

Proyecto de énfasis

María Paula Farias Rodríguez

Daniel Felipe Moreno González

Rodrigo Gutiérrez Cabrera

Asesor de proyecto

Escuela Colombiana de Ingeniería Julio Garavito

Énfasis sistemas de gestión.

Bogotá D.C

2022-1

Tabla de contenido.

Palabras claves	3
Introducción	5
Las 10 cláusulas de la ISO 27001:2015	6
Cuadro resumen/comparativo	10

Palabras claves.

1. Palabras claves:

- 1.1. Procesos:** Conjunto de operaciones a que se somete una cosa para elaborarla o transformarla. Según la definición aportada por la ISO9001:2015 un proceso es definido como un conjunto de actividades interrelacionadas que, partiendo de uno o más elementos de entradas se transforman, generando un resultado o una salida. En adición a esto, la UNE661777:2015 define a un proceso como un conjunto de actividades interrelacionadas que, partiendo, de uno o más elementos se transforma y genera salidas de tipo ambiental, seguridad y salud en el trabajo, de calidad, de seguridad de la información, entre otras.
- 1.2. Mapa de procesos:** Permite identificar los procesos de una empresa y relacionarlos entre sí según su orden de ejecución. Adicionalmente, la definición de la ISO 9000 Es la representación gráfica de los procesos que componen una organización ordenados desde un punto de vista del ciclo productivo de la empresa para mostrar la relación que nace desde las necesidades del cliente y terminando en el ciclo con la entrega del producto/servicio al propio cliente; cabe mencionar que según la UNE661777:2015 afirma que un mapa de procesos es una representación gráfica de la secuencia e interacción de los diferentes procesos que tienen lugar en una organización.
- 1.3. Ficha técnica de indicadores:** Es un instrumento de transparencia al hacer pública la forma en que se calculan los valores del indicador y comunicar los detalles técnicos que facilitan su comprensión.
- 1.4. Sistema de gestión de calidad:** Es la gestión de servicios que se ofrecen, y que incluye planear, controlar, y mejorar, aquellos elementos de una organización, que de alguna manera afectan o influyen en la satisfacción del cliente y en el logro de los resultados deseados por la organización. Según la ISO 9000 es un conjunto de normas sobre calidad y gestión de calidad, establecidas por la Organización Internacional de Normalización (ISO). Se pueden aplicar en cualquier tipo de organización o actividad orientada a la producción de bienes o servicios
- 1.5. Sistema de gestión ambiental:** Es un marco formal para mejorar el desempeño ambiental y desarrollar su trabajo de forma más eficiente en líneas generales. Por otro lado, un Sistema de Gestión Ambiental basado en la norma ISO 14001, facilita que una organización controle todas sus actividades, servicios y productos que pueden causar algún impacto sobre el medio ambiente, además ayuda a minimizar todos los impactos ambientales que generan su operación
- 1.6. Sistema integrado de gestión:** Es una herramienta en la que se plasma el protocolo y requisitos a seguir a diario en aspectos tales como la salud, la seguridad, el ambiente y la calidad, con el fin de lograr una estructura integral, eficiente y óptima de todos los procesos de la organización en general. Por su parte, la UNE661777:2015 enuncia que un SIG (sistema integrado de gestión) es un conjunto formado por la estructura

organizacional, las responsabilidades, los procedimientos, los procesos y los recursos que se establecen para llevar a cabo la gestión integrada de los sistemas.

- 1.7. Estadística:** Es la rama de la matemática que estudia la variabilidad, colección, organización, análisis, interpretación, y presentación de los datos, así como el proceso aleatorio que los genera siguiendo las leyes de la probabilidad.
- 1.8. Indicador:** Instrumento que provee información relevante para evaluar el desempeño o progreso de un proceso, actividad o situación.
- 1.9. ISO 9001:2015:** Norma y guía internacional la cual ayuda a comprender porque ISO9001 genera beneficios para la organización en el ámbito de la calidad. Además de esto, le permite a la empresa visualizar los requisitos y pasos a seguir para lograr poder obtener tanto dichos beneficios como su respectiva certificación.
- 1.10. ISO 14001:2015:** Es la norma que tiene como objetivo implementar un sistema de gestión ambiental cumpliendo con los requisitos necesarios para que la organización sea responsable y comprometida con la protección medioambiental.
- 1.11. Mercado objetivo o target:** Grupo de destinatarios a los que va dirigido un producto o servicio. Cabe mencionar que este grupo de destinatarios previamente se le realizó un proceso de segmentación y selección dependiendo las características, propiedades del producto/servicio y de las necesidades de las partes involucradas.
- 1.12. Productos o servicios conformes:** Son todos aquellos productos o servicios que cumplen con todos los requisitos tanto organizacionales como de los clientes y proveedores.
- 1.13. Ficha técnica de proceso:** Documento donde se recogen las características más relevantes para el control de las actividades teniendo en cuenta sus características, entradas, salidas, personas involucradas, capacidad, normativa, objetivos, recomendaciones e indicadores de desempeño.
- 1.14. Estrategia:** Es una metodología que busca alcanzar un objetivo por medio de un plan de acción que se descompone en objetivos estratégicos para cada área funcional de la organización.
- 1.15. Alineación estratégica:** Grado de consistencia y coherencia que existe entre el plan estratégico, la cultura organizacional, así como todas las actividades y tareas que se realizan en el proceso de ejecución de la estrategia.
- 1.16. Cliente:** Parte interesada que recibe el producto o servicio de una organización. Define a una persona o entidad que adquiere un producto o servicio de otra. También puede hacer referencia a ciudadanos, usuarios, pacientes o cualquiera que sea receptor de una organización.
- 1.17. Auditoria:** Proceso por el que se obtienen evidencias y se evalúan objetivamente, por un tercero, para indicar el grado en el que se están cumpliendo los criterios de auditoría; se puede considerar como un examen orientado a comprobar si las acciones llevadas a cabo para la calidad y sus resultados son acordes a lo esperado o planteado inicialmente.
- 1.18. Riesgo:** Según la definición aportada por la norma UNE66177:2005 un riesgo es la combinación de la probabilidad y las consecuencias que se derivan de la materialización de un suceso peligrosos especificado.

Introducción.

Actualmente en un mundo en el que la globalización y la evolución de la tecnología son pilares fundamentales para la sociedad, tanto las personas como las organizaciones deben tener acceso y control de la información sensible ya sea de carácter externo e interno a estos. Además de esto, las organizaciones deben estar en la capacidad de proteger de manera adecuada la información ya que de no hacerlo podrían incurrir en consecuencias tanto operativas, financieras y legales potencialmente negativas a tal punto de poder llevar una organización a la “quiebra” o al “fracaso”.

Por lo tanto, teniendo en cuenta lo previamente mencionado la ISO (Organización internacional para la estandarización) en el 2009 publica una norma la cual contempla los requisitos y aspectos a abarcar por parte de la empresa para lograr implementar un sistema de gestión de la seguridad de la información (SGSI) de alto nivel. La norma a la que se hace referencia se denomina ISO27001 y tiene como función principal proporcionar un marco teórico robusto para proteger la información interna y externa sin distinción de tamaño, sector económico o tipo de organización.

Las 10 cláusulas de la ISO 27001:2015.

1. El alcance la ISO 27001 define el propósito de la norma, los tipos de organizaciones para las que se ha diseñado esta y los requisitos que debe cumplir la organización para que sea considerada como conforme.
2. En la ISO 27001 solo se referencia la ISO 27000, que es útil para la comprensión de los requisitos y su cumplimiento
3. Los términos y definiciones utilizados en la ISO 27001 son:
 - **Control de accesos:** El cual es un proceso que garantiza que solo las personas que tengan accesos a los activos son las que necesitan de estos.
 - **Efectividad:** Es la medida donde las actividades planeadas por la organización se ejecutan de la manera adecuada consiguiendo los resultados esperados
 - **Evaluación de riesgos:** Proceso en el cual se identifican riesgos por medio del análisis del nivel de riesgo de cada riesgo particular y evaluado, así reduciendo los riesgos a niveles aceptables.
 - **Tratamiento de riesgos:** Proceso o acción el cual reduce los riesgos identificados
 - **Gerencia:** Grupo de personas los cuales toman decisiones dentro de la organización, establecen la dirección estratégica, determinar y conseguir los objetivos de los accionistas
4. Para escoger la prioridad para proteger los activos de información de la organización depende del contexto en el que se opere, pero para esto existen dos niveles
 - **Contexto interno:** Las áreas que puede influir al momento de evaluar los problemas internos son: la madurez, cultura organizativa, la gestión, los recursos, la madurez de los recursos, el formato de los activos de información. La sensibilidad/valor de los activos de información, la consistencia, el sistema, la complejidad del sistema y el espacio físico
 - **Contexto externo:** Las áreas que puede influir al momento de evaluar los problemas externos son: La competencia, el dueño, los organismos reguladores, la economía y lo político, las consideraciones ambientales, la frecuencia de ataques a la información y los accionistas
5. La norma ISO 27001 le da gran importancia al liderazgo por de la siguiente manera:
 - **Política de seguridad:** La responsabilidad de un gran liderazgo es establecer una política de seguridad de la información que este alineada con los objetivos que tiene planteada la organización. Así mismo debe incluir un compromiso para cumplir los requisitos aplicables para el mejoramiento de la seguridad de la información (Requisitos legales, expectativas del cliente y compromisos contractuales) y también deberá incluir la mejora continua.

