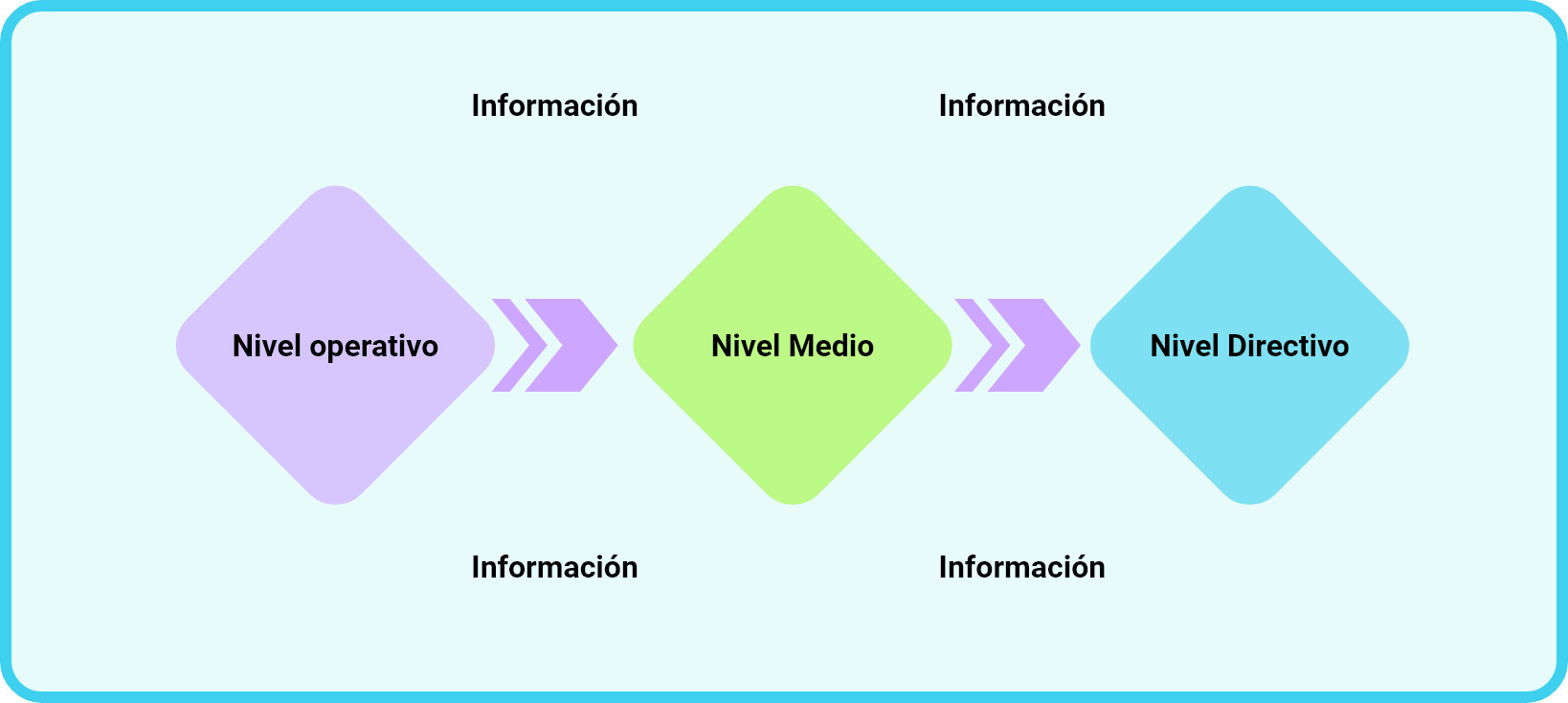
La necesidad de la información de una organización cambia dependiendo de la naturaleza del trabajo, la actividad a hacer y las metas que se quieran obtener, varían de consenso al grado que ocupen los individuos en la organización, o sea, los directivos necesitan de más información que los técnicos para lograr desarrollar su trabajo y estar sujetos a la naturaleza interna o externa.

Por otro lado, la necesidad de contar con información es de gran importancia para las organizaciones, al mismo tiempo toda empresa necesita tener acceso a la mayor cantidad de información posible. No importa el área funcional de la empresa, cada uno de los elementos que la integran necesitan en mayor o menor grado.

Para el nivel directivo en una empresa, la información es utilizada para diseñar estrategias y trazar el camino que se debe seguir, por tal motivo es de vital importancia que esta información sea oportuna y especifica. En el área intermedia de la información se utiliza para diseñar estrategias específicas que permitan el logro de los objetivos que se establecieron en el nivel directivo. Por otro lado, en el nivel operativo, la información se detallada en los procesos, productos, actividades que los trabajadores necesitan para llevar a cabo las tareas de sus respectivas áreas.

A continuación, se revisará cómo es el manejo de la información en una organización en los diferentes niveles.

**Figura 1.** Manejo de la información



Nota. El arte del manejo de la información y la información difusa. Huerta. (2016).

**Información Información**

**Nivel operativo Nivel medio Nivel directivo**

**Información Información**

La información está inmersa en cualquier actividad de la vida cotidiana y por tanto es de gran importancia para entender un asunto a realizar en cualquier ámbito, ya sea en el trabajo o en cualquier otro campo. La información es necesaria e importante para cualquier proceso que realice una organización, pues permite que se evite cometer errores, existen cinco (5) tipos de información, los cuales son:

1. **Información confidencial**

Es un tipo de información sensible que está restringida por las leyes o regulada para clases particulares de individuos. Hace falta una habilitación formal de estabilidad para manejar y entrar a documentos clasificados. Hay habitualmente 4 grados de sensibilidad de la información, cada cual con diversos tipos de autorizaciones de estabilidad.

1. **Información pública**

Es aquella información que, cualquier persona que sea su soporte y forma de expresión, obre en poder de las Administraciones Públicas a las que hace referencia la ley y los organismos públicos vinculados o dependientes en su poder.

1. **Información personal**

Se refiere a los datos que vinculan potencialmente a un sujeto específico. Cualquier información que podría ser usada para diferenciar una persona de otra, y que podría ser utilizada para quitarle el anonimato a los datos anónimos.

1. **Información interna**

La información interna son datos que se generan a partir dentro del comercio, que cubre zonas como operaciones, mantenimiento, personal y finanzas.

1. **Información externa**

La información externa es la que proviene del mercado, consumidores y participantes. Es algo como estadísticas de encuestas, formularios, averiguaciones y comentarios de los consumidores.

La información tiene como características.

* Su significado
* Su importancia
* Vigencia
* Validez
* Valor

La evaluación de la información es un proceso que se utiliza para decidir de forma sistemática, el mérito, el costo y el sentido de un trabajo, alguna capacidad intelectual, física o de alguien en funcionalidad de ciertos criterios en relación con un grupo de reglas. Comúnmente se utiliza para caracterizar y ver el rendimiento que se lleva dentro de una organización, verificando que la información con la que se trabaja es confiable. Cuando se habla del manejo de la información, se habla también de la información difusa, así que por lo tanto la información difusa es, según Rosas Sánchez (2012), “es el conjunto organizado de datos que constituye un mensaje sobre un cierto fenómeno o entidad pero que tiene la característica de ser poco clara, exacta o concreta”.

La información difusa se comprende como el grupo de datos que difícilmente tienen la posibilidad de ser procesados o analizados para obtener información veraz que logre ofrecer los instrumentos elementales a las personas y los guíe en la toma de elecciones. Es fundamental que en el funcionamiento de los datos acerca de la información difusa, participen las piezas que se delegan de generarla. Además, se necesita que la alta dirección de la organización logre procesar la información para establecer su nivel de utilidad. Hay ciertos puntos que tienen la posibilidad de tener en cuenta para ofrecer claridad en el desempeño de la información difusa, los cuales son:

* Inquietud de conocimiento.
* Búsqueda de información.
* Obtención de información difusa.
* Uso de herramientas.

A continuación, se puede analizar el proceso del manejo de la información difusa para las organizaciones.

