TABLA DE INTEGRACIÓN NORMAS NTC ISO 27001:2013 e ISO 31000:2018

COLOR DEL TEXTO	DEFINICIÓN DEL COLOR
	El texto en color negro pertenece a la norma **NTC-ISO/IEC 27001:2013** (textualmente)
	El texto en color azul pertenece a la norma **ISO 31000:2018** (textualmente)
	El texto en color azul pertenece a la norma **INTEGRAL** (por ejemplo S.I.G.)
	El texto en color naranja pertenece texto o conectores **ADICIONALES** a las normas

27001:2013	31000:2018	QUÉ HACER ?	GUIA PARA INTEGRAR	REDACCIÓN DEL MODELO INTEGRAL
Numerales	**Numerales**	**Equivalencia de X con Y**	**Cual norma de la base para la integración**	
4. CONTEXTO DE LA ORGANIZACIÓN	NO LO TIENE	27001	27001:2013	**4. CONTEXTO DE LA ORGANIZACIÓN**
NO LO TIENE	**6.3.3 CONTEXTOS EXTERNO E INTERNO** (Primer Parráfo)	31000	31000:2018	**4.1. CONTEXTOS EXTERNO E INTERNO** Los contextos externo e interno son el entorno en el cual la organización busca definir y lograr sus objetivos.
NO LO TIENE	Segundo Parráfo	31000 Incluyendo Seguridad de la información	31000:2018	El contexto del proceso de la gestión del riesgo y seguridad de la información, se debería establecer a partir de la comprensión de los entornos externo e interno en los cuales opera la organización y debería refeljar el entorno específico de la actividad en la cual se va a aplicar el proceso de la gestión del riesgo y seguridad de la información,.
NO LO TIENE	Tercer Parráfo	31000	31000:2018	La comprensión de contexto es importante porque:
NO LO TIENE	Primera Viñeta	31000 Incluyendo Seguridad de la información	31000:2018	a) la gestión del riesgo y seguridad de la información, tiene lugar en el contexto de los objetivos y las actividades de la organización;
NO LO TIENE	Segunda Viñeta	31000	31000:2018	b) los factores organizacionales pueden ser una fuente de riesgo;
NO LO TIENE	Tercera Viñeta	31000 Incluyendo Seguridad de la información	31000:2018	c) el propósito y alcance del proceso de la gestión del riesgo y seguridad de la información, puede estar interrelacionado con los objetivos de la organzación como un todo.
4.1. CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO (Primer Parráfo)	**5.4.1 COMPRENSIÓN DE LA ORGANIZACIÓN Y DE SU CONTEXTO** (Segundo Parráfo)	27001 + 31000 Incluyendo S.I.G.	27001:2013	**4.1.1 COMPRENSIÓN DE LA ORGANIZACIÓN Y DE SU CONTEXTO** 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 S.I.G. El análisis del contexto externo de la organización puede incluir pero no limitarse a:
NO LO TIENE	Primera Viñeta	31000	31000:2018	a) los factores sociles, culturales, políticos, legales, reglamentarios, financieros, tecnológicos, económincos y ambientales ya sea a nivel iternacional, nacional, reginal o local;
NO LO TIENE	Segunda Viñeta	31000	31000:2018	b) los impulsores clave y las tendencias que afectan a los objetivos de la organización;
NO LO TIENE	Tercera Viñeta	31000	31000:2018	c) las relaciones, percepciones, valores, necesidades y expectativas de las partes interesadas externas;
NO LO TIENE	Cuarta Viñeta	31000	31000:2018	d) las relaciones contractuales y los compromisos;
NO LO TIENE	Quinta Viñeta	31000	31000:2018	e) la complejidad de las redess y dependencias.