- **Roles y responsabilidades:** Debe existir una buena comunicación entre los involucrados, para esto es necesario designar a un líder del equipo de seguridad de la información que haga parte de la gerencia y que tenga un conocimiento en la gestión de seguridad de la información, el cual estará encargado de la capacitación, el control de los controles y la presentación de informes.
6. La ISO 27001 ayuda a la identificación de los riesgos que se puedan presentar de la seguridad de la información. Para esto es importante tener en cuenta los siguientes conceptos:
- **Evaluación de riesgos:** Es importante para aumentar la posibilidad de identificar los riesgos potenciales por medio de la utilización de las técnicas de evaluación sistemática, para la asignación de recursos a abordar en las áreas que tengan mayor prioridad y para tomar decisiones estratégicas respecto a la gestión de riesgos de seguridad de la información y poder lograr los objetivos propuestos.
 - **Tratamiento de riesgos:** Para cada riesgo identificado se puede aceptar el riesgo o tratarlo, para el tratamiento de riesgos existen las siguientes opciones:
 - ✓ La evasión del riesgo, que consiste en dejar de realizar la actividad o procesar la información que está expuesta al riesgo.
 - ✓ La eliminación del riesgo, que consiste en eliminar la fuente del riesgo.
 - ✓ El cambio de probabilidad, que consiste en poner en funcionamiento un control el cual disminuya los posibles incidentes de seguridad de la información.
 - ✓ El cambio en las consecuencias, el cual consiste en poner en funcionamiento un control el cual disminuya el impacto por la ocurrencia de un incidente.
 - ✓ Transferencia del riesgo, El cual redirecciona la actividad a un tercero el cual tenga mayor capacidad para tratar el riesgo.
 - ✓ Aceptar el riesgo, Es cuando se considera que el costo del tratamiento del riesgo es mayor que el costo del impacto que puede causar aceptar el riesgo.
7. En la cláusula 7 se abarca todo lo relacionado con los recursos entre los que se pueden encontrar a las personas, infraestructura, medioambiente, recursos físicos, materiales, herramientas, el conocimiento y la experiencia del talento humano y por tanto de la organización. Es importante recalcar que cuando se realice la planificación de los objetivos de calidad se debe tener en cuenta la capacidad actual (incluyendo recursos propios y externos proporcionados por proveedores o socios).

Por otro lado, para implementar y mantener un SGSI efectivo, se requiere contar con los recursos de apoyo necesarios los cuales a su vez deben ser capaces y competentes.

- **Competencia:** La implementación de controles efectivos de seguridad de la información depende del conocimiento y las habilidades de sus empleados, proveedores y contratistas. Es decir, para asegurar una base adecuada de conocimientos y habilidades la organización debe: definir que conocimientos y habilidades requieren, determinar quién necesita del conocimiento y habilidades y establecer como evaluar que el personal tenga los conocimientos y habilidades adecuadas. Cabe mencionar que se debe tener información documentada al respecto y ende aquellas organizaciones que poseen matrices de capacitación/habilidades pueden satisfacer este requisito de registro.
 - **Concienciación:** La organización además de garantizar la competencia del personal en relación con la seguridad de la información, debe informar que cada uno de los trabajadores, proveedores y contratistas identifiquen y comprendan los elementos del SGSI. Asimismo, los stakeholders previamente mencionados
 - **Comunicación:** Al igual que todos los procesos en una organización para que funcione el SGSI de manera efectiva debe existir una buena comunicación ya que es pilar fundamental para el éxito corporativo. Es por tal motivo que en la ISO27001 se detalla de manera concisa lo que necesita, cuando se necesita y a quien se necesita ser comunicado, además de quien es el responsable de la comunicación y cuáles son los procesos de comunicación.
8. El objetivo de implementar la ISO 27001 es tener un control adecuado de la creación y entrega del producto o servicio.
- **Evaluación de riesgos de la seguridad de la información:** La evaluación de los riesgos se debe realizar una vez al año o con una mayor frecuencia si se evidencia uno o más riesgos significativos.
O también se deben revisar si hay cambios en los activos, la información o los procesos de la organización, cuando se identifiquen nuevos riesgos o cuando los datos muestren que la probabilidad y consecuencia de cualquier riesgo identificado hayan tenido un cambio.
 - **Tratamiento de riesgos de seguridad de la información:** Se deben realizar cambios cada que son necesarios y se deber autorizar de nuevo. También se debe evaluar el impacto del plan y tener registro de los resultados de la evaluación.
9. Existen 3 maneras para hacer la evaluación de desempeño que son: El seguimiento de la efectividad de los controles, auditorías internas y revisión por la dirección.
- **Seguimiento, medición, análisis y evaluación:** Debido al montón de datos que se manejan se debe tomar una decisión de que es lo que se va a monitorear. Se deberá tener un registro de lo que se está monitoreando, analizando y revisando
 - **Auditorías internas:** El propósito de las auditorías internas es evaluar los procesos del SGSI e identificar oportunidades de mejora. Por ende, también le proporcionan a la gerencia la verificación y desempeño de todo el sistema (otro de sus grandes ventajas es que pueden llegar a evitar resultados no provistos en resultados de auditorías externas que pueden afectar a la organización). Dichas auditorías internas deben comprobar: el éxito de los procesos, procedimientos y controles

para conseguir resultados esperados, la consistencia del seguimiento de los procesos y controles y si su SGSI cumple a cabalidad con todo lo expresado y requerido por la ISO27001.

En continuación a lo anterior, para asegurar que las auditorias se llevan a cabo a un alto nivel y que por lo tanto aportan a la compañía deben ser realizadas por personas competentes, certificadas, que comprendan y apliquen de manera idónea la norma, respetadas y que tengan experiencia al respecto.

Adicionalmente, a las auditorias se les debe dar el tiempo suficiente para realizarse y se deben realizar de manera periódica (manteniendo de esta forma un plan de auditorías); la organización debe recordar que el auditor externo verificara el plan de auditorías interno para garantizar que todos los procesos del SGSI incluyan evidencias de bajo rendimiento y la gestión de riesgos de seguridad de la información durante un ciclo de tres años.

10. El objetivo de la implementación del SGSI, así como de la cláusula 10 o mejora es reducir la probabilidad de que ocurran eventos de seguridad de la información, así como reducir su impacto. Es importante tener en cuenta que ningún SGSI es perfecto por lo que se debe día a día buscar su mejora continua.

- **No conformidad y acción correctiva:** La mejora se consigue aprendiendo de los incidentes y problemas de seguridad identificados por las auditorias o por los stakeholders (por ejemplo: problemas de rendimiento, las quejas y reclamos)

La organización debe para cada oportunidad identificada mantener registro de: Lo que ocurrió, si el evento tuvo consecuencias indeseables, las acciones que se tomaron al respecto, la causa raíz del evento (en caso de si efectivamente se determinó), las acciones tomadas para eliminar la causa raíz y la evaluación de la efectividad de cualquier acción tomada.

- **Análisis de causa-raíz:** Para identificar acciones correctivas efectivas y adecuadas es recomendable complementar un análisis de causa raíz del problema. Unas de las mejores herramientas para dicho análisis es el “5 porqués” y los diagramas de Pareto. Para la aplicación de la primera de las herramientas mencionadas se debe evitar que todo problema llegue a la causa superficial “porque no hay dinero” sino que se tiene que profundizar más al respecto porque este no siempre termina siendo la causa principal.

Cuadro resumen/comparativo.