* Necesidad de información
* Búsqueda de información
* Obtención de todo tipo de información
* Uso de herramientas para localizar y obtener información clara y precisa
* Evaluación de la información
* Procesamiento y producción de la información
* Toma de decisiones

**Preparación de la información documentada para la auditoría**

La preparación de la información documentada es una actividad clave en la planificación de las auditorías. En esta etapa, el equipo auditor se encarga de recopilar y revisar la información de la empresa que se va a auditar, lo que les permite:

* Preparar la realización de la auditoría mediante listas de chequeo, ya sean físicas o digitales.
* Definir técnicas y detalles de muestreo apropiados de acuerdo al tamaño de la organización y sus procesos.
* Garantizar que al final de la auditoría se disponga de la información documentada y que se cumplan con los requisitos.

La imagen y expresión corporal del auditor es vital en esta relación con sus auditados, por lo que es importante tener en cuenta:

* **Puntualidad:** el auditor debe llegar a la hora acordada, ni antes ni después, para cumplir con el cronograma de la auditoría y respetar el tiempo de las personas involucradas en el proceso.
* **Vestuario:** el auditor debe adecuarse al entorno de auditoría, los procesos o departamentos a visitar, utilizando la vestimenta apropiada según la normativa y las prácticas de la empresa auditada.
* **Imagen del auditor:** debe transmitir seguridad, control, orden y limpieza, para establecer una impresión profesional y generar confianza en el auditado durante el proceso de auditoría.
* **Comunicación verbal:** el auditor debe cuidar su tono de voz transmitiendo seguridad y tranquilidad, con el fin de evitar poner nervioso al auditado y fomentar una interacción efectiva durante la auditoría.
* **Comunicación no verbal:** el auditor debe cuidar en todo momento su expresión corporal, ya que esta puede influir significativamente en la percepción de los auditados y en la efectividad de la comunicación durante la auditoría.

Los métodos y técnicas de auditoría son variables y dependen de factores como la organización, los procesos, la ubicación o los lugares de la auditoría, así como los objetivos y criterios establecidos.

En este sentido, es recomendable que el auditor inicie con preguntas abiertas y luego vaya cerrándolas para confirmar y verificar la información.

Cuando se seleccionan los tipos de preguntas para la auditoría, es importante conocer algunas metodologías que ayudarán al auditor a alcanzar los objetivos planificados.

Las preguntas pueden clasificarse según su finalidad funcional, como se muestra en la siguiente tabla:

**Tabla 1.** Tipos de preguntas para realizar auditorías

|  |  |
| --- | --- |
| **Tipos de preguntar** | **Definición** |
| Preguntas abiertas | Permiten conocer las generalidades de los procesos. |
| Preguntas cerradas | El auditor utiliza esta pregunta para obtener información concreta, realizar verificación o comprobación de los datos obtenidos, son preguntas que no dan opciones al auditado, solo debe responder “sí” o “no”. |
| Preguntas hipotéticas | Se utilizan para comprobar la planificación de un proceso, una actividad o situación que no ha ocurrido pero que el sistema de gestión debe tener en cuenta. |
| Preguntas de aclaración | Son preguntas realizadas por el auditor para aclarar la respuesta recibida con anterioridad. |

**Técnicas de redacción**

La redacción es el proceso por medio del cual se compone un discurso escrito, definiéndose como un arte, pero sin embargo constituyéndose como una técnica. Es la medida que se usa para comprobar que un escrito tenga coherencia. Es el acto en el que se pone por escrito un grupo de ideas ordenadas de manera lógica y coherentemente, teniendo como objetivo la creación de un texto en el cual el mensaje se transmita con una intención definida. De acuerdo a lo mencionado, se pueden definir las siguientes técnicas de redacción:

* **Descripción:** es un discurso (oral o escrito) que detalla y explica las propiedades de un espacio, persona, cosa o situación.
* **Búsqueda de información:** es el relato de unos hechos reales o imaginarios que les suceden a unos personajes en un espacio.
* **Exposición:** el acto de exponer de forma oral o redactada un asunto o tema para un auditorio.
* **Argumentación:** es una exposición de información cuya finalidad es enseñar, por medio de razonamientos lógicos, la validez de un criterio, una crítica o una visión, y paralelamente persuadir a los interlocutores o llamarlos a la acción.
* **Diálogo:** es la comunicación en la que ocurre un intercambio de información entre dos o más personas. Podría ser oral o escrito.
* **Resumen:** es un escrito que se usa para sintetizar las ideas más resaltantes de un texto de manera concisa, estructurada y coherente.

La ortografía es una sección de la gramática que se encarga de la manera más adecuada de redactar los vocablos, cuyo primordial uso es la comunicación, y para lograr esta conexión con la realidad, se necesita que se elaboren los mensajes de manera idónea y comprensible.

Las técnicas de la ortografía son muchas, por lo cual una buena ortografía parte directamente de cada una de las personas en su deseo de mejorar y ser cada día más perfecto a la hora de escribir, por lo tanto, unas de las técnicas para tener en cuenta son:

* Realizar un listado de palabras que generen dificultad al escribir.
* Revisar y conocer las reglas para prefijos y sufijos.
* Memorizar los conjuntos de palabras especiales.
* Leer.
* Fortalecer la memoria visual.
* Practicar la redacción.
* Conocer la utilización de signos de puntuación.
* Conocer el significado de las palabras.

## Revisión del proceso

Un proceso es una serie de ocupaciones que conducen a construir un fin definido. Un proceso se trata entonces, generalmente, de una sucesión de operaciones llevadas a cabo en orden específico y con un objetivo.

En las auditorías, existe un proceso en el cual la teoría y la práctica son ocupaciones administrativas de revisión de documentos y de labores ejecutadas dentro del sistema benéfico de la organización, para la verificación de cumplimiento de la normativa y los métodos internos en sus rutinas cotidianas.

En este sentido, el auditor debería utilizar ciertas técnicas, como entrevistas con todos los jefes departamentales, observación directa de las ocupaciones y los procesos de ejecución y, finalmente, la revisión de todos los registros accesibles para asegurar el cumplimiento de los sistemas de calidad, legislación del gobierno y fiscal, así como de las reglas de estabilidad internas.

Como todo proceso auditor, este proceso consta de 6 etapas, las cuales son fundamentales para poder realizar el proceso de auditoría de manera correcta, esos puntos son:

1. **Reunión inicial**

Es un paso forzoso y, más allá de aquello, sustancial para una auditoría. En esta junta deberían estar presentes los representantes o directores de la organización auditada, en el instante que sea más apropiado para cada una de las piezas, así como los ayudantes de la compañía que permanecen al mando de los procesos auditables. El valor de eso radica en el hecho, de brindarle a las piezas relacionadas en el proceso una guía inicial empero breve de las ocupaciones siguientes. Para evadir la mayor parte de los malentendidos o conflictos que logren surgir en esta actividad.

1. **Abrir los canales de comunicación**

El segundo paso es implantar claridad en el hecho de que el auditado o auditados tienen la posibilidad de manifestar en todo instante sus preocupaciones y dudas al equipo responsable para borrar cada una de las preguntas o confusiones del proceso. Asimismo, los auditores tienen que comunicarle al equipo de la organización o a los relacionados en la junta inicial de los progresos de la actividad y tenerlos al tanto de los adelantos y descubrimientos a fin de brindar transparencia en todo instante.

1. **Establecer las responsabilidades del equipo auditor**

Así sea que una sola persona o un equipo de auditores, es importante establecer el papel de cada uno a lo largo del proceso de auditoría para facilitar todo su desarrollo. En esta actividad, hay observadores que su labor se resume en el registro visual de las ocupaciones y procesos en la productividad rutinaria de la compañía y decidir probables malas prácticas o incumplimientos de la normativa. Son profesionales en que intervienen en las ocupaciones cotidianas de la organización y ajustan las prácticas para asegurar la total legalidad y calidad de los procesos.