NO LO TIENE	Tercer Parráfo	31000	31000:2018	El análisis del contexto interno de la organización puede incluir, pero no limitarse a:
NO LO TIENE	Sexta Viñeta	31000	31000:2018	f) la visión, la misión y los valores;
NO LO TIENE	Séptima Viñeta	31000	31000:2018	g) la gobernanza, la estrucura de la organización, los roles y la rendición de cuentas;
NO LO TIENE	Octava Viñeta	31000	31000:2018	h) la estrategia, los objetivos y las políticas;
NO LO TIENE	Novena Viñeta	31000	31000:2018	i) la cultura de la organización;
NO LO TIENE	Décima Viñeta	31000	31000:2018	j) las normas, las directrices y los modelos adoptados pr la organización;
NO LO TIENE	Décima Primer Viñeta	31000	31000:2018	k) las capacidades, entendidas en términos de recursos y conocimiento (por ejemplo, capital, tiempo, personas, propiedad intelectual, procesos, sistemas y tecnologías);
NO LO TIENE	Décima Segunda Viñeta	31000	31000:2018	l) los datos, los sistemas de información y los flujos de información;
NO LO TIENE	Décima Tercer Viñeta	31000	31000:2018	m) las relaciones con partes interesadas internas, teniendo en cuenta sus percepciones y valores;

NO LO TIENE	Décima Cuarta Viñeta	31000	31000:2018	n) las relaciones contractuales y los compromisos;
NO LO TIENE	Décima Quinta Viñeta	31000	31000:2018	o) las interdependencias e interconexiones.
4.2 COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS (Primer Parráfo)	NO LO TIENE	27001	27001:2013	**4.2 COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS** La organización debe determinar:
a)	NO LO TIENE	27001 Incluyendo S.I.G.	27001:2013	a) las partes interesadas que son pertinentes al S.G.I.; y
b)	NO LO TIENE	27001 Incluyendo Riesgo	27001:2013	b) los requisitos de estas partes interesadas pertinentes a seguridad de la información y gestión del riesgo.
NOTA	NO LO TIENE	27001	27001:2013	NOTA Los requisitos de las partes interesadas pueden incluir los requisitos legales y reglamentarios, y las obligaciones contractuales.
4.3 DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (Primer Parráfo)	**6.3.2 DEFINICIÓN DEL ALCANCE**	27001 Incluyendo S.I.G.	27001:2013	**4.3 DETERMINACIÓN DEL ALCANCE DEL S.I.G.** La organización debe determinar los límites y la aplicabilidad del S.G.I. para establecer su alcance.
NO LO TIENE	Segundo Parráfo	31000	31000:2018	Como el proceso de la gestión del riesgo puede aplicarse a niveles distintos (por ejemplo: estratégico, operacional, de programa, de proyecto u otras actividades), es importante tener claro el alcance considerado, los objetivos pertinentes a considerar y su alineamiento con los objetivos de la organización.
Segundo Parráfo	NO LO TIENE	27001	27001:2013	Cuando se determina este alcance, la organización debe considerar:
a)	NO LO TIENE	27001	27001:2013	a) las cuestiones externas e internas referidas en el numeral 4.1, y
b)	NO LO TIENE	27001	27001:2013	b) los requisitos referidos en el numeral 4.2;
c)	NO LO TIENE	27001	27001:2013	c) las interfaces y dependencias entre las actividades realizadas por la organización, y las que realizan otras organizaciones;
NO LO TIENE	Primera Viñeta	31000	31000:2018	d) los objetivos y las decisiones que se necesitan tomar;
NO LO TIENE	Segunda Viñeta	31000	31000:2018	e) los resultados esperados de las etapas a ejecutar en el proceso;
NO LO TIENE	Tercera Viñeta	31000	31000:2018	f) el tiempo, la ubicación, las inclusiones y las exclusiones especificas;
NO LO TIENE	Cuarta Viñeta	31000	31000:2018	g) las herramientas y las técnicas apropiadas de evaluación del riesgo;
NO LO TIENE	Quinta Viñeta	31000	31000:2018	h) los recursos requeridos, responsabilidades y registros a conservar;
NO LO TIENE	Sexta Viñeta	31000	31000:2018	i) las relaciones con otros proyectos, procesos y actividades.
Tercer Parráfo	NO LO TIENE	31000	31000:2018	El alcance debe estar disponible como información documentada.
4.4 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (Primer Parráfo)	NO LO TIENE	27001 Incluyendo S.I.G.	27001:2013	**4.4 SISTEMA INTEGRADO DE GESTIÓN** La organización debe establecer, implementar, mantener y mejorar continuamente un S.I.G., de acuerdo con los requisitos de esta Norma integral.