CAPITULO	NOMBRE	ISO9001 (CALIDAD)	ISO14001 (AMBIENTAL)	ISO 27001 (CIBERSEGURIDAD)
2	Objeto y campo de aplicación.	En esta norma se encuentran los requisitos para un sistema de gestión de la calidad cuando una organización necesita demostrar su capacidad de suministrar productos y servicios que cumplen a cabalidad con los requisitos y/o necesidades del cliente. En adición a esto, cuando las organizaciones aspiran aumentar la satisfacción del cliente a través de la aplicación eficaz del sistema de gestión.	Esta norma plasma los requisitos de un sistema de gestión ambiental para organizaciones que busquen administrar sus responsabilidades de tal forma que aporten y aporten a la sostenibilidad ambiental. Es decir, dicho sistema en coherencia con la política ambiental de la empresa, buscaran la mejora del desempeño ambiental, el cumplimiento de los requisitos legales y otros requisitos y el logro de todos los objetivos ambientales.	Esta norma muestra los requisitos de un sistema de gestión de la seguridad de la información dentro del contexto de la organización. Esta norma incluye también los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información dependiendo de las necesidades que tenga la organización.
3	Términos y definiciones.	<p>Relativos al sistema:</p> <ol style="list-style-type: none"> 1. Sistema de gestión: Conjunto de elementos de una organización interrelacionados que interactúan para establecer políticas, objetivos y procesos para el logro de estos objetivos. 2. Sistema de gestión de la calidad: Parte de un sistema de gestión relacionada con la calidad. 	<p>Relacionados con la organización y liderazgo:</p> <ol style="list-style-type: none"> 1. Sistema de gestión: Conjunto de elementos de una organización interrelacionados que interactúan para establecer políticas, objetivos y procesos para el logro de estos objetivos. 2. Sistema de gestión ambiental: Parte del sistema de gestión usado para gestionar aspectos ambientales, cumplir con las obligaciones 	

		<p>3. Política: Intención y dirección de una organización como las expresa formalmente su alta dirección.</p> <p>4. Política de la calidad: Política relativa a la calidad.</p> <p>5. Visión. Aspiración de aquello que una organización querría llegar a ser, tal como lo expresa la alta dirección.</p> <p>6. Misión: Propósito de la existencia de la organización, tal como lo expresa la alta dirección.</p> <p>7. Estrategia: Plan para lograr un objetivo a largo plazo o global.</p> <p>Relacionados a la persona(s):</p> <p>1. Alta dirección: Persona o grupo de personas que dirige y controla una organización al más alto nivel.</p> <p>2. Consultor del sistema de gestión de la calidad: Persona que ayuda a la organización en la realización de un sistema de gestión de la calidad, dando</p>	<p>legales y los requisitos voluntarios, y tener en cuenta el riesgo asociado con las amenazas y oportunidades.</p> <p>3. Política ambiental: Intenciones y dirección de una organización, como las expresa formalmente su alta dirección, relacionadas con el desempeño ambiental.</p> <p>4. Organización: Persona o grupo de personas que tienen sus propias funciones y responsabilidades, autoridades y relaciones para el logro de sus objetivos.</p> <p>5. Alta dirección: Persona o grupo de personas que dirige y controlan una organización al más alto nivel.</p> <p>6. Parte interesada: Persona u organización que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad.</p> <p>Relacionados con la planificación:</p> <p>1. Medio ambiente: Entorno en el cual</p>	
--	--	--	--	--

		<p>asesoramiento o información.</p> <p>3. Participación: Tomar parte en una actividad, evento o situación.</p> <p>4. Compromiso: Participación en, y en contribución a, las actividades para lograr objetivos compartidos.</p> <p>Relacionados a la organización:</p> <p>1. Organización: Persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para lograr sus objetivos.</p> <p>2. Parte interesada: Persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad.</p> <p>3. Cliente: Persona u organización que podría recibir o que recibe un producto o un servicio desinado a esa persona u organización o requerido por ella.</p>	<p>una organización opera, incluidos el aire, agua, la tierra, los recursos naturales, la flora, la fauna, los seres humanos y sus interrelaciones.</p> <p>2. Aspecto ambiental: Elemento de las actividades, productos o servicios de una organización que interactúa o puede interactuar con el medio ambiente.</p> <p>3. Condición ambiental: Estado o característica del medio ambiente, determinado en un punto específico en el tiempo.</p> <p>4. Impacto ambiental: Cambio en el medio ambiente, ya sea adverso o beneficioso, como resultado total o parcial de los aspectos ambientales de una organización.</p> <p>5. Objetivo: Resultado a lograr.</p> <p>6. Objetivo ambiental: Objetivo establecido por la organización, coherente con la política ambiental.</p> <p>7. Requisito: Necesidad o expectativa que está establecida, generalmente</p>	
--	--	---	--	--

		<p>4. Proveedor: Organización que proporciona un producto o un servicio.</p> <p>5. Proveedor externo: Proveedor que no es parte de la organización.</p> <p>Relacionados a la actividad:</p> <p>1. Mejora: Actividad para mejorar el desempeño.</p> <p>2. Mejora continua: Actividad recurrente para mejorar el desempeño.</p> <p>3. Gestión: Actividades coordinadas para dirigir y controlar una organización.</p> <p>4. Gestión de la calidad: Gestión con respecto a la calidad.</p> <p>5. Planificación de la calidad: Parte de la gestión de la calidad orientada a establecer los objetivos de la calidad y a la especificación de los procesos operativos necesarios y de los recursos relacionados para lograr los objetivos de la calidad.</p>	<p>implícita u obligatoria.</p> <p>8. Requisitos legales y otros requisitos: Requisitos legales que una organización que debe cumplir y otros requisitos que decide cumplir.</p> <p>9. Riesgo: Efecto de la incertidumbre sobre los objetivos.</p> <p>10. Riesgos y oportunidades: Efectos potenciales adversos (amenazas) y efectos potenciales beneficiosos (oportunidades)</p> <p>Relacionados con soporte y operación.</p> <p>1. Competencia: Capacidad para aplicar conocimientos y habilidades con el fin de lograr los resultados previstos</p> <p>2. Información documentada: Información que una organización tiene que controlar y mantener, y el medio en el que está contenida.</p> <p>3. Ciclo de vida: Etapas consecutivas e interrelacionadas de un sistema de producto o servicio, desde la</p>	
--	--	--	--	--

		<p>6. Control de la calidad: Parte de la gestión de la calidad orientada a proporcionar confianza en que se cumplirán los requisitos de la calidad.</p> <p>7. Control de la calidad: Parte de la gestión de la calidad orientada al cumplimiento de los requisitos de la calidad.</p> <p>8. Mejora de la calidad: Parte de la gestión de la calidad orientada a aumentar la capacidad de cumplir con los requisitos de la calidad.</p> <p>9. Actividad: El menor objeto de trabajo identificado en un proyecto.</p> <p>10. Gestión de proyectos: Planificación, organización, seguimiento, control e informe de todos los aspectos de un proyecto y la motivación de todos aquellos que están involucrados en el para alcanzar los objetivos del proyecto.</p> <p>11. Objeto de la configuración:</p>	<p>adquisición de materia prima o su generación a partir de recursos naturales hasta el tratamiento al finalizar su vida</p> <p>4. Contratar externamente: Establecer un acuerdo mediante el cual una organización externa realiza parte de una función o proceso de una organización.</p> <p>5. Proceso: Conjunto de actividades interrelacionadas o que interactúan, que transforman elementos de entrada en elementos de salida.</p> <p>Relacionados con la evaluación de desempeño y con la mejora:</p> <p>1. Auditoría: Proceso sistemático, independiente y documentado para obtener las evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoría.</p>	
--	--	---	--	--

		<p>Objeto dentro de una configuración que satisface una función de uso final.</p> <p>Relacionados a el proceso:</p> <ol style="list-style-type: none"> 1. Proceso: Conjunto de actividades mutuamente relacionadas que utilizan las entradas para proporcionar un resultado previsto. 2. Proyecto: Proceso único, consistente en un conjunto de actividades coordinadas y controladas con fechas de inicio y de finalización, llevadas a cabo para lograr un objetivo conforme con requisitos específicos, incluyendo las limitaciones de tiempo, costo y recursos. 3. Contrato: Acuerdo vinculante. 4. Diseño y desarrollo: Conjunto de procesos que transforman los requisitos para un objeto en 	<ol style="list-style-type: none"> 2. Conformidad: Cumplimiento de un requisito. 3. No conformidad: Incumplimiento de un requisito. 4. Acción correctiva: Acción para eliminar la causa de una no conformidad y prevenir que vuelva a ocurrir. 5. Mejora continua: Actividad recurrente para mejorar el desempeño. 6. Eficacia: Grado en el cual se realiza las actividades planificadas y se logran los resultados planificados. 7. Indicador: Representación medible de la condición o estado de las operaciones, de la gestión o de las condiciones. 8. Seguimiento: Determinación del estado de un sistema, un proceso (3.26) o una actividad. 9. Medición: Proceso para determinar un valor. 10. Desempeño: Resultado medible. 11. Desempeño ambiental: Desempeño relacionado con la gestión de 	
--	--	---	--	--