1. **Recopilación y verificación de la información**

Para los estándares de todo el mundo, solo la información verificable es válida como prueba en un proceso de auditoría. En este sentido, se necesita registrar cada descubrimiento a modo de muestra y establecer que cumpla con los estándares para ser guardada como prueba. Ciertos de los procedimientos más clásicos son las entrevistas y la observación de las labores cotidianas, así como de la revisión de los documentos de administración interna.

1. **Generación de incumplimientos**

El siguiente paso es decidir qué proceso o archivo no cumple con las reglas, estándares o la legislación presente. Asimismo, además tienen la posibilidad de ser considerados procesos fuertes o positivos en este periodo, previa a la generación de las conclusiones.

1. **Conclusiones de la auditoría**

Nuevamente se debería formar una junta con los guías y observadores del proceso de auditoría para compartir las conclusiones de esta. Aquí, se presentan los hallazgos y la información importante a lo largo de la observación, revisión y verificación. Esto a fin de debatir y concertar las conclusiones en un archivo que va a ser transmitido a las piezas relacionadas o auditados que forma parte del proceso de preparación y repartición que sirve como la última fase.

**Aplicación de métodos de auditoría**

Para la realización de auditorías, se puede utilizar una variedad de métodos de auditoría. El método por utilizar dependerá del objetivo, alcance, criterios, duración, ubicación, entre otros factores. La norma ISO 19011 proporciona en la siguiente tabla 2, ejemplos de métodos de auditoría que se pueden usar, solos o en combinación, para alcanzar los objetivos:

**Tabla 2.** Ejemplos de métodos de auditoría

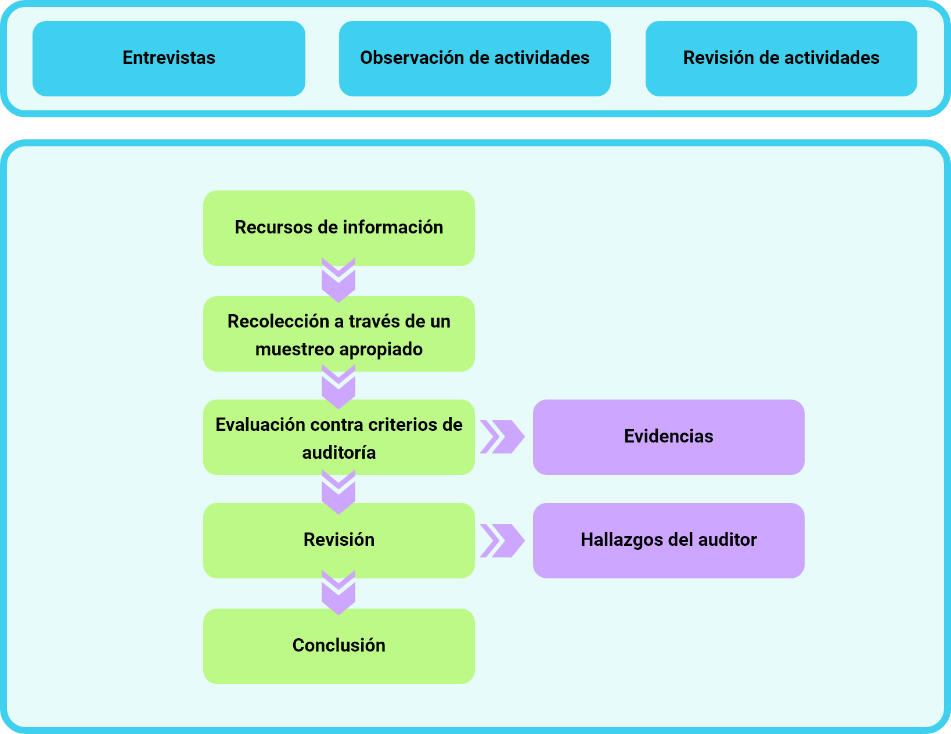
| **Alcance de la participación entre el auditor y el auditado** | **Ubicación del auditor** | |
| --- | --- | --- |
| **En el sitio** | **Remota** |
| **Interacción humana** | * Realización de entrevistas. * Completar listas de verificación y cuestionarios con participación del auditado. * Realización de una revisión de documentos con participación del auditado. * Muestreo. | **A través de comunicación interactiva significa:**   * Realización de entrevistas. * Observar el trabajo realizado con guía remota. * Completando lista de verificación y cuestionarios. * Realización de revisión de documentos con participación de los propietarios. |
| **Sin interacción humana** | * Realización de revisión de documentos (por ejemplo, registros, análisis de datos). * Observar el trabajo realizado y llevando a cabo una visita “in-situ”. Complementando listas de verificación. | * Realizar revisión de documentos (por ejemplo, registros, análisis de datos). * Observar el trabajo realizado a través de medios de vigilancia, teniendo en cuenta los requisitos sociales, estatutarios y normativos del análisis de datos. |

* Las actividades de auditoría en el sitio se realizan en la ubicación del auditado.
* Las actividades de auditoría remota se realizan en cualquier lugar que no sea la ubicación del auditado, independientemente de la distancia.
* Las actividades de auditoría interactiva implican la interacción entre el personal auditado y el equipo de auditoría.
* Las actividades de auditoría no interactivas no implican interacción humana con las personas que representan al auditado, pero sí implican la interacción con el equipo, las instalaciones y la documentación.

La información es el grupo de datos que configuran un mensaje que emite un emisor y que se pretende llegue al receptor para que pueda quedar reportado. Continuamente se realiza por medio de un canal que es el que uno de los dos interlocutores eligió.

Las técnicas de recolección de información son herramientas de la auditoría empresarial, en la que se usan procedimientos de recolección, para detectar de forma estricta y concreta las fallas en las zonas, en sistemas, sobre los cuales se practicarán las respectivas pruebas. A continuación, se presenta la recopilación de información en la auditoría.

**Figura 2.** Recopilación de información en una auditoría



Nota. SENA (2022).

**Entrevistas Observación de actividades Revisión de documentos**

Recursos de información

Recopilación a través de un muestreo apropiado

Evaluación contra criterios de auditoria Evidencia de auditoria

Revisión Hallazgos de auditor

Conclusión

Dentro de las auditorías, se pueden encontrar diversas técnicas de recolección de información, entre las cuales se incluyen:

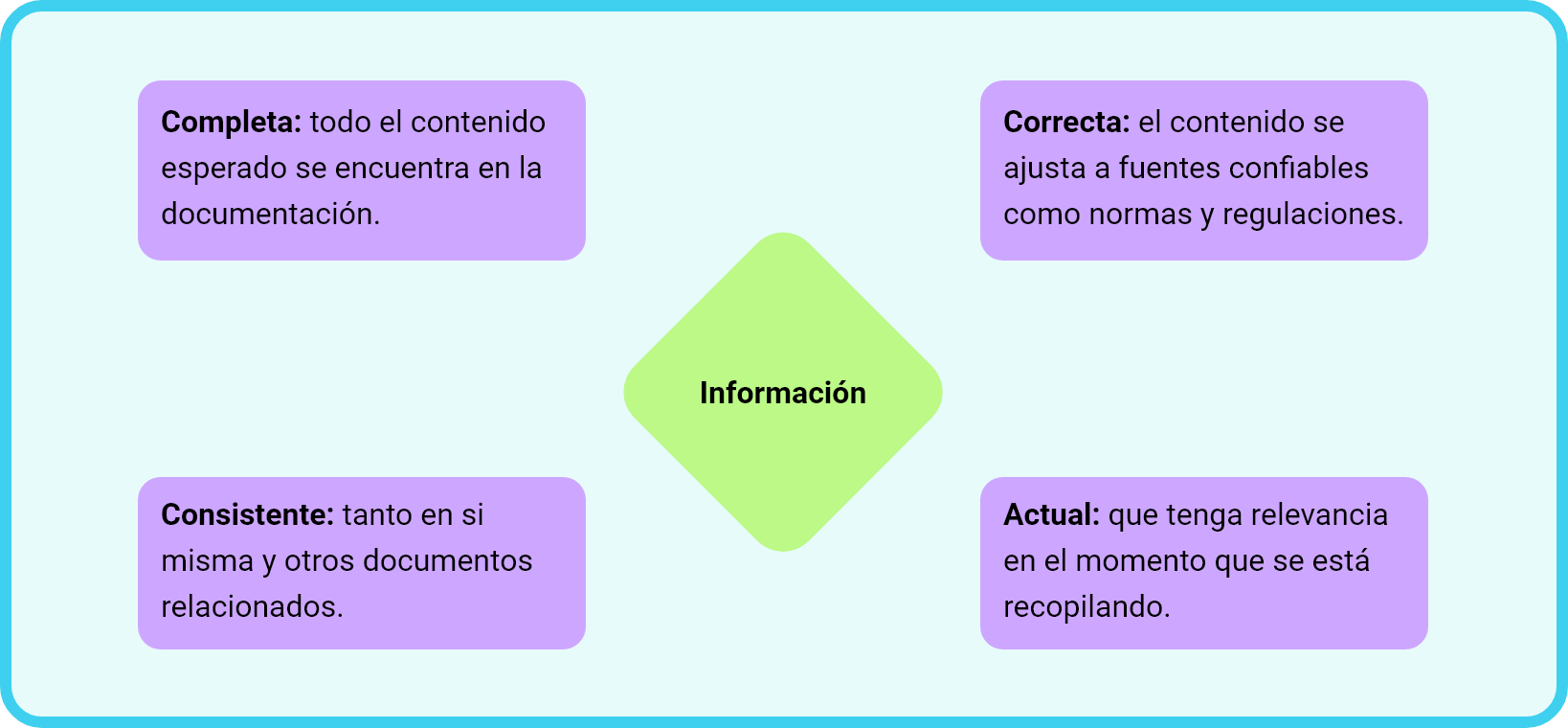
* **Técnicas de verificación ovular o visual:** estas técnicas involucran la observación directa, la comparación de documentos o la confrontación de información, así como la revisión selectiva.
* **Técnicas de verificación oral o verbal**: en esta categoría se incluyen la indagación a través de preguntas, encuestas y cuestionarios, así como las entrevistas con el personal relevante.
* **Técnicas de verificación documental**: esta técnica abarca la comprobación, la computación, el rastreo, la revisión analítica y el estudio general (exploración). Dentro de esta categoría se engloban las siguientes técnicas:
* **Técnicas de verificación física**: implican la revisión de documentos físicos, como facturas, recibos o registros en papel.
* **Técnicas de verificación escrita**: incluyen la revisión de documentos escritos, como contratos, acuerdos o políticas de la organización.

El tipo de información que se maneja en un proceso de auditoría, debe tener características especiales para garantizar un proceso satisfactorio. Es importante que la información sea:

* **Relevante:** la información debe ser pertinente para los objetivos de la auditoría y estar relacionada con los criterios establecidos.
* **Suficiente:** debe existir la cantidad adecuada de información para respaldar las conclusiones y hallazgos de la auditoría.
* **Confiable:** la información debe ser precisa y verificable, proveniente de fuentes fiables y procesos confiables.
* **Oportuna:** debe estar disponible cuando se necesita para la auditoría y no debe haber demoras significativas.
* **Clara y comprensible:** la información debe ser presentada de manera que sea fácilmente entendible por quienes la utilizan.
* **Sensible a los riesgos:** debe incluir información sobre los riesgos significativos relacionados con los objetivos de la auditoría.
* **Sensible a la importancia relativa:** debe priorizarse la información más relevante y significativa.
* **Completa:** debe abordar todos los aspectos relevantes de los objetivos de la auditoría.
* **No sesgada:** la información no debe estar influenciada por sesgos o intereses particulares.

Estos principios aseguran que la información utilizada en una auditoría sea sólida, confiable y útil para la toma de decisiones y la evaluación de procesos y sistemas. En resumen, se pueden definir los siguientes cuatro aspectos que se utilizan comúnmente y que abarcan lo que un auditor necesita para su proceso:

**Figura 3.** Características de la información



**Información**

* **Completa:** todo el contenido esperado se encuentra en la documentación.
* **Correcta:** el contenido se ajusta a fuentes confiables como normas y regulaciones.
* **Consistente:** tanto en sí misma y otros documentos relacionados.
* **Actual:** que tenga relevancia en el momento que se está recopilando.

## Verificación del sistema

Las listas de verificación son documentos que integran anotaciones claves para la ejecución de las ocupaciones de auditoría. Principalmente hechas como un formulario, cuestionario o planilla, estas listas son como una ayuda para que el auditor siga una sucesión estructurada de visualizaciones a lo largo de la ejecución de la auditoría. Si se emplean, dichas listas tienen que fundamentarse en un procedimiento conveniente de recolección de datos y el auditor tendrá que estar entrenado en su uso. Las listas de verificación tienen que contestar a la especificidad de cada auditoría. Éstas tienen que ser primordiales, objetivas y de simple uso, lectura y conocimiento, además de detectar datos y hechos.

La lista de verificación se ha diseñado para supervisar la ejecución de actividades repetitivas en las organizaciones, como revisar el cumplimiento de una lista de requisitos. Esto permite recopilar información y datos de manera organizada. Se utiliza para verificar actividades que están estandarizadas, como se presenta a continuación:

1. **¿Para qué sirven las listas de verificación?**

* Revisar que todas las actividades se realicen de forma organizada y en el orden establecido.
* Inspeccionar la propiedad.
* Verificar productos y/o procesos.
* Analizar los problemas identificados.
* Examinar las causas de los defectos.
* Verificar las operaciones en la organización.
* Recolectar datos para futuros análisis.

1. **¿Qué necesita para crear una lista de verificación?**

* Deben estar diseñadas de acuerdo con el tipo de auditoria implementado en la organización para verificar y recopilar la información o datos.
* Deben ser efectivas estableciendo cuáles son los criterios que se deben verificar, si es de cumplimiento o no conformidad y su frecuencia de seguimiento o verificación.
* Tener un mecanismo de observación que proporcione información adicional.
* Deben informar sobre el estado de las operaciones de la organización y evaluar los procesos sin necesidad de estadísticas o gráficos más complejos.
* Deben ser simples y fáciles de leer y comprender.

1. **¿Cuáles son los objetivos de las listas de verificación?**

* Promover en la organización la auditoría.
* Actuar como proyecto de muestreo y administrador del tiempo.
* Dar pruebas sobre las notas recopiladas para el proceso de auditoría de campo.
* Facilitar la continuación del proceso de auditoría.
* Proporcionar una base de información para planear futuras auditorías.

1. **¿Cuáles son los posibles aspectos a verificar?**

* Verificar si se han seguido los procedimientos.
* Revisar si los productos cumplen con las especificaciones.
* Determinar si las medidas dimensionales, como color, peso, rugosidad, etc., se encuentran dentro de las tolerancias.
* Comprobar si ha cumplido los ensayos de resistencia, impermeabilidad, etc.
* Examinar si se han llenado los registros.
* Chequear si ha existido alguna incidencia.
* Verificar si los equipos se encuentran en correcto estado de mantenimiento.

Después de comprender qué es una lista de verificación y su importancia en los procesos de auditoría, y tras revisar los objetivos y los posibles aspectos que deben verificarse, examinaremos un ejemplo de una lista de verificación diseñada para auditar la norma ISO 9001:2015:

**Tabla 3.** Ejemplo de lista de verificación

|  |  |  |
| --- | --- | --- |
| Lista de verificación para el proceso de auditoría | | |
| Criterios de auditoría | **Notas del auditor** | **Hallazgos**  **C: conformidad**  **NC: no conformidad**  **O: observación** |
| En este espacio se diligencian las políticas o procedimientos que se van a evaluar. | En este espacio se diligencian todas las cuestiones internas y externas, preguntas, muestras u otra información que le sirva al auditor como ayuda para la búsqueda de evidencias. | En este espacio se diligencian los diferentes hallazgos encontrados, especificando el numeral de la norma auditada y clasificándolos en conformidad, no conformidad y observaciones. |
| Fecha: | **Nombre del auditor:** | **Página:** |

# 

## Seguridad y confidencialidad de la información

La confidencialidad, una vez que se hace referencia a sistemas de información, posibilita a los usuarios autorizados entrar a datos confidenciales y salvaguardados. Hay mecanismos específicos que avalan la confidencialidad y protegen los datos de intrusos no deseados o que van a provocar mal. La confidencialidad pertenece a los pilares de estabilidad de la información, junto con la disponibilidad y totalidad. La información o los datos confidenciales tienen que divulgarse sólo a usuarios autorizados.