NO LO TIENE	**5.3 INTEGRACIÓN** (Primer Parráfo)	31000 Incluyendo Seguridad de la información	31000:2018	**4.4.1 Integración** La integración de la gestión del riesgo y la seguridad de la información, depede de la compresión de las estructuras y el contexto de la organización. Las estructuras difieren dependiendo del próposito, las metas y la complejidad de la organización. El riesgo se gestiona en cada parte de la estrucura de la organización. Todos los miembros de una organización tienen la responsabilidad de gestionar el riesgo y la seguridad de la información.
NO LO TIENE	Segundo Parráfo	31000 Incluyendo Seguridad de la información	31000:2018	La gobernanza guía el curso de la organización, sus relaciones externas e internas y las reglas, los procesos y las prácticas necesarios para alcanzar su propósito. Las estructuras de gestión convierten la orientación de la gobernanza en la estrategia y los objetivos asociados requeridos para lograr los niveles deseados de desempeño sostenible y de viabilidad en el largo plazo. La determinación de los roles para la rendición de cuentas y la supervisión de la gestión del riesgo y la seguridad de la información, dentro de la organización son partes integrales de la gobernanza de la organización.
NO LO TIENE	Tercer Parráfo	31000 Incluyendo Seguridad de la información	31000:2018	La integración de la gestión del riesgo y la seguridad de la información, en la organización es un proceso dinámico e iterativo, y se debería adaptar a las necesidades y a la cultura de la organización. La gestión del riesgo y la seguridad de la información, debería ser una parte de, y no estar separada del propósito, la gobernanza, el liderazgo y compromiso, la estrategia, los objetivos y las operaciones de la organización.
5. LIDERAZGO	NO LO TIENE	27001	27001:2013	**5. LIDERAZGO**
5.1 LIDERAZGO Y COMPROMISO (Primer Parráfo)	**5.2 LIDERAZGO Y COMPROMISO** (Primer Parráfo)	31000 + 27001	31000:2018	**5.2 LIDERAZGO Y COMPROMISO** La alta dirección y los órganos de supervisión, cuando sea aplicable, deberían asegurar que la gestión del riesgo y la seguridad de la información, estén integradas en todas las actividades de la organización y debe demostrar liderazgo y compromiso con respecto al S.I.G.:

a)	Segunda Viñeta Quinta Viñeta	27001 Incluyendo Gestión del riesgo	27001:2013	a) asegurando que se establezcan la política de la seguridad de la información y la gestión del riesgo que establezca un enfoque, un plan o una línea de acción y los objetivos de la seguridad de la información y la gestión del riesgo, y que estos sean compatibles con la dirección estratégica de la organización;
b)	NO LO TIENE	27001 Incluyendo S.I.G.	27001:2013	b) asegurando la integración de los requisitos del S.I.G. en los procesos de la organización;
c)	Tercera Viñeta	27001 Incluyendo S.I.G.	27001:2013	c) asegurando que los recursos necesarios para el S.I.G. estén disponibles;
d)	Octava Viñeta	27001 Incluyendo S.I.G. y Gestión del riesgo	27001:2013	d) comunicando la importancia y el valor de una gestión de la seguridad de la información y gestión del riesgo, eficaz y de la conformidad con los requisitos del S.I.G., a la organización y sus partes interesadas;
e)	NO LO TIENE	27001 Incluyendo S.I.G.	27001:2013	e) asegurando que el S.I.G. logre los resultados previstos;
NO LO TIENE	Cuarta Viñeta	31000	31000:2018	f) asignando autoridad, responsabilidad y obligación de rendir cuentas en los niveles apropiados dentro de la organización;
f)	NO LO TIENE	27001 Incluyendo S.I.G.	27001:2013	g) dirigiendo y apoyando a las personas, para contribuir a la eficacia del S.I.G.;
g)	Novena Viñeta	27001	27001:2013	h) promoviendo el seguimiento sistemáico y la mejora continua, y
h)	NO LO TIENE	27001	27001:2013	i) apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidad.
NO LO TIENE	Segundo Parráfo	31000	31000:2018	Esto ayudará a la organización a:
NO LO TIENE	Sexta Viñeta	31000	31000:2018	j) reconocer y aordar todas las obligaciones, así como sus compromisos voluntarios;
NO LO TIENE	Séptima Viñeta	31000	31000:2018	k) establecer la magnitud y el tipo de riesgo que puede o no ser tomado para guiar el desarrollo de los criterios del riesgo, asegurando que se comunican a la organización y a sus partes interesadas.