		<p>requisitos más detallados para ese objeto.</p> <p>Términos relativos al sistema:</p> <ol style="list-style-type: none">1. Sistema: Conjunto de elementos interrelacionados o que interactúan.2. Sistema de gestión: Conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas, objetivos y procesos para lograr estos objetivos.3. Sistema de gestión de la calidad: Parte de un sistema de gestión relacionada con la calidad.4. Ambiente de trabajo: Conjunto de condiciones bajo las cuales se realiza el trabajo.5. Política: Intenciones y dirección de una organización como las expresa formalmente su alta dirección.6. Política de la calidad: Política relativa a la calidad.	<p>aspectos ambientales.</p>	
--	--	--	------------------------------	--

		<p>7. Misión: Propósito de la existencia de la organización, tal como lo expresa la alta dirección.</p> <p>8. Visión: Aspiración de aquello que una organización querría llegar a ser, tal como lo expresa la alta dirección.</p> <p>Relacionados a los requisitos:</p> <p>1. Objeto u ítem: Cualquier cosa que puede percibirse o concebirse.</p> <p>2. Calidad: Grado en el que un conjunto de características inherentes de un objeto cumple con los requisitos.</p> <p>3. Clase: Categoría o rango dado a diferentes requisitos para un objeto que tienen el mismo uso funcional.</p> <p>4. Requisito: Necesidad o expectativa establecida, generalmente implícita u obligatoria.</p> <p>5. Requisito de la calidad: Requisito relativo a la calidad</p>		
--	--	---	--	--

		<p>6. Requisito legal: Requisito obligatorio especificado por un organismo legislativo.</p> <p>7. No conformidad: Incumplimiento de un requisito.</p> <p>8. Defecto: No conformidad relativa a un uso previsto o especificado.</p> <p>9. Conformidad: Cumplimiento de un requisito.</p> <p>10. Capacidad: Aptitud de un objeto para realizar una salida que cumplirá los requisitos para esa salida.</p> <p>11. Trazabilidad: Capacidad para seguir el histórico, la aplicación o la localización de un objeto.</p> <p>12. Confiabilidad: Capacidad para desempeñar como y cuando se requiera.</p> <p>13. Innovación: Objeto nuevo o cambiado que crea o redistribuye valor.</p> <p>Relacionados al resultado:</p>		
--	--	---	--	--

		<ol style="list-style-type: none"> 1. Objetivo: Resultado a lograr. 2. Objetivo de la calidad: Objetivo relativo a la calidad. 3. Éxito: Logro de un objetivo. 4. Éxito sostenido: Éxito durante un periodo de tiempo. 5. Salida: Resultado de un proceso. 6. Producto: Salida de una organización que puede producirse sin que se lleve a cabo ninguna transacción entre la organización y el cliente. 7. Servicio: Salida de una organización con al menos una actividad, necesariamente llevada a cabo entre la organización y el cliente. 8. Desempeño: Resultado medible. 9. Riesgo: Efecto de la incertidumbre. 10. Eficiencia: Relación entre el resultado alcanzado y los recursos utilizados. 11. Eficacia: Grado en el que se realizan las actividades planificadas y se 		
--	--	---	--	--

		<p>logran los resultados planificados.</p> <p>Términos relativos a los datos, la información y la documentación:</p> <ol style="list-style-type: none">1. Datos: Hechos sobre un objeto.2. Información: Datos que poseen significado.3. Sistema de información: Red de canales de comunicación utilizados dentro de una organización.4. Documento: Información y el medio en el que está contenida.5. Información documentada: Información que una organización tiene que controlar y mantener, y el medio que la contiene.6. Manual de la calidad: Especificación para el sistema de gestión de la calidad de una organización.7. Plan de la calidad: Especificación de los procedimientos y recursos asociados a aplicar, cuando deben aplicarse y		
--	--	---	--	--

		<p>quien debe aplicarlos a un objeto específico.</p> <p>8. Verificación: Confirmación, mediante la aportación de evidencia objetiva de que se han cumplido con los requisitos.</p> <p>Relacionados al cliente:</p> <ol style="list-style-type: none">1. Retroalimentación: Opiniones, comentarios y muestras de interés por un producto, un servicio, o un proceso de tratamiento de quejas.2. Satisfacción del cliente: Percepción del cliente sobre el grado en que se han cumplido las expectativas.3. Queja: Expresión de insatisfacción hecha a una organización, relativa a su producto, servicio, o al propio proceso de tratamiento de quejas, donde explícita o implícitamente se espera una respuesta o resolución.4. Servicio al cliente: Interacción de la		
--	--	--	--	--

		<p>organización con el cliente a lo largo del ciclo de vida de un producto o un servicio.</p> <p>Relacionados con las acciones:</p> <ol style="list-style-type: none">1. Acción preventiva: Acción tomada para eliminar la causa de una no conformidad u otra situación potencial no deseable.2. Acción correctiva: Acción para eliminar la causa de una no conformidad y evitar que vuelva a ocurrir.3. Concesión: Autorización para utilizar o liberar un producto o servicio que no es conforme con los requisitos especificados.4. Reproceso: Acción tomada sobre un producto o servicio no conforme para hacerlo conforme con los requisitos.5. Desecho: Acción tomada sobre un producto o servicio no conforme para impedir su uso		
--	--	---	--	--

		<p>inicialmente previsto.</p> <p>Relacionados con la auditoría:</p> <ol style="list-style-type: none">1. Auditoría: 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.2. Auditoría combinada: Auditoría llevada a cabo conjuntamente a un único auditado en dos o más sistemas de gestión.3. Programa de auditoría: Conjunto de una o mas auditorías planificadas para un periodo de tiempo determinado y dirigidas hacia un propósito específico.4. Alcance de la auditoría: Extensión y límites de una auditoría.		
--	--	---	--	--

		<p>5. Plan de auditoría: Descripción de las actividades y de los detalles acordados de una auditoría.</p> <p>6. Hallazgos de la auditoría: Resultados de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de esta.</p> <p>7. Conclusiones de la auditoría: Resultado de una auditoría, tras considerar los objetivos de la auditoría y todos los hallazgos de esta.</p>		
4.1	Comprensión de la organización y de su contexto.	La organización debe establecer las cuestiones externas e internas relacionadas con su propósito y su direccionamiento estratégico y que a su vez afectan la capacidad de cumplir con los objetivos del sistema de gestión de la calidad (SGC).	La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que por tanto afectan a su capacidad de lograr los resultados previstos de su sistema de gestión ambiental.	La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan su capacidad para lograr los resultados previstos de su SGSI.
4.2	Comprensión de las necesidades y de su contexto.	Debido al potencial efecto en la capacidad de la organización de entrega regularmente de los productos y servicios que satisfagan los requisitos de los clientes y los reglamentarios, la organización debe identificar de manera clara las partes interesadas	La organización debe determinar las partes interesadas que son pertinentes al sistema de gestión ambiental junto con sus necesidades y expectativas. Además de esto, identificar cuáles de estas necesidades y expectativas se convierten en obligaciones de cumplimiento.	La organización debe determinar las partes interesadas que son pertinentes al SGI y los requisitos de estas partes interesadas.

		pertenecientes al SGC y los requisitos de estas.		
4.3	Determinación del alcance del sistema de gestión.	<p>La organización debe identificar los límites y aplicabilidad del SGC para definir su alcance. Por lo tanto, cuando se define el alcance se debe considerar las cuestiones internas y externas, los requisitos de las partes interesadas y los productos y servicios de la organización.</p> <p>Es de suma importancia recordar que el alcance del sistema debe mantenerse y estar disponible como información documentada.</p>	<p>La organización debe determinar los límites y la aplicabilidad del sistema de gestión ambiental para establecer su alcance. Cabe mencionar que para determinar dicho alcance la organización debe tener en cuenta las cuestiones internas y externas, los requisitos legales y otros requisitos, las unidades, funciones, límites físicos, actividades, productos, servicios de la organización y la autoridad y capacidad para ejercer control e influencia.</p> <p>Es de suma importancia recordar que el alcance del sistema debe mantenerse y estar disponible como información documentada.</p>	<p>La organización debe determinar los límites y la aplicabilidad del SGI para establecer su enlace.</p> <p>Cuando es determinado el alcance, la organización debe considerar las cuestiones externas e internas, los requisitos y las interfaces y dependencias entre las actividades realizadas por la organización y las que realizan otras organizaciones.</p> <p>El alcance debe estar disponible como información documentada.</p>
4.4	Sistema de gestión.	<p>Sistema de gestión de la calidad y sus procesos:</p> <p>La organización debe establecer, implementar, mantener y mejorar de manera continua un SGC con sus procesos necesarios y respectivas interacciones.</p> <p>Por otro lado, la organización a la hora de identificar los procesos necesarios para el SGC debe: definir las entradas requeridas y salidas esperadas de los procesos, la secuencia e interacción de los procesos, definir e implementar criterios y</p>	<p>Sistema de gestión ambiental:</p> <p>La organización con el fin de mejorar su desempeño ambiental debe establecer, implementar y mejorar de manera continua un sistema de gestión ambiental en donde están incluidos todos los procesos necesarios y sus interacciones.</p>	<p>La organización debe establecer, implementar, mantener y mejorar continuamente el SGSI, de acuerdo con los requisitos de esta Norma.</p>