Una vez que se habla de un registro de auditoría además se habla de los tokens. Es fundamental rememorar que los tokens son los que por medio del uso de cookies permiten validar la identidad del cliente. Hay herramientas que permiten revisar cual es la fortaleza de los tokens provocados por una aplicación “web”.

Un registro de auditoría es una serie de tokens de auditoría. Cada “token” de auditoría tiene información del acontecimiento, como ID de cliente, hora y fecha. Un “token header” empieza un registro de auditoría, y un token opcional tráiler, lo concluye. Otros “tokens” de auditoría tienen dentro información importante para el acontecimiento de la evaluación.

La siguiente tabla muestra los nombres de “tokens” con una breve explicación de cada uno de ellos:

**Tabla 4.** Tipos de “token”

| Nombre de “token” | Descripción |
| --- | --- |
| “Acl” | Información de Entrada de Control de Acceso (ACE) y Lista de Control de Acceso (ACL). |
| “Arbitrary” | Datos con información de formato y de tipo. |
| “Argument” | Valor de argumento de llamada de sistema. |
| “Attribute” | Información de *v-“*node” de archivo. |
| “Cmd” | Argumentos de comandos y variables de entornos. |
| “exec\_args” | Argumentos de llamada de sistema *exec*. |
| “exec\_env” | Variables de entorno de llamada de sistema *exec*. |
| “Exit” | Información de salida de programa. |
| “File” | Información de archivo de auditoría. |
| “Fmri” | Indicador de recursos de gestión de estructura. |
| “Group” | Información de grupos de procesos. |
| “Header” | Indica el comienzo del registro de auditoría. |

El subsistema de auditoría se encarga de defender los datos, incrementando la garantía de que sean auditados y no se hayan cambiado ni modificado fuera del proceso. Esta alternativa además salvaguarda la confidencialidad de los datos mediante archivos cifrados y firmando los datos de registro, en muchas organizaciones tienen que ser guardados en sitios con alta seguridad para prevenir modificaciones y eliminaciones casuales o motivadas.

A continuación, se mostrará los procedimientos para seleccionar, analizar y gestionar los registros de auditoría:

**Tabla 5.** Procedimientos de selección, gestión y registros de auditoría

| Tarea | Descripción | Para obtener instrucciones |
| --- | --- | --- |
| Mostrar los formatos de los registros de auditoría. | Muestra el tipo de información que se recopila para un evento de auditoría y el orden en que se presenta la información. | Cómo visualizar formatos de registros de auditoría. |
| Fusionar registros de auditoría. | Combina los archivos de auditoría de varios equipos en una pista de auditoría. | Cómo fusionar archivos de auditoría de la pista de auditoría. |
| Seleccionar los registros para examinar. | Selecciona eventos determinados de estudio. | Cómo seleccionar eventos de auditoría de la pista de auditoría. |
| Mostrar registros de auditoría. | Habilita la visualización de registros de auditoría binarios. | Cómo visualizar el contenido de los archivos de auditoría binarios. |
| Depurar archivos de auditoría denominados incorrectamente. | Proporciona una indicación de hora final para auditar archivos de auditoría que quedaron abiertos inadvertidamente en el servicio de auditoría. | Cómo depurar un archivo de auditoría “not\_terminated”. |
| Evitar el desbordamiento de la pista de auditoría. | Impide que los sistemas de archivos de auditoría se llenen. | Cómo evitar el desbordamiento de la pista de auditoría. |

Nota. Tomada de gestión de registros de auditoría. Oracle (2011).

El mantenimiento del registro de auditoría incluye numerosas piezas de la funcionalidad que permiten automatizar el registro de auditoría en políticas concretas. El mantenimiento de registros y la presentación de informes resaltan el valor del desarrollo y mantenimiento de la memoria institucional por medio de informes bien diseñados y ocupaciones de mantenimiento de registros eficaces. Los registros disponibles facilitan el diseño y el reparto de informes que tienen la posibilidad de informar el personal, el liderazgo del programa y los aliados externos de la sociedad.

**Pilares de la seguridad de la información**

Las organizaciones se ven cada día más expuestas a un creciente número de ataques virtuales y delitos cibernéticos, lo que hace que la protección de los datos sea una prioridad. Para incrementar la seguridad de la información, es indispensable conocer los tres pilares fundamentales de la seguridad de la información, que se presentan a continuación:

* **Integridad:** hace referencia a la cualidad de la información para ser correcta y no haber sido modificada.
* **Confidencialidad:** la cualidad de la información para no ser divulgada a personas o sistemas no autorizados.
* **Disponibilidad:** entendemos aquella información a la que podemos acceder cuando la necesitamos a través de los canales correctos.

## ISO 27000

Es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. Permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

En la actualidad, se conoce que para defender la información en las organizaciones no basta con la construcción de procedimientos y controles de estabilidad sin una orientación o regla general establecida y testeada. Gracias a esto, la Organización Internacional de Estandarización (ISO), pone a disposición una pluralidad de estándares de reconocimiento y aplicación universal, agrupados en el núcleo familiar de ISO 27000, con el fin de desarrollar una óptima utilización de la estabilidad de la información.

La norma ISO 27000 proviene de la norma BS 7799 del Reino Unido, que fue publicada en 1995 con el objetivo de proporcionar a las organizaciones, una serie de buenas prácticas relacionadas con la gestión de la seguridad de la información.

Esta norma, o conjunto de normas, es aplicable a organizaciones de cualquier tamaño y actividad y tiene como objetivo el desarrollo de estándares para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). El SGSI garantiza la adecuada implementación de controles de seguridad para proteger la información de manera efectiva.

La implantación de un Sistema de Gestión de Seguridad de la Información (SGSI) conlleva varios beneficios para las organizaciones. El principal beneficio es la reducción de los riesgos relacionados con la seguridad de la información, lo que disminuye la probabilidad de sufrir incidentes que puedan afectarla. Además de esto, se pueden mencionar otros beneficios importantes, como:

* Proporciona una metodología sistemática para implementar un SGSI que puede adaptarse a las necesidades de cualquier organización o empresa.
* Facilita la integración coherente de los objetivos de seguridad de la información con los objetivos comerciales, los procesos, la gestión de la organización y la capacitación y sensibilización de los empleados.
* Permite la adopción de prácticas internacionalmente aceptadas en seguridad de la información y su adaptación a las necesidades específicas de cada organización.
* Establece un lenguaje común en el ámbito de la seguridad de la información, lo que facilita la certificación del SGSI por parte de entidades u organismos acreditados.