NO LO TIENE	Tercer Parráfo	31000 Incluyendo Seguridad de la información	31000:2018	La alta dirección rinde cuentas por gestionar el riesgo mientras que los órganos de supervisión rinden cuentas por la supervisión de la gestión del riesgo y la seguridad de la información. Frecuentemente se espera o se requiere que los grupos de supervisión:
NO LO TIENE	Décima Primer Viñeta	31000	31000:2018	l) se aseguren de que los riesgos se consideran apropiadamente cuando se establezcan los objetivos de la organización;
NO LO TIENE	Décima Segunda Viñeta	31000	31000:2018	m) comprendan los riesgos a los que hace frente la organización en la busqueda de sus objetivos;
NO LO TIENE	Décima Tercer Viñeta	31000	31000:2018	n) se aseguren de que los sistemas para gestionar estos riesgos se implementen y operen eficazmente;
NO LO TIENE	Décima Cuarta Viñeta	31000	31000:2018	o) se aseguren de que estos riesgos sean apropiados en el contexto de los objetivos de la organización;
NO LO TIENE	Décima Quinta Viñeta	31000	31000:2018	p) se aseguren de que la información sobre estos riesgos y su gestión se comunique de la manera apropiada.
5.2 POLÍTICA (Primer Parráfo)	NO LO TIENE	27001 Incluyendo Gestión del riesgo	27001:2013	**5.2 POLÍTICA** La alta dirección debe establecer una política de la seguridad de la información y la gestión del riesgo que:
a)	NO LO TIENE	27001	27001:2013	a) sea adecuada al propósito de la organización;
b)	NO LO TIENE	27001 Incluyendo Gestión del riesgo	27001:2013	b) incluya objetivos de seguridad de la información y la gestión del riesgo (véase el numeral 6.2) o proporcione el marco de referencia para el establecimiento de los objetivos de la seguridad de la información y la gestión del riesgo;
c)	NO LO TIENE	27001 Incluyendo Gestión del riesgo	27001:2013	c) incluya el compromiso de cumplir los requisitos aplicables relacionados con la seguridad de la información y la gestión del riesgo; y
d)	NO LO TIENE	27001 Incluyendo S.I.G	27001:2013	d) incluya el compromiso de mejora continua del S.I.G.
Segundo Parráfo	NO LO TIENE	27001 Incluyendo Gestión del riesgo	27001:2013	La política de la seguridad de la información y la gestión del riesgo debe:
e)	NO LO TIENE	27001	27001:2013	e) estar disponible como información documentada;
f)	NO LO TIENE	27001	27001:2013	f) comunicarse dentro de la organización; y
g)	NO LO TIENE	27001	27001:2013	g) estar disponible para las partes interesadas, según sea apropiado.
5.3 ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN (Primer Parráfo)	**5.4.3 ASIGNACIÓN DE ROLES, AUTORIDADES, RESPONSABILIDADES Y OBLIGACIÓN DE RENDIR CUENTAS EN LA ORGANIZACIÓN** (Primer Parráfo)	27001 + 31000	27001:2013	**5.3 ASIGNACIÓN DE ROLES, AUTORIDADES, RESPONSABILIDADES Y OBLIGACIÓN DE RENDIR CUENTAS EN LA ORGANIZACIÓN** La alta dirección y los órganos de supervisión, cuando sea aplicable, debe asegurarse de que las responsabilidades, autoridades y la obligación de rendir cuentas para los roles pertinentes a la seguridad de la información se asignen y comuniquen a todos los niveles de la organización.
Segundo Parráfo	NO LO TIENE	27001	27001:2013	La alta dirección debe asignar la responsabilidad y autoridad para:

a)	NO LO TIENE	27001 Incluyendo Integral	27001:2013	a) asegurarse de que el sistema de gestión de la seguridad de la información sea conforme con los requisitos de esta Norma Integral;
b)	NO LO TIENE	27001	27001:2013	b) informar a la alta dirección sobre el desempeño del S.I.G.
NO LO TIENE	Primera Viñeta	31000	31000:2018	c) enfatizar que lgestión del riesgo es una responsabilidad principal;
NO LO TIENE	Segunda Viñeta	31000	31000:2018	d) identificar a las personas que tienen asignada la obligación de rendir cuentas y la autoridad para gestionar el riesgo (dueños del riesgo).