		<p>los métodos de medición para asegurarse de eficiencia y eficacia de la operación y control de procesos, definir y asignar los recursos necesarios para los procesos y definir las responsabilidades y autoridades para los diferentes procesos. En continuación a esto, la organización también debe abordar los riesgos y oportunidades, evaluar e implementar cualquier cambio necesario para asegurar el logro de los resultados provistos y la mejora del sistema en general.</p>		
5.1	Liderazgo y compromiso.	<p>La alta dirección debe evidenciar liderazgo y compromiso con el SGC asumiendo la responsabilidad y obligación de rendir cuentas de la eficacia del SGC, estableciendo la política de la calidad y los objetivos de la calidad (éstos deben ser compatibles con el contexto y el direccionamiento estratégico de la organización), asegurando la integración de los requisitos del SGC en los procesos de negocio y Promoviendo el uso del enfoque a procesos y el pensamiento basado en riesgos.</p> <p>Además de esto, a organización evidencia el liderazgo y compromiso</p>	<p>La alta dirección debe demostrar liderazgo y compromiso hacia el sistema de gestión ambiental asumiendo la obligación de rendir cuentas con relación a la eficacia del sistema de gestión ambiental, asegurando que se establezcan la política ambiental y los objetivos ambientales, y que estos sean compatibles con la dirección estratégica y el contexto de la organización, asegurando la integración de los requisitos del sistema de gestión ambiental dentro de los procesos de negocio de la organización, asegurando que los recursos necesarios para el sistema de gestión ambiental estén disponibles; comunicando la importancia de una gestión ambiental eficaz y de la conformidad con los requisitos del SGSI; asegurando que el SGSI logre los resultados</p>	<p>La alta dirección debe demostrar liderazgo y compromiso con respecto al SGSI asegurando que se establezca la política de la seguridad de la información y los objetivos de la seguridad de la información, y que estos sean compatibles con la dirección estratégica de la organización; asegurando la integración de los requisitos del SGSI en los procesos de la organización; asegurando que los recursos necesarios para el SGSI estén disponibles; comunicando la importancia de una gestión de la información eficaz y de la conformidad con los requisitos del SGSI; asegurando que el SGSI logre los resultados</p>

		asegurando que los recursos necesarios para el SGC estén disponibles, comunicando la importancia de una gestión de la calidad eficaz y conforme con los requisitos del sistema, asegurando que el SGC logre los resultados previstos, comprometiendo, dirigiendo y apoyando a las personas, para contribuir a la eficacia del sistema, incentivando la mejora, apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo en sus áreas de responsabilidad.	conforme con los requisitos del sistema de gestión ambiental, asegurando que el sistema de gestión ambiental logre los resultados previstos. Adicionalmente para lograr demostrar esto la organización de debe dirigir y apoyar a las personas, para contribuir a la eficacia del sistema de gestión ambiental, promover la mejora continua y apoyar otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidad.	previstos; dirigiendo y apoyando a las personas, para contribuir a la eficacia del SGSI; promoviendo la mejora continua; y apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidad.
5.1.2	Enfoque al cliente.	La alta dirección mediante: la determinación, comprensión y cumplimiento en forma constante de los requisitos del cliente y los legales, la identificación y gestión de los riesgos y oportunidades que pueden afectar a la conformidad de los productos y los servicios y a la capacidad de aumentar la satisfacción del cliente, demuestra liderazgo y compromiso con respecto al enfoque del cliente. Cabe resaltar que la organización debe mantener como pilar fundamental el enfoque u objetivo del aumento de la satisfacción del cliente.	La alta dirección mediante la determinación, comprensión y cumplimiento de los requisitos ambientales y legales que afectan de manera directa a los tres clientes principales de la norma, las personas, la sociedad y el planeta. Además de esto, identificar riesgos y oportunidades que puedan contribuir a el desarrollo y bienestar de los tres clientes ya previamente enunciados.	La alta dirección mediante la determinación, comprensión y cumplimiento de los diferentes requisitos deberá velar por la seguridad de la información de cada uno de sus clientes o usuarios logrando de esta manera su satisfacción y por tanto alta confiabilidad.
5.2	Política.	La alta dirección debe definir, implementar y mantener una política de	La alta dirección debe definir, implementar y mantener una política	La alta dirección debe establecer una política de la seguridad de la

		<p>la calidad que sea adecuada al propósito y contexto de la organización, es decir, que apoye su direccionamiento estratégico. También esta debe proporcionar un marco de referencia para la definición de los objetivos de la calidad, compromiso de cumplir los requisitos aplicables y con la mejora continua del SGC.</p> <p>Así pues, la política de la calidad debe comunicarse, entenderse, aplicarse y estar disponible como información documentada y para en general todas las partes interesadas según corresponda.</p>	<p>ambiental la cual sea adecuada al propósito y contexto de la organización (que tenga en cuenta los requisitos legales y otros requisitos), incluida la naturaleza, magnitud e impactos ambientales de sus actividades, productos y servicios. Además, dicha política debe proporcionar un marco de referencia para el establecimiento de los objetivos ambientales y a su vez incluya compromisos para la protección del medio ambiente, incluida la prevención de la contaminación y otros compromisos pertinentes al contexto de la organización; es importante mencionar que esta política debe incluir también un compromiso de mejora continua del sistema de gestión ambiental para mejorar el desempeño ambiental.</p> <p>Teniendo en cuenta lo previamente mencionado, la política ambiental debe mantenerse como información documentada, comunicarse dentro de la organización a todas las personas y estar disponible para las partes interesadas.</p>	<p>información que sea adecuada al propósito de la organización, incluya objetivos de seguridad de la información o proporcione el marco de referencia para el establecimiento de los objetivos de la seguridad de la información; incluya el compromiso de cumplir los requisitos aplicables relacionados con la seguridad de la información e incluya el compromiso de mejora continua del SGSI.</p> <p>La política de la seguridad de la información debe estar disponible como información documentada, comunicarse dentro de la organización y estar disponible para las partes interesadas.</p>
5.3	Roles, responsabilidades y autoridades en la organización.	La alta dirección debe otorgar la responsabilidad y autoridad para asegurar que: el sistema es conforme con los requisitos de la norma, los procesos generan las salidas previstas, se	La alta dirección debe asegurarse de que las responsabilidades y autoridades para las funciones pertinentes se asignen y comuniquen dentro de la organización con el fin de informar a la	La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen.

		<p>comunique a la alta dirección sobre el desempeño del sistema y sobre las oportunidades de mejora. Adicionalmente, se debe asegurar tanto el enfoque al cliente a través de la organización como la continua integridad del SGC cuando se planifican e implementan cambios en el sistema.</p> <p>En conclusión, la alta Dirección debe asegurarse que las responsabilidades y autoridades para los roles se asignen, comuniquen y comprendan dentro de la organización.</p>	<p>alta dirección sobre el sistema de gestión, incluido su desempeño y además, asegurarse que el sistema de gestión ambiental es conforme con los requisitos de la ISO14001:2015.</p>	<p>La alta dirección debe asignar la responsabilidad y autoridad para asegurarse de que el SGSI sea conforme con los requisitos de esta Norma e informar a la alta dirección sobre el desempeño del SGSI</p>
6.1	<p>Acciones para abordar riesgos y oportunidades.</p>	<p>La organización al planificar el sistema debe considerar las cuestiones internas y externas analizadas en el numeral 4.1 y los requisitos de partes interesadas definidos en el numeral 4.2. Adicionalmente, debe identificar los riesgos y oportunidades con el fin de asegurar que el sistema logre los resultados previstos, incrementar los efectos deseables, prevenir o reducir efectos no deseados y lograr la mejora.</p> <p>En adición a esto, la organización debe planificar: acciones para abordar los riesgos y oportunidades</p>	<p>La organización debe planificar, implementar y mantener los procesos para cumplir los requisitos del capítulo 6. Por tanto, al planificar el sistema de gestión ambiental, la organización debe considerar: las cuestiones referidas en el numeral 4.1, los requisitos referidos en el numeral 4.2, el alcance de su sistema de gestión ambiental.</p> <p>Asimismo, la organización debe determinar los riesgos y oportunidades relacionados con sus aspectos ambientales, requisitos legales y otros requisitos, otras cuestiones requisitos identificados en el numeral 4.1 y 4.2. Lo anterior es abordado para:</p>	<p>Generalidades:</p> <p>Al planificar el SGSI, la organización debe determinar los riesgos y oportunidades que en necesario tratar con el fin de asegurarse de que el SGSI pueda lograr sus resultados previstos, prevenir o reducir efectos indeseados y lograr la mejora continua.</p> <p>La organización debe planificar:</p> <p>Las acciones para tratar estos riesgos y oportunidades, la manera de integrar e implementar estas acciones en sus procesos del SGSI y la manera de evaluar la eficacia de estas acciones</p>