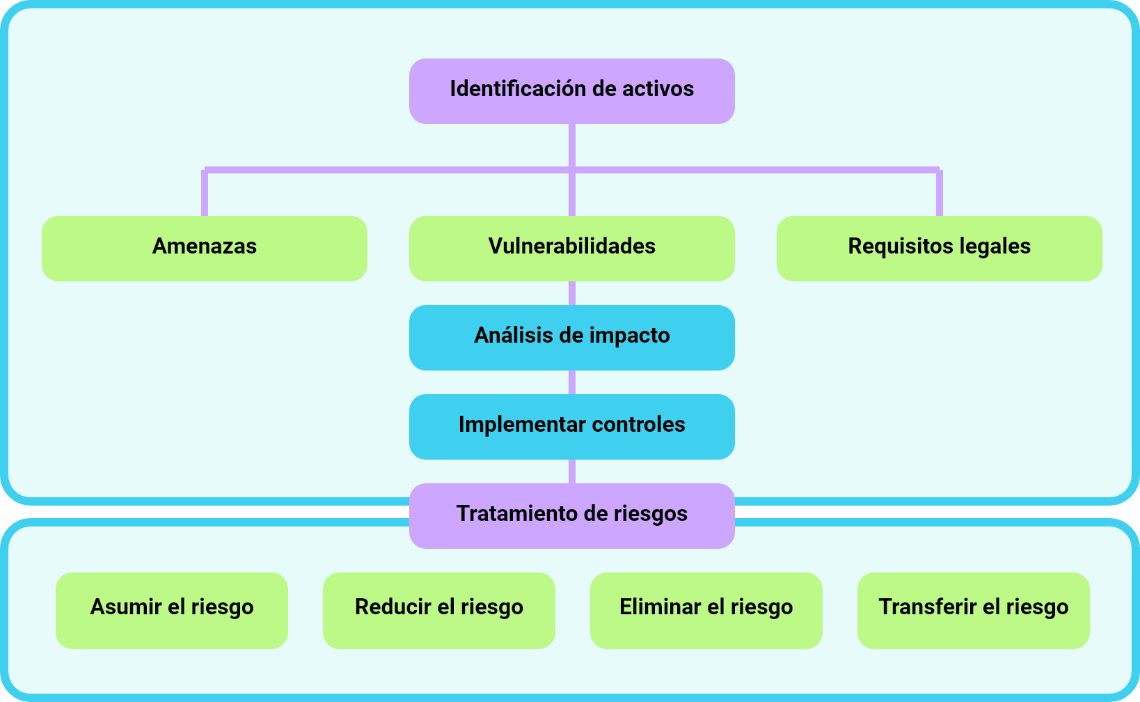
En resumen, la implementación de un SGSI contribuye a proteger la información de la organización y a alinear la seguridad de la información con los objetivos comerciales, lo que puede tener un impacto positivo en la competitividad y la confianza de los clientes.

**Implementando la Norma ISO 27001**

La norma ISO 27001 es una herramienta fundamental para establecer un Sistema de Gestión de Seguridad de la Información (SGSI) en una organización. Esta norma proporciona un marco de trabajo que ayuda a definir el alcance, las políticas, las medidas y las metodologías necesarias para garantizar la seguridad de la información.

Uno de los aspectos clave de la ISO 27001 es la evaluación de riesgos, que es el proceso central para identificar y gestionar las amenazas y vulnerabilidades que pueden afectar a la seguridad de la información de una organización. La norma sugiere una metodología para llevar a cabo esta evaluación de riesgos, que es fundamental para tomar decisiones informadas sobre las medidas de seguridad a implementar. A continuación, se revisará la metodología sugerida en la norma:

**Figura 4**. Método de evaluación y tratamiento del riesgo



**Identificación de activos**

1. **Amenazas**
2. **Vulnerabilidad**

* Análisis del impacto
* Implementar controles

1. **Requisitos legales**

**Tratamiento de riesgos**

1. **Asumir el riesgo**
2. **Reducir el riesgo**
3. **Eliminar el riesgo**
4. **Transferir el riesgo**

De acuerdo a la anterior figura se explicará cada uno de los aspectos o pasos que se deben definir y cuál es su función.

* **Identificar activos de información**

Son todos aquellos activos como infraestructura, equipos, así mismo intelectuales o informativos como ideas, proyectos. También la marca y la reputación de la organización.

* **Vulnerabilidades**

Identificar aquellas debilidades de los activos de la información que lo hacen susceptibles a sufrir ataques o daños.

* **Amenazas**

Son aquellos sucesos que pueden presentar vulnerabilidad y dañan la información, tales como desastres naturales, incendios o ataques de virus informáticos, espionaje, etc.

* **Requisitos legales**

Se deben identificar los requisitos legales y contractuales que están obligados a cumplir con sus clientes, proveedores y socios.

* **Identificar los riesgos**

Definir para cada activo las probabilidades de amenazas o vulnerabilidades que puedan causar un daño total o parcial comprometiendo su disponibilidad, confidencialidad e integridad.

* **Cálculo del riesgo**

Este se realiza a partir de la probabilidad de ocurrencia del riesgo y el impacto que este tiene sobre la organización.

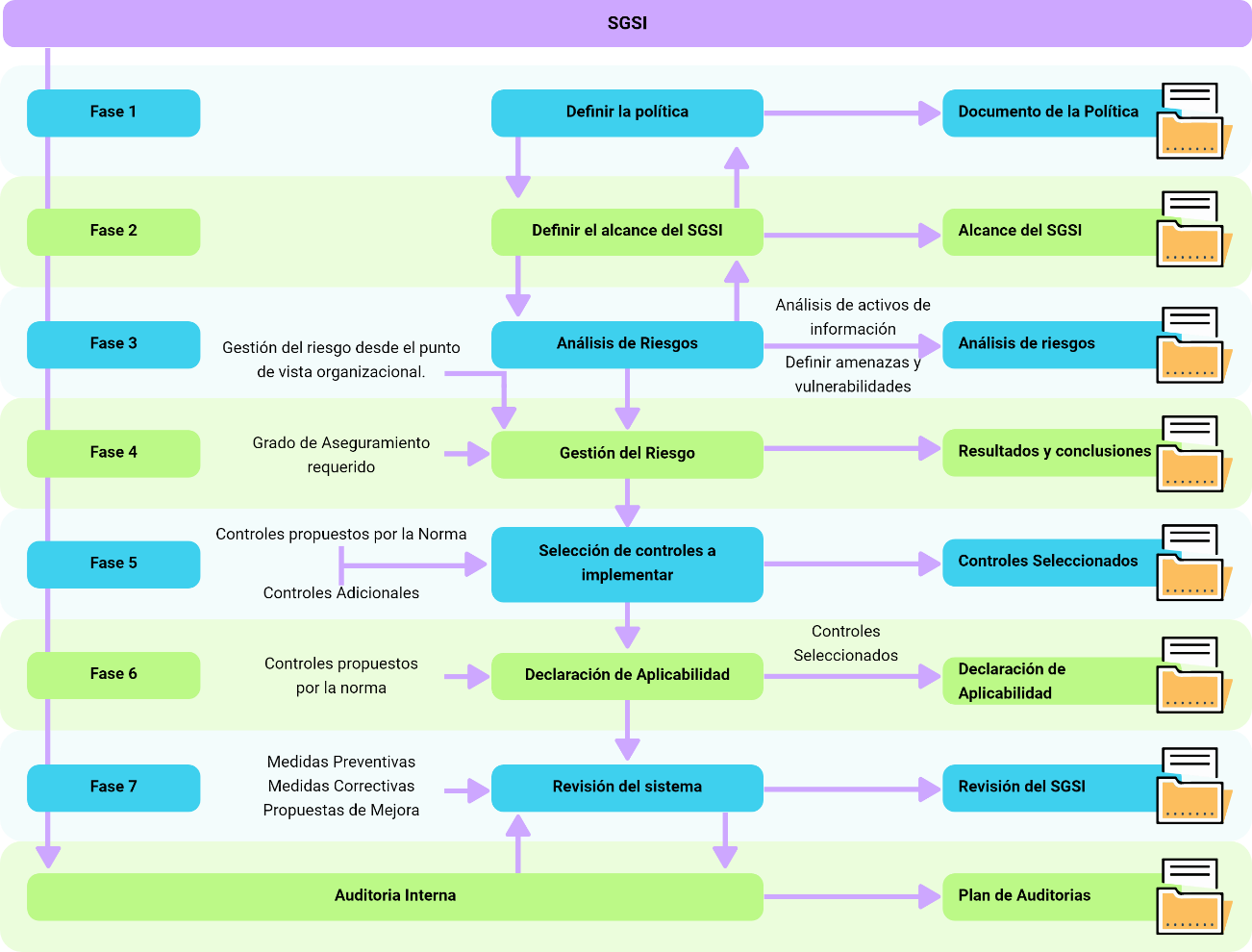
Teniendo en cuenta que el riesgo es el resultado de la multiplicación del impacto y la probabilidad de suceso.