NOTA	NO LO TIENE	27001	27001:2013	NOTA La alta dirección también puede asignar responsabilidades y autoridades para informar sobre el desempeño del S.I.G. dentro de la organización.
NO LO TIENE	**5.4.2 ARTICULACÓN DEL COMPROMISO CON LA GESTIÓN DEL RIESGO** (Primer Parráfo)	31000	31000:2018	**5.4 ARTICULACÓN DEL COMPROMISO CON LA GESTIÓN DEL RIESGO** La alta dirección y los organismos de supervisión, cuando sea aplicable, deberían articular y demostrar su compromiso continuo con la gestión del riesgo y la seguridad de la información mediante una política, una declaración u otras formas que expresen claramente los objetivos y el compromiso de la organización con la gestión del riesgo y la seguridad de la información. El compromiso debería incluir, pero no limitarse a:
NO LO TIENE	Primera Viñeta	31000	31000:2018	a) el propósito de la organización para gestionar el riesgo y la seguridad de la información, y los vínculos con sus objetivos y otras polícas;
NO LO TIENE	Segunda Viñeta	31000	31000:2018	b) el refuerzo de la necesidad de integrar la gestión del riesgo y la seguridad de la información en toda la cultura de la organización;
NO LO TIENE	Tercera Viñeta	31000	31000:2018	c) el liderazgo en la integración de la gestión del riesgo y la seguridad de la información en las actividades principales del negocio y la toma de decisiones;
NO LO TIENE	Cuarta Viñeta	31000	31000:2018	d) las autoridades, las responsbilidades y la obligación de rendir cuentas;
NO LO TIENE	Quinta Viñeta	31000	31000:2018	e) la disponibilidad de los recursos necesarios;
NO LO TIENE	Sexta Viñeta	31000	31000:2018	f) la manera de maejar los objetivos en conflicto;
NO LO TIENE	Séptima Viñeta	31000	31000:2018	g) la medición e informe como parte de los indicadores de desempeño de la organización;
NO LO TIENE	Octava Viñeta	31000	31000:2018	h) la revisión y la mejora.
NO LO TIENE	Último Parráfo	31000	31000:2018	El compromiso con la gestión del riesgo y la seguridad de la información se debería comunicar dentro de la organización y a las partes interesadas, de manera apropiada.
6. PLANIFICACIÓN	NO LO TIENE	27001	27001:2013	**6. PLANIFICACIÓN**
6.1 ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES	NO LO TIENE	27001	27001:2013	**6.1 ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES**
6.1.1 Generalidades (Primer Parráfo)	**6.1 Generalidades** (Primer Parráfo)	27001 Incluyendo S.I.G.	27001:2013	**6.1.1 Generalidades** Al planificar el S.I.G., la organización debe considerar las cuestiones referidas en el numeral 4.1 y los requisitos a que se hace referencia en el numeral 4.2, y determinar los riesgos y oportunidades que es necesario tratar. El proceso de la gestión del riesgo implica la aplicación sistemática de políticas, procedimientos y prácticas a las actividades de comunicación y consulta, establecimiento del contexto y evaluación, tratamiento, seguimiento, revisión, registro e informe dle riesgo, con el fin de:
a)	NO LO TIENE	27001 Incluyendo S.I.G.	27001:2013	a) asegurarse de que el S.I.G. pueda lograr sus resultados previstos;
b)	NO LO TIENE	27001	27001:2013	b) prevenir o reducir efectos indeseados; y
c)	NO LO TIENE	27001	27001:2013	c) lograr la mejora continua.
Segundo Parráfo	NO LO TIENE	27001	27001:2013	La organización debe planificar:
d)	NO LO TIENE	27001	27001:2013	d) las acciones para tratar estos riesgos y oportunidades; y
e)	NO LO TIENE	27001	27001:2013	e) la manera de:
1)	NO LO TIENE	27001 Incluyendo S.I.G.	27001:2013	1) integrar e implementar estas acciones en sus procesos del S.I.G.,
2)	NO LO TIENE	27001	27001:2013	2) evaluar la eficacia de estas acciones.