		<p>identificados, la manera de integrar e implementar las acciones en los procesos del sistema y evaluar la eficacia de estas acciones.</p>	<p>brindar seguridad de que el sistema de gestión ambiental puede lograr sus resultados previstos, prevenir o reducir los efectos indeseados (incluido el potencial de qué condiciones ambientales externas afecten la organización) y lograr la mejora continua.</p> <p>Por otro lado, dentro del alcance del sistema de gestión ambiental, la organización debe determinar las situaciones de emergencia potenciales, incluidas las que pueden tener un impacto ambiental; toda la información mencionada debe mantenerse documentada por parte de la organización.</p>	<p>Valoración de riesgos de la SI:</p> <p>La organización debe definir y aplicar un proceso de valoración de riesgos de la SI que establezca y mantenga criterios de riesgo de la SI que incluyan los criterios de aceptación de riesgos y los criterios para realizar valoraciones de riesgos de la SI; asegurarse que las valoraciones repetidas de riesgos de la SI produzcan resultados consistentes, válidos y comparables; Identifique los riesgos de SI; Analice los riesgos de la SI y evalúe los riesgos de SI.</p> <p>Tratamiento de riesgos de la SI:</p> <p>La organización debe definir y aplicar un proceso de tratamiento de riesgos de la SI para seleccionar las opciones apropiadas de tratamiento de riesgos de la SI, teniendo en cuenta los resultados de la valoración de riesgos; determinar todos los controles que sean necesarios para implementar las opciones escogidas para el tratamiento de riesgos de la SI; comparar los controles determinados con los del Anexo A, y verificar que no se han omitido controles necesarios; producir una</p>
--	--	---	---	--

				<p>declaración de aplicabilidad que contenga los controles necesarios y la justificación de las inclusiones, ya sea que se implementen o no; formular un plan de tratamiento de riesgos de la SI; y obtener, de parte de los dueños de los riesgos, la aprobación de plan de tratamiento de riesgos de la SI, y la aceptación de los riesgos residuales de la seguridad de la información.</p> <p>La organización debe conservar la información documentada acerca del proceso de tratamiento de riesgos de la SI.</p>
6.2	Objetivos y planificación para lograrlos.	<p>Objetivos de la calidad.</p> <p>La organización debe definir los objetivos de la calidad para las funciones, niveles y procesos del sistema. Por consiguiente, los objetivos de la calidad deben ser coherentes con la política de la calidad, deben ser medibles, deben cumplir los requisitos aplicables, tienen que estar relacionados con la conformidad de los productos y servicios y el aumento de la satisfacción del cliente, deben ser objeto de seguimiento y ser comunicados.</p> <p>Planificación de acciones para cumplir los objetivos de calidad.</p>	<p>Objetivos ambientales.</p> <p>La organización debe establecer los objetivos ambientales en las funciones y niveles pertinentes teniendo en cuenta los aspectos ambientales significativos, sus requisitos legales y otros, y considerando sus riesgos y oportunidades. Así pues, los objetivos ambientales deben ser tanto coherentes con la política ambiental, ser medibles (de ser posible), ser objeto de seguimiento, así como ser comunicados a cada persona de la organización.</p> <p>Planificación de acciones para cumplir los objetivos ambientales.</p>	<p>La organización debe establecer los objetivos de SI en las funciones y niveles pertinentes.</p> <p>Los objetivos de SI deben ser coherentes con la política de SI; ser medibles; tener en cuenta los requisitos de la SI aplicables, y los resultados de la valoración y del tratamiento de los riesgos; ser comunicados; y ser actualizados, según sea apropiado.</p> <p>La organización debe conservar la información documentada sobre los objetivos de la SI.</p> <p>Cuando se hace la planificación para lograr sus objetivos de la SI, la</p>

		A causa de los aspectos anteriormente indicados al planificar el logro de los objetivos, la organización debe definir el que va a hacer, que recursos se requieren para esto, quien será el responsable, cuando se finalizarán y como se evaluarán los resultados.	Cuando se realiza la planificación para lograr sus objetivos ambientales, la organización debe determinar que se va a hacer, que recursos se requieren para esto, quienes serán responsables, cuando se finalizara y como se evaluarán los resultados, incluidos de seguimiento de los avances para el logro de objetivos ambientales medibles. Dicho de otra manera, la organización debe considerar como se pueden integrar las acciones para el logro de los objetivos ambientales en los procesos de negocio de la organización.	organización debe determinar lo que se va a hacer; que recursos se requerirán; quién será responsable; cuándo finalizara; y cómo se evaluarán los resultados.
6.3	Planificación de los cambios.	Cuando la organización identifique una necesidad de cambios en el SGC, se deben llevar a cabo de manera planificada y sistemática.	-	
7.1	Recursos.		La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión ambiental.	La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI.
7.1.2	Personas.	La organización debe establecer y asignar las personas necesarias para la implementación eficaz del SGC y para la operación y control de sus procesos.		
7.1.3	Infraestructura.	La organización debe establecer, asignar y mantener la infraestructura necesaria para que la operación de		

		los procesos sea eficaz y se logre la conformidad de los productos y servicios.		
7.1.4	Ambiente para la operación de los procesos.	La organización debe establecer, asignar y mantener el ambiente requerido para la operación de sus procesos y para lograr la conformidad de los productos y servicios.		
7.1.6	Conocimientos de la organización.	<p>La organización debe establecer los conocimientos necesarios para la operación de sus procesos y para la conformidad de los productos y servicios. Sin embargo, estos conocimientos deben protegerse y estar disponibles en la extensión necesaria.</p> <p>Por otra parte, cuando se tratan las necesidades y tendencias cambiantes, la organización debe tener en cuenta sus conocimientos actuales y determinar cómo adquirir conocimientos adicionales necesarios las actualizaciones requeridas.</p>		
7.2	Competencia.	La organización debe: establecer la competencia requerida de las personas que realizan un trabajo que afecta al desempeño y eficacia del SGC, asegurar que las personas sean competentes, basados en la educación, formación, o experiencia laboral, implementar acciones para alcanzar la competencia necesaria de	La organización debe: determinar la competencia necesaria de las personas que realizan bajo su control, un trabajo que afecta a su desempeño ambiental y su capacidad para cumplir sus requisitos legales y otros requisitos, asegurarse de que estas personas sean competentes, basándose en la educación, formación,	La organización debe determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta su desempeño de la seguridad de la información; asegurarse de que estas personas sean competentes, basándose en la educación, formación o experiencia adecuadas;

		<p>las personas y evaluar la eficacia de las acciones tomadas. Además de esto, se debe conservar la información documentada apropiada, como evidencia de la competencia.</p>	<p>o experiencia laboral, implementar acciones para alcanzar la competencia necesaria de las personas, determinar las necesidades de formación asociadas con sus aspectos ambientales y su sistema de gestión ambiental. En adición a esto, cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones tomadas (al igual que en todos los numerales de la norma se debe tener información documentada apropiada como evidencia).</p>	<p>cuando sea posible tomar acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones tomadas y conservar la información documentada apropiada como evidencia de la competencia.</p>
7.3	Toma de conciencia.	<p>La organización debe trabajar para que sus empleados sean conscientes de: La política de calidad, los objetivos de calidad pertinentes, la contribución que realizan a la eficiencia del sistema de gestión de calidad y las implicaciones que conlleva no cumplir los requisitos del sistema.</p>		<p>Las personas que realizan el trabajo bajo el control de la organización deben tomar conciencia de la política de la seguridad de la información; su contribución a la eficacia del SGSI, incluyendo los beneficios de una mejora del desempeño de la seguridad de la información y las implicaciones de la no conformidad con los requisitos del SGSI.</p>
7.4	Información documentada.	<p>El sistema de gestión de calidad de la organización debe incluir: La información documentada requerida por la norma y la información documentada que la organización determine como necesaria para una mayor eficiencia. La extensión de la información documentada varía de</p>	<p>El sistema de gestión ambiental de la organización debe incluir: La información documentada requerida por la norma y la información documentada que la organización determine como necesaria para una mayor eficiencia del SGA.</p> <p>Creación y actualización:</p>	<p>El SGSI de la organización debe incluir la información documentada requerida por esta Norma y la información documentada que la organización ha determinado que es necesaria para la eficacia del SGSI.</p> <p>Creación y actualización:</p>