* **Plan de tratamiento del riesgo**

En este punto se define la política de tratamiento de los riesgos en función de los puntos anteriores.

En la siguiente figura, se revisarán las fases para la implementación de un adecuado Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO 27001. A través de una elaboración y recopilación adecuadas, es posible garantizar la confidencialidad, integridad y disponibilidad de la información relacionada con este SGSI.

**Figura 5.** Fases para implementar un SGSI



## Requisitos aplicables según la norma

Un Sistema de Gestión de la Seguridad de la Información (SGSI), es un conjunto de políticas y procedimientos que sirven para estandarizar la gestión de la Seguridad de la Información. Esta estandarización contiene las definiciones y los términos que se utilizarán durante toda la serie 27000. Para aplicar cualquier normativa se necesita conocer un vocabulario perfectamente definido, por lo que así se evitará cualquier mala interpretación de conceptos técnicos y gestión.

A continuación, se dejará algunos detalles de cada uno de los estándares que están incluidos en la familia de ISO 27000.

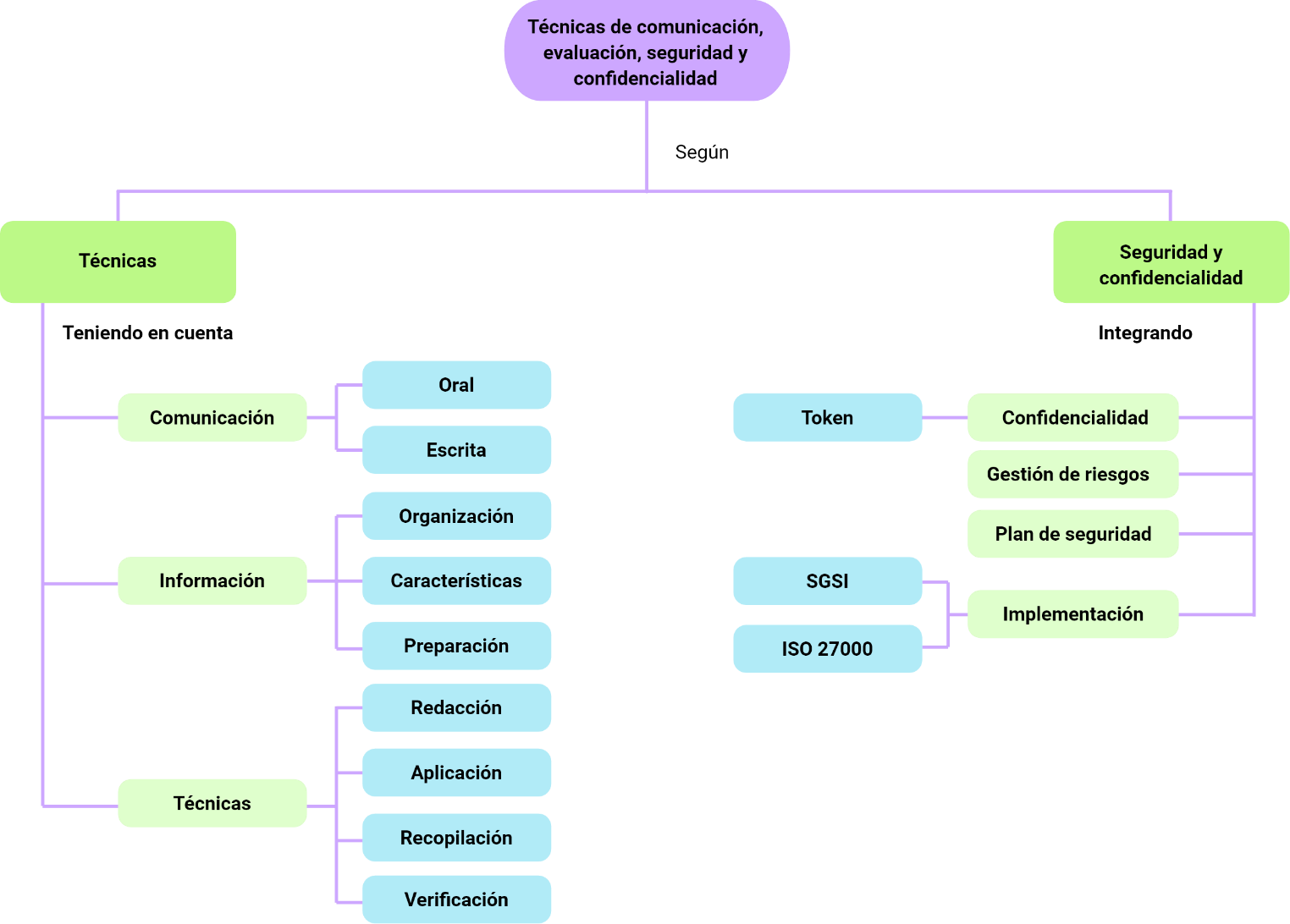
**Tabla 6.** Familia de las Normas ISO 27000

| Tipo | Norma | Descripción |
| --- | --- | --- |
| Vocabulario común. | ISO 27000. | Especifica los requerimientos y necesidades para implantar y gestionar un SGSI. Es una norma certificable. |
| Vocabulario común. | ISO 27006. | Establece los requisitos que deben cumplir aquellas organizaciones que quieran ser acreditadas para certificar a otras en el cumplimiento de la ISO 27001. |
| ISO 27009. | Complementa la norma 27001 para incluir requisitos y nuevos controles añadidos que son de aplicación en sectores específicos, con el objetivo de hacer más eficaz su implantación. |
| Guía de aprendizaje. | ISO 27002. | Define un conjunto de buenas prácticas para la implantación del SGSI, a través de 114 controles, estructurados en 14 dominios y 35 objetivos de controles. |
| ISO 27003. | Proporciona una guía para la implantación de forma correcta un SGSI, centrándose en los aspectos importantes para realizar con éxito dicho proceso. |
| ISO 27004. | Proporciona pauta orientadas a la correcta definición y establecimiento de métricas que permitan evaluar de forma correcta el rendimiento del SGSI. |
| ISO 27005. | Define cómo se debe realizar la gestión de riesgos vinculados a los sistemas de gestión de la información orientado en cómo establecer la metodología a emplear. |
| ISO 27007. | Es una guía que establece los procedimientos para realizar auditorías internas o externas con el objetivo de verificar y certificar. |
| ISO 27008. | Define cómo se deben evaluar los controles del SGSI con el fin de revisar la adecuación técnica de los mismos, de forma que sean eficaces para la mitigación de riesgos. |
| ISO 27013. | Establece una guía para la integración de las normas 27001 (SGSI) y 20000 Sistema de Gestión de Servicios (SGS) en aquellas organizaciones que implementan ambas. |
| ISO 27014. | Establece principios para el gobierno de la seguridad de la información, para que las organizaciones puedan evaluar, monitorizar y comunicar las actividades relacionadas con la seguridad de la información. |
| ISO 27015. | Facilita los principios de implantación de un SGSI en empresas que prestan servicios financieros, tales como servicios bancarios o banca electrónica. |
| ISO 27016. | Proporciona una guía para la toma de decisiones económicas vinculadas a la gestión de la seguridad de la información, como apoyo a la dirección de las organizaciones. |
| Requisitos específicos. | ISO 27010. | Indica cómo debe ser tratada la información cuando es compartida entre varias organizaciones, qué riesgos pueden aparecer y los controles que se deben emplear para mitigarlos, especialmente cuando están relacionados con la gestión de la seguridad en infraestructuras críticas. |
| ISO 27011. | Establece los principios para implantar, mantener y gestionar un SGSI en organizaciones de telecomunicaciones, indicando como implantar los controles de manera eficiente. |
| ISO 27017. | Proporciona una guía de 37 controles específicos para los servicios *cloud*, estos controles están basados en la norma 27002. |
| ISO 27018. | Complementa a las normas 27001 y 27002 en la implantación de procedimientos y controles para proteger datos personales en aquellas organizaciones que proporcionan servicios en *cloud* para terceros. |
| ISO 27019. | Facilita una guía basada en la norma 27002 para aplicar a las industrias vinculadas al sector de la energía, de forma que puedan implantar un SGSI. |

Nota. La familia de normas ISO 27000. ISOTools (2022).