NO LO TIENE	**6.3.4 Definición de los criterios del riesgo** (Primer Parráfo)	31000	31000:2018	**6.1.2 Definición de los criterios del riesgo** La organización debería precisar la cantidad y el tipo de riesgo que puede o no puede tomar, con relación a los objetivos. También debería definir los criterios para valorar la importancia del riesgo y para apoyar los procesos de toma de decisiones. Los criterios del riesgo se deberían alinear con el marco de referencia de la gestión del riesgo y seguridad de la información, y adaptar al propósito y al alcance específicos de la actividad considerada. Los criterios del riesgo deberían reflejar los valores, objetivos y recursos de la organización y ser coherentes con las políticas y declaraciones acerca de la gestión del riesgo y seguridad de la información. Los criterios se deberían definir teniendo en consideración las obligaciones de la organización y los puntos de vista de sus partes interesadas.
NO LO TIENE	Segundo Parráfo	31000	31000:2018	Aunque los criterios del riesgo se deberían establecer al principio del proceso de la evaluación del riesgo, éstos son dinámicos, y deberían revisarse continuamente y si fuese necesario, modificarse.
NO LO TIENE	Tercer Parráfo	31000	31000:2018	Para establecer los criterios del riesgo, se debería considerar lo siguiente:
NO LO TIENE	Primera Viñeta	31000	31000:2018	a) la naturaleza y los tipos de las incertidumbres que pueden afectar a los resultados y objetivos (tanto tangibles como intangibles);
NO LO TIENE	Segunda Viñeta	31000	31000:2018	b) cómo se van a definir y medir las consecuencias (tanto positivas como negativas) y la probabilidad;
NO LO TIENE	Tercera Viñeta	31000	31000:2018	c) los factores relacionados con el tiempo;
NO LO TIENE	Cuarta Viñeta	31000	31000:2018	d) la coherencia en el uso de las mediciones;
NO LO TIENE	Quinta Viñeta	31000	31000:2018	e) cómo se va a determinar el nivel de riesgo;
NO LO TIENE	Sexta Viñeta	31000	31000:2018	f) cómo se tendran en cuenta las combinaciones y las secuencias de múltiples riesgos;
NO LO TIENE	Séptima Viñeta	31000	31000:2018	h) la capacidad de la organización.
6.1.2 VALORACION DE RIESGOS DE LA SEGURIDAD DE LA INFORMACION	**6.4 EVALUACIÓN DEL RIESGO**	31000	31000:2018	**6.1.3 Evaluación del riesgo**
NO LO TIENE	**6.4.1. Generalidades** (Primer Parráfo)	31000	31000:2018	**6.1.3.1 Generalidades** La evaluación del riesgo es el proceso global de identificación del riesgo, análisis del riesgo y valoración del riesgo.
NO LO TIENE	Segundo Parráfo	31000	31000:2018	La evaluación del riesgo se debería llevar a cabo de manera sistemática, iterativa y colaborativa, basándose en el conocimiento y los puntos de vista de las partes interesadas. Se debería utilizar la mejor información disponible, complementada por investigación adicional, si fuese necesario.
Primer Parráfo	NO LO TIENE	27001	27001:2013	La organización debe definir y aplicar un proceso de valoración de riesgos de la seguridad de la información que:
a)	NO LO TIENE	27001	27001:2013	a) establezca y mantenga criterios de riesgo de la seguridad de la información que incluyan:
1)	NO LO TIENE	27001	27001:2013	1) Los criterios de aceptación de riesgos; y
2)	NO LO TIENE	27001	27001:2013	2) los criterios para realizar valoraciones de riesgos de la seguridad de la información;
b)	NO LO TIENE	27001	27001:2013	b) asegure que las valoraciones repetidas de riesgos de la seguridad de la información produzcan resultados consistentes, válidos y comparables;
e)	**6.4.2 Identificación del riesgo** (Primer Parráfo)	31000	31000:2018	6.1.3.2 **Identificación del riesgo** El propósito de la identificación del riesgo es encontrar, reconocer y describir los riesgos que pueden ayudar o impedir a una organización lograr sus objetivos. Para la identificación de los riesgos es importante contar con información pertinente, apropiada y actualizada.
NO LO TIENE	Segundo Parráfo	31000 + 27001 Incluyendo S.I.G.	31000:2018	La organización puede utilizar un rango de técnicas para identificar incertidumbres que pueden afectar a uno o varios objetivos. Se deberían considerar los factores siguientes y la relación entre estos factores:
e) 1)	NO LO TIENE	27001	27001:2013	a) los riesgos asociados con la perdida de la confidencialidad de integridad y de disponibilidad de información dentro del alcance del S.I.G.