		<p>una empresa a otra, debido a: El tamaño de la empresa y el tipo de actividad que realiza, la complejidad de los procesos con los que cuenta y la competencia de las personas.</p>	<p>Al momento de crear y actualizar la información documentada, la organización debe asegurarse de que lo siguiente sea adecuado: La identificación y descripción, el formato y la revisión y aprobación con respecto a la conveniencia y adecuación.</p> <p>Control de la información documentada:</p> <p>La información documentada se debe controlar para asegurarse de que: Este disponible y sea idónea para su uso, dónde y cuándo se necesite; esté protegida adecuadamente.</p> <p>La información documentada de origen externo se debe determinar según sea apropiado, y controlar.</p>	<p>Cuando se crea y actualiza información documentada, la organización debe asegurarse de que sea apropiado la identificación y descripción; el formato y sus medios de soporte; y la revisión y aprobación con respecto a la idoneidad y adecuación.</p> <p>Control de la información documentada:</p> <p>La información documentada requerida por el SGSI y por la ISO 27001 se debe controlar para asegurarse de que esté disponible y adecuada para su uso, donde y cuando se necesite; esté protegida adecuadamente.</p> <p>Para el control de la información documentada, la organización debe tratar las siguientes actividades: Distribución, acceso, recuperación y uso; almacenamiento y preservación, incluida la preservación de la legibilidad; y retención y disposición.</p> <p>La información documentada de origen externo que la organización considero necesaria para la planificación y operación del SGSI debe ser identificada y controlada.</p>
--	--	--	---	---

8	Operación.			
8.1	Planificación y control operacional.	<p>La organización debe planear, implantar y controlar los procesos necesarios para cumplir los requisitos establecidos, por medio de: La determinación de todos los requisitos de los servicios y productos de esta, los criterios para los procesos y que se acepten los servicios y los productos, la determinación de todos los recursos necesarios para conseguir la conformidad de los requisitos de los servicios y los productos, la determinación y almacenamiento de la información documentada.</p>	<p>La organización debe establecer, implementar, controlar y mantener los procesos necesarios para satisfacer los requisitos del sistema de gestión ambiental mediante: El establecimiento de criterios de operación para los procesos y la implementación del control de los procesos de acuerdo con los criterios de operación.</p> <p>La organización debe controlar los cambios planificados y examinar las consecuencias de los cambios no previstos, tomando acciones para mitigar los efectos adversos cuando sea necesario.</p> <p>La organización debe asegurarse de que los procesos contratados externamente estén controlados o que se tenga influencia sobre ellos. En el SGA se debe definir el tipo y grado de control o influencia que se va a aplicar a estos procesos.</p>	<p>La organización debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos de SI. La organización también debe implementar planes para lograr los objetivos de la SI.</p> <p>La organización debe mantener la información documentada en la medida necesaria para tener la confianza en que los procesos se han llevado a cabo según lo planificado.</p> <p>La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no previstos, tomando acciones para mitigar los efectos adversos, cuando sea necesario.</p> <p>La organización debe asegurar que los procesos contratados externamente estén controlados.</p>
8.2	Preparación y respuestas ante emergencias.	<p>La empresa debe actuar en una salida no conforme de las siguientes formas: Con la corrección, separación, contención, devolución o suspensión de productos, información del cliente y obtención de la autorización para la</p>	<p>La organización debe establecer, implementar y mantener los procesos necesarios acerca de como prepararse y responder a situaciones potenciales de emergencia identificadas. Para esto la organización debe: Prepararse para responder, mediante la planificación de acciones</p>	<p>La organización debe llevar a cabo valoraciones de riesgos de la SI a intervalos planificados o cuando se propongan u ocurran cambios significativos.</p> <p>La organización debe conservar la información documentada de los</p>

		<p>aceptación bajo concesión.</p> <p>Cuando se realicen todas las correcciones de las salidas no conformes la organización debe verificar la conformidad con los requisitos.</p> <p>La información que se debe consignar en los documentos de la organización es: La descripción de la conformidad, la descripción de las acciones tomadas, la descripción de todas las concesiones obtenidas y la identificación de la autoridad que ha decidido la acción a tomar respecto a la no conformidad.</p>	<p>para prevenir o mitigar los impactos ambientales adversos provocados por situaciones de emergencia; responder a situaciones de emergencias reales; tomar acciones para prevenir o mitigar las consecuencias de las situaciones de emergencia y el impacto ambiental potencial; poner a prueba periódicamente las acciones de respuesta planificadas; evaluar y revisar periódicamente los procesos y las acciones de respuesta planificadas y proporcionar información y formación pertinentes a las partes interesadas, incluidas las personas que trabajan bajo su control.</p>	<p>resultados de las valoraciones de riesgos de la SI.</p>
9	Evaluación del desempeño .			
9.1	Seguimiento, medición, análisis y evaluación.	<p>La organización tiene que establecer: A qué es necesario hacerle una medición y un seguimiento, los métodos que se van a utilizar para realizar el seguimiento, medición, análisis y evaluación necesarios para obtener los resultados esperados, cada cuanto se realizan los seguimientos y mediciones y cuando se debe hacer el análisis y evaluación de los resultados de seguimiento y medición.</p>	<p>La organización debe hacer seguimiento, medición, análisis y evaluación de su desempeño ambiental.</p> <p>La organización debe determinar: A qué hacerle seguimiento y medición; los métodos que se van a usar para el seguimiento, medición, análisis y evaluación para asegurar resultados acertados; los criterios para evaluar el desempeño ambiental, y los indicadores adecuados; cada cuanto se debe realizar el seguimiento y medición y cada cuanto se debe analizar y evaluar los</p>	<p>La organización debe evaluar el desempeño de la SI y la eficacia del SGSI.</p> <p>La organización debe determinar a qué es necesario hacer seguimiento y qué es necesario medir, incluidos los procesos y controles de la seguridad de la información; los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos; cuándo se deben llevar a cabo el seguimiento y la medición; quién debe</p>

		<p>La organización debe tener toda la información necesaria documentada.</p> <p>Satisfacción del cliente:</p> <p>La organización debe hacer el seguimiento de los comentarios de los clientes para poder cumplir sus necesidades y expectativas. LA organización debe establecer los métodos a utilizar para realizar el seguimiento y revisión de la información.</p> <p>Análisis y evaluación:</p> <p>La organización debe analizar y evaluar los datos y la información necesaria que sale del seguimiento y medición.</p> <p>Los resultados obtenidos son utilizados para la evaluación de: La conformidad de los productos y servicios ofrecidos, el nivel de satisfacción del cliente, el desempeño y la eficiencia del sistema, la eficacia de lo planteado en el proceso, la eficiencia de todas las acciones tomadas para realizar los riesgos y las oportunidades, la labor que realizan los proveedores externos y la necesidad de mejorar el SGC.</p>	<p>resultados del seguimiento y la medición.</p> <p>Adicionalmente debe asegurarse de que se usan y mantienen equipos de seguimiento y medición calibrados o verificados, según corresponda; evaluar su desempeño ambiental y la eficacia del sistema de gestión ambiental; comunicar externa e internamente la información que considere necesaria para obtener un buen desempeño ambiental y por último debe conservar la información documentada apropiada como evidencia de los resultados del seguimiento, medición, el análisis y la evaluación.</p> <p>Evaluación del cumplimiento:</p> <p>La organización debe establecer, implementar y mantener los procesos necesarios para evaluar el cumplimiento de sus requisitos legales y otros requisitos.</p> <p>Debe determinar la frecuencia con la que se evaluará el cumplimiento; evaluar el cumplimiento y emprender las acciones de su estado de cumplimiento.</p> <p>Debe documentar la información como evidencia de los resultados de la evaluación del cumplimiento.</p>	<p>llevar a cabo el seguimiento y la medición; cuándo se debe analizar y evaluar los resultados del seguimiento y medición; y quién debe analizar y evaluar estos resultados.</p> <p>La organización debe conservar información documentada apropiada como evidencia de los resultados del monitoreo y de la medición.</p>
--	--	---	---	--