# Síntesis

El componente formativo Técnicas de comunicación, evaluación, seguridad y confidencialidad, se centra en aspectos esenciales para garantizar una evaluación precisa en el ámbito de las auditorías. La comunicación efectiva con todas las partes involucradas permite comprender a fondo los procesos y desafíos de la organización. La evaluación, por su parte, implica analizar datos y pruebas de manera imparcial para identificar áreas de mejora de manera objetiva. La seguridad en el contexto de la auditoría se refiere a la protección de la integridad de la información y a la prevención de posibles filtraciones de datos sensibles. Finalmente, la confidencialidad juega un papel crucial al mantener la privacidad de la información empresarial y prevenir conflictos de interés. En conjunto, estas técnicas y principios aseguran la calidad y confiabilidad de las auditorías, promoviendo la transparencia y facilitando la mejora continua en las organizaciones.



# Material complementario

| **Tema** | **Referencia APA del Material** | **Tipo de material**  **(Video, capítulo de libro, artículo, otro)** | **Enlace del Recurso o**  **Archivo del documento o material** |
| --- | --- | --- | --- |
| 1.Técnicas de comunicación | Herrera, P. (2021). *Técnicas de comunicación Asertiva ¡Así logras llegar a un acuerdo!*[Video]. YouTube. | Video | <https://www.youtube.com/watch?v=wUVWHRYJkNo> |
| 1.1 Revisión de proceso a técnicas de aplicación | El administrador 3.0. (2021). *Técnicas de auditoria administrativa / aprender técnicas de auditoria administrativa 2021.*[Video]. YouTube. | Video | <https://www.youtube.com/watch?v=KQHFFKfqmAY> |
| 1.2 Verificación del sistema | Mesa, A. (2020). *Listas de Verificación en auditorías.*  [Video]. YouTube. | Video | <https://www.youtube.com/watch?v=G7o_yIC2dL4> |
| 2. Seguridad y confidencialidad de la información. | nqa.com. (2013*).*ISO 27001 Guía de implantación para la seguridad de la información**.** | Norma | <https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf> |
| 2.1 ISO 27000 | Procem Consultores. (2018). *ISO 27001- Seguridad de la Información.*  [Video]. YouTube. | Video | <https://www.youtube.com/watch?v=BNdPQU32p2Y> |

# 

# Glosario

**Amenazas:** son aquellas cosas que pueden suceder que dañan los activos de la información, tales como desastres naturales, incendios o ataques de virus, espionaje, etc.

**Confidencialidad:** la cualidad de la información para no ser divulgada a personas o sistemas no autorizados.

**Diálogo:** es la comunicación en la que ocurre un intercambio de información entre dos o más personas.

**Emisor:** la persona (o personas) que emite un mensaje.

**Receptor:** la persona (o personas) que recibe el mensaje.

**Redacción:** es el proceso por medio del cual se compone un discurso escrito siendo la redacción un arte, pero sin embargo además siendo una técnica.

**SGSI:** Sistema de Gestión de la Seguridad de la Información.

# Referencias bibliográficas

Arenas Ramírez, A. (2016). Información difusa. <https://www.gestiopolis.com/informacion-difusa/>

EALDE, (2020). Elaborar la lista de verificación en auditorías internas ISO 9001:2015. <https://www.ealde.es/lista-verificacion-auditoria-iso-9001/>

Coelho, F. (2017). Comunicación oral. <https://www.significados.com/comunicacion-oral/>

Firma-e (2014). Pilares de la Seguridad de la Información: confidencialidad, integridad y disponibilidad. <https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad/>

Fonseca, (2011). Existen varios tipos de ruido.

Huerta Zamora, A. (2016). El arte del manejo de la información y la información difusa. <https://www.gestiopolis.com/arte-del-manejo-la-informacion-la-informacion-difusa/>

Isotools, (s.f.). ISO 27000. Sistemas de Gestión la Seguridad de la Información. <https://www.isotools.us/normas/riesgos-y-seguridad/iso-27001/>

Intedya, (2015). ISO 27000 y el conjunto de estándares de Seguridad de la Información. <https://www.intedya.com/internacional/757/noticia-iso-27000-y-el-conjuntode-estandares-de-seguridad-de-la-informacion.html>

Morales, A. (2019). Qué es la comunicación. <https://www.todamateria.com/que-es-la-comunicacion/>

Normas ISO. (s.f). ISO 27001 Seguridad de la información. <https://www.normas-iso.com/iso-27001/>

Oracle. (2011). Gestión de registros de auditoría. <https://docs.oracle.com/cd/E24842_01/html/E23286/audittask-91.html>

Oracle. (s.f.). Guía de administración del sistema: servicios de seguridad. <https://docs.oracle.com/cd/E24842_01/html/E23286/auditref-20.html#:~:text=Un%20registro%20de%20auditor%C3%ADa%20es,token%20opcional%20trailer%2C%20lo%20concluye>.

Rosas, Sánchez, L. (2012). El uso de información difusa en la toma de decisiones empresariales. <https://www.gestiopolis.com/el-uso-de-informacion-difusa-en-la-toma-de-decisiones-empresariales/>

Vaca López, Andrea, (2017). Auditar la comunicación, un paso adelante en la evaluación de intangibles. <https://www.ugc.edu.co/sede/armenia/files/editorial/auditar_la_comunicacion_un_paso_adelante_en_la_evaluacion_de_intangibles.pdf>

# Créditos

|  |  |  |
| --- | --- | --- |
| Nombre | Cargo | Regional y Centro de Formación |
| Claudia Patricia Aristizábal | Responsable del equipo | Dirección General |
| Norma Constanza Morales Cruz | Responsable de línea de producción | Regional Tolima - Centro de Comercio y Servicios |
| May Stefanny González | Experta temática | Regional Norte de Santander - Centro de Industria empresa y servicios regionales |
| Gloria Lida Álzate Suarez | Diseñadora Instruccional | Regional Distrito Capital - Centro de Gestión Industrial |
| Andrés Felipe Velandia Espitia | Asesor Metodológico | Regional Distrito Capital - Centro de Diseño y Metrología |
| Rafael Neftalí Lizcano Reyes | Responsable Equipo Desarrollo Curricular | Regional Santander - Centro Industrial de Diseño y la Manufactura |
| Jhon Jairo Rodríguez Pérez | Corrector de Estilo | Regional Distrito Capital - Centro de Diseño y Metrología |
| Sergio Augusto Ardila Ortiz | Diseñador Instruccional | Regional Tolima - Centro de Comercio y Servicios |
| Viviana Esperanza Herrera Quiñonez | Asesora Metodológica | Regional Tolima - Centro de Comercio y Servicios |
| Aruzidna Sánchez Alonso | Diseñadora web | Regional Tolima - Centro de Comercio y Servicios |
| Oscar Daniel Espitia Marín | Desarrollador Fullstack | Regional Tolima - Centro de Comercio y Servicios |
| Gilberto Junior Rodríguez Rodríguez | Storyboarde Ilustración | Regional Tolima - Centro de Comercio y Servicios |
| Nelson Iván Vera Briceño | Producción audiovisual | Regional Tolima - Centro de Comercio y Servicios |
| Oleg Litvin | Animador | Regional Tolima - Centro de Comercio y Servicios |
| Oscar Daniel Espitia Marín | Actividad Didáctica | Regional Tolima - Centro de Comercio y Servicios |
| Jorge Bustos Gómez | Validación y vinculación en plataforma LMS | Regional Tolima - Centro de Comercio y Servicios |
| Gilberto Naranjo Farfán | Validación de contenidos accesibles | Regional Tolima - Centro de Comercio y Servicios |