NO LO TIENE	Primera Viñeta	31000	31000:2018	b) las fuentes de riesgo tangibles e intangibles;
NO LO TIENE	Segunda Viñeta	31000	31000:2018	c) las causas y los eventos;
NO LO TIENE	Tercera Viñeta	31000	31000:2018	d) las amenazas y las oportunidades;
NO LO TIENE	Cuarta Viñeta	31000	31000:2018	e) las vulnerabilidades y las capacidades;
NO LO TIENE	Quinta Viñeta	31000	31000:2018	f) los cambios en los contextos externo e interno;
NO LO TIENE	Sexta Viñeta	31000	31000:2018	g) los indicadoresde riesgo emergentes;
NO LO TIENE	Séptima Viñeta	31000	31000:2018	h) la naturaleza y el valor de los activos y recursos;
NO LO TIENE	Octava Viñeta	31000	31000:2018	i) las consecuencias y sus impactos en los objetivos;
NO LO TIENE	Novena Viñeta	31000	31000:2018	j) las limitaciones de conocimiento y la confiabilidad de la información;
NO LO TIENE	Décima Viñeta	31000	31000:2018	k) los factores relacionados con el tiempo;
e) 2)	NO LO TIENE	27001	27001:2013	l) identificar a los dueños de los riesgos;
NO LO TIENE	Décima Primer Viñeta	31000	31000:2018	m) los sesgos, los supuestos y las creencias de las personas involucradas.

NO LO TIENE	Último Parráfo	31000	31000:2018	La organización debería identificar los riesgos, tanto si sus fuentes están o no bajo su control. Se debería considerar que puede haber más de un tipo de resultado, que puede dar lugar a una variedad de consecuencias tangibles o intangibles.
NO LO TIENE	**6.4.3 Análisis del riesgo** (Primer Parráfo)	31000	31000:2018	**6.1.3.3 Análisis del riesgo** El propósito del análisis del riesgo es comprender la naturaleza del riesgo y sus características incluyendo, cuando sea apropiado, el nivel del riesgo. El análisis del riesgo implica una consideración detallada de incertidumbres, fuentes de riesgo, consecuencias, probabilidades, eventos, escenarios, controles y su eficacia. Un evento puede tener múltiples causas y consecuencias y puede afectar a múltiples objetivos.
NO LO TIENE	Segundo Parráfo	31000	31000:2018	El análisis del riesgo se puede realizar con diferentes grados de detalle y complejidad, depediendo del propósito del análisis, la disponibilidad y la confiabilidad de la información y los recursos disponibles. Las técnicas de análisis pueden ser cualitativas, cuantitativas o una combinación de éstas, dependiendo de las circunstancias y del uso previsto.
NO LO TIENE	Tercer Parráfo	31000	31000:2018	El análisis del riesgo debería considerar factores tales como:
NO LO TIENE	Primera Viñeta	31000	31000:2018	a) la probabilidad de los eventos y de las consecuencias;
NO LO TIENE	Segunda Viñeta	31000	31000:2018	b) la naturalza y la magnitud de las consecuencias;
NO LO TIENE	Tercera Viñeta	31000	31000:2018	c) la complejidad y la interconexión;
NO LO TIENE	Cuarta Viñeta	31000	31000:2018	d) los factores relacionados con el tiempo y la volatilidad;
NO LO TIENE	Quinta Viñeta	31000	31000:2018	e) la eficacia de los controles existentes;
NO LO TIENE	Sexta Viñeta	31000	31000:2018	f) los niveles de sensibilidad y de confianza;
d) 1)	NO LO TIENE	27001	27001:2013	g) valorar las consecuencias potenciales que resultaran si se materializan los riesgos identificados en 6.1.3.2 a);
d) 2)	NO LO TIENE	27001	27001:2013	h) valorar la probabilidad realista de que ocurran los riesgos identificados en 6.1.3.2 a); y
d) 3)	NO LO TIENE	27001	27001:2013	i) determinar los niveles de riesgo.