<p>9.2</p>	<p>Auditoría interna.</p>	<p>La organización tiene que planificar cada cuanto debe realizar las auditorías internas, para obtener información sobre el SGC como:</p> <ul style="list-style-type: none"> a) La conformidad con los requisitos de la organización para el SGC b) Se implanta y se mantiene de forma eficaz <p>La organización debe:</p> <ul style="list-style-type: none"> a) Planificar, establecer, implantar y mantener diferentes programas de auditorías que incluyen la frecuencia, la metodología, la responsabilidad, los requisitos y elaboración de informes, también deben considerar la importancia de todos los procesos que se encuentran involucrados, los cambios que pueden afectar a la organización y los resultados que se obtienen de las auditorías previas. b) Se deben definir los criterios en los que se basa la 	<p>La organización debe realizar auditorías internas en intervalos acordados para obtener información acerca de si el SGA es conforme con los requisitos propios de la organización para sus SGA y los requisitos de la norma; y si se implementa y mantiene eficazmente.</p> <p>Programa de auditoría interna:</p> <p>La organización debe establecer, implementar y mantener uno o varios programas de auditoría interna y también debe tener en cuenta la importancia ambiental de los procesos involucrados. Debe definir los criterios de auditoría y el alcance para cada auditoría; seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría; y asegurarse de que los resultados de las auditorías se informen a la dirección pertinente.</p>	<p>La organización debe llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si el SGSI es conforme con los propios requisitos de la organización para sus SGSI y los requisitos de esta norma; si la organización debe planificar, establecer, implementar y mantener uno o varios programas de auditoría que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación, y la elaboración de informes, Los programas de auditoría deben tener en cuenta la importancia de los procesos involucrados y los resultados de las auditorías previas; para cada auditoría, definir los criterios y el alcance de ésta; seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría; asegurarse de que los resultados de las auditorías se informan a la dirección pertinente; y conservar información documentada como evidencia de la implementación del programa de auditoría y de los resultados de ésta.</p>
------------	---------------------------	--	---	--

		<p>auditoría y el alcance que se evaluará en cada auditoría.</p> <p>c) Se debe realizar la selección de los auditores y realizar las auditorías asegurándose la objetividad y la imparcialidad del proceso de auditoría.</p> <p>d) Una vez finalizada la auditoría los resultados deben quedar plasmados en un informe para la alta dirección.</p> <p>e) La auditoría puede generar que se deban realizar acciones correctivas.</p> <p>f) La información debe estar bien almacenada como evidencia de la implantación del programa de auditoría y los resultados.</p>		
9.3	Revisión por la dirección.	<p>La dirección tiene que revisar el SGC de la organización en intervalos planificados, para lograr esto debe realizar y planificar las condiciones sobre:</p> <p>A) El estado en que se encuentran las acciones de las revisiones realizadas</p>	<p>LA alta dirección debe asegurarse de que el SGA tenga la conveniencia, adecuación y eficacia continuas.</p> <p>La revisión por la alta dirección debe incluir consideraciones sobre:</p> <p>a) Es estado de las acciones de las</p>	<p>La alta dirección debe revisar el SGSI de la organización a intervalos planificados, para asegurarse de su conveniencia, adecuación y eficacia continuas.</p> <p>La revisión por la dirección debe incluir consideraciones sobre el estado de las acciones con relación a las revisiones</p>

		<p>B) Los cambios realizados en las cuestiones internas y externas que son referentes al SGC</p> <p>C) La información sobre el desempeño y la eficiencia del SGC incluye: La satisfacción del cliente y de las partes interesadas, el grado en el que se han conseguido los objetivos de la calidad, el desempeño de todos los procesos y la conformidad de los productos, las no conformidades y las acciones correctivas, los resultados obtenidos por el seguimiento y la medición, los resultados de las auditorías internas, el desempeño de los proveedores externos, adecuación de los recursos internos, la eficiencia de todas las acciones que se toman para abordar los riesgos y las oportunidades.</p> <p>D) la eficiencia de todas las acciones que se toman</p>	<p>revisiones por la dirección previas</p> <p>b) Los cambios en las cuestiones externas e internas que sean pertinentes al sistema de gestión ambiental; las necesidades y expectativas de las partes interesadas, incluidos los requisitos legales y otros requisitos; sus aspectos ambientales significativos; y los riesgos y oportunidades</p> <p>c) El grado en el que se han logrado los objetivos ambientales</p> <p>d) La información sobre el desempeño ambiental de la organización, incluidas las tendencias relativas a no conformidades y acciones correctivas; resultados de seguimiento y medición; cumplimiento de los requisitos legales y otros requisitos; y resultados de las auditorías</p> <p>e) Adecuación de los recursos</p> <p>f) Las comunicaciones pertinentes de las</p>	<p>previas por la dirección; los cambios en las cuestiones externas e internas que sean pertinentes al SGC; retroalimentación sobre el desempeño de la SI, incluidas las tendencias relativas a no conformidades y acciones correctivas, seguimiento y resultados de las mediciones, resultados de auditoría, y cumplimiento de los objetivos de la SI; retroalimentación de las partes interesadas; resultados de la valoración de riesgos y estado del plan de tratamiento de riesgos; y las oportunidades de mejora continua.</p> <p>Los elementos de salida de la revisión por la dirección deben incluir las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambio en el SI.</p> <p>La organización debe conservar la información documentada como evidencia de los resultados de las revisiones por la dirección.</p>
--	--	--	---	--

		<p>para abordar los riesgos</p> <p>E) Las oportunidades y las oportunidades de mejora.</p>	<p>partes interesadas, incluidas las quejas</p> <p>g) Las oportunidades de mejora continua</p> <p>Las salidas deben incluir:</p> <p>a) Las conclusiones sobre la conveniencia, adecuación y eficacia continuas del SGA</p> <p>b) Las decisiones relacionadas con las oportunidades de mejora</p> <p>c) Las decisiones relacionadas con cualquier necesidad de cambio en el SGA, incluidas los recursos</p> <p>d) Las acciones necesarias cuando no se hayan logrado los objetivos ambientales</p> <p>e) Las oportunidades de mejora la integración del SGA a otros procesos de negocio</p> <p>f) Cualquier implementación para la dirección estratégica de la organización</p>	
10	Mejora.			
10.1	Generalidades.	Es importante que la organización tenga muy en cuenta la oportunidad de mejora para cumplir todos los requisitos del cliente e incrementar la satisfacción de este.	La organización debe determinar las oportunidades de mejora e implementar las acciones necesarias para lograr los resultados en su SGA.	

		<p>Para fortalecer el SGC la organización debe tomar iniciativas para realizar proyectos de mejora.</p> <p>Es importante que la organización reconozca sus oportunidades de mejora con la relación SGC con el fin de mejora de forma continua la satisfacción con el cliente.</p>		
10.2	No conformidades y acciones correctivas.	<p>No conformidades:</p> <ul style="list-style-type: none"> a) Para reaccionar ante la no conformidad se debe tomar acciones para controlarla y corregirla y hacer frente a las consecuencias b) Se debe evaluar las acciones para eliminar las causas de la no conformidad por medio de: La revisión y el análisis de la no conformidad, la determinación de las causas y la determinación de si existen no conformidades similares c) Implementar acciones necesarias d) Revisar la eficacia de cualquier acción correctiva tomada e) Cada que sea necesario 	<p>Cuando se presente un no conformidad la organización debe:</p> <ul style="list-style-type: none"> a) Reaccionar ante la no conformidad y cuando sea aplicable tomar acciones para controlarla y corregirla; y hacer frente a las consecuencias, incluida la mitigación de los impactos ambientales adversos b) Evaluar la necesidad de acciones para eliminar las causas de la no conformidad ya que no vuelva a ocurrir, mediante la revisión de la no conformidad; la determinación de las causas de la no conformidad; y finalmente la determinación de si existen no conformidades 	<p>Cuando ocurra una no conformidad, la organización debe reaccionar ante la no conformidad, y según sea aplicable tomar acciones para controlarla y corregirla, y hacer frente a las consecuencias; evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir ni ocurra en otra parte, mediante la revisión de la no conformidad, la determinación de las causas de la no conformidad, y la determinación de si existe no conformidades similares, o que potencialmente podrían ocurrir; implementar cualquier acción necesaria; revisar la eficacia de las acciones correctivas tomadas; y hacer cambios al SGSI si es necesario.</p> <p>Las acciones correctivas deben ser apropiadas a</p>

		<p>actualizar los riesgos y oportunidades determinados durante la planificación</p> <p>f) Hacer cambios al sistema de gestión de la calidad cada que sea necesario</p> <p>Información documentada como evidencia:</p> <p>a) La naturaleza de las no conformidades y cualquier acción tomada posteriormente</p> <p>b) Los resultados de cualquier acción correctiva.</p>	<p>similares, o que potencialmente puedan ocurrir.</p> <p>c) Implementar cualquier acción necesaria</p> <p>d) Revisar la eficacia de cualquier acción correctiva tomada</p> <p>e) Si es necesario, hacer cambios al SGA</p>	<p>los efectos de las no conformidades encontradas.</p> <p>La organización debe conservar la información documentada adecuada, como evidencia de la naturaleza de las no conformidades y cualquier acción posterior tomada; y los resultados de cualquier acción correctiva.</p>
10.3	Mejora continua.	La organización debe tener en cuenta los resultados del análisis y evaluación, y las salidas de la revisión de dirección, para identificar si hay oportunidades de mejora.	La organización debe mejorar continuamente la convivencia, adecuación y eficacia del SGA para mejorar el desempeño ambiental	La organización debe mejorar continuamente la convivencia, adecuación y eficacia del SGSI