NO LO TIENE	Cuarto Parráfo	31000	31000:2018	El análisis del riesgo puede estar influenciado por cualquier divergencia de opiniones, sesgos, percepciones del riesgo y juicios. Las influencias adicionales son la calidad de la información utilizada, los supuestos y las exclusiones establecidos, cualquier limitación de las técnicas y cómo se ejecutan éstas. Estas influencias se deberían considerar, documentar y comunicar a las personas que toman decisiones.
NO LO TIENE	Quinto Parráfo	31000	31000:2018	Los eventos de alta incertidumbre pueden ser difíciles de cuantificar. Esto puede ser una cuestión importante cuando se analizan eventos con consecuencias severas. En tales casos, el uso de una combinación de técnicas generalmente proporciona una visión más amplia.
NO LO TIENE	Sexto Parráfo	31000	31000:2018	El análisis del riesgo proporciona una entrada para la valoración del riesgo, para las decisiones sobre la manera de tratar los riesgos y si es necesario hacerlo y sobre la estrategia y los métodos más apropiados de tratamiento del riesgo. Los resultados proporcionan un entendimiento profundo para tomar decisiones, cuando se está eligiendo entre distintas alternativas, y las opciones implican diferentes tpos y niveles de riesgo.
e) 1)	**6.4.4 Valoración del riesgo** (Primer Parráfo)	31000+ 27001	31000:2018	**6.1.3.4 Valoración del riesgo** El propósito de la valoración del riesgo es apoyar a la toma de decisiones. La valoración del riesgo implica comparar los resultados del análisis de riesgos con los criterios del riesgo establecidos en 6.1.3.1 a), para determinar cuándo se requiere una acción adicional. Esto puede conducir a una decisión de:
NO LO TIENE	Primera Viñeta	31000	31000:2018	a) no hacer nada más;
NO LO TIENE	Segunda Viñeta	31000	31000:2018	b) considerar opciones para el tratamiento del riesgo;
NO LO TIENE	Tercera Viñeta	31000	31000:2018	c) realizar un análisis adicional para comprender mejor el riesgo;
NO LO TIENE	Cuarta Viñeta	31000	31000:2018	d) mantener los controles existentes;
NO LO TIENE	Quinta Viñeta	31000	31000:2018	e) reconsiderar los objetivos.
e) 2)	NO LO TIENE	27001	27001:2013	f) priorizar los riesgos analizados para el tratamiento de los riesgos.
NO LO TIENE	Segundo Parráfo	31000	31000:2018	Las decisiones deberían tener en cuenta un contexto más amplio y las consecuencias reales y percibidas por las partes interesadas externas e internas.
NO LO TIENE	Tercer Parráfo	31000	31000:2018	Los resultados de la valoración del riesgo se deberían registrar, comunicar y luego validar a los niveles apropiados de la organización.
Último Parráfo	NO LO TIENE	27001 Incluyendo S.I.G.	27001:2013	La organización debe conservar información documentada acerca del proceso de valoración de riesgos del S.I.G.
6.1.3 TRATAMIENTO DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN	**6.5 Tratamiento del riesgo**	31000	31000:2018	**6.1.4 Tratamiento del riesgo**

Primer Parráfo	**6.5.1. Generalidades** (Primer Parráfo)	31000 + 27001	31000:2018	**6.1.4.1 Generalidades** La organización debe definir y aplicar un proceso de tratamiento de riesgos. El propósito del tratamiento del riesgo es seleccionar e implementar opciones para abordar el riesgo.
NO LO TIENE	NO LO TIENE	31000	31000:2018	El tratamiento del riesgo implica un proceso iterativo de:
a)	Primera Viñeta	31000 + 27001	31000:2018	a) formular y seleccionar opciones apropiadas para el tratamiento del riesgo teniendo en cuenta los resultados de la valoración de riesgos;
b)	NO LO TIENE	27001 Incluyendo S.I.G.	27001:2013	b) determinar todos los controles que sean necesarios para implementar las opciones escogidas para el tratamiento de riesgos del S.I.G.;
NOTA	NO LO TIENE	27001	27001:2013	NOTA Las organizaciones pueden diseñar los controles necesarios, o identificarlos de cualquier fuente.
c)	NO LO TIENE	27001	27001:2013	c) comparar los controles determinados en 6.1.4.1 b) con los del Anexo A y verificar que no se han omitidos controles necesarios;
NOTA 1	NO LO TIENE	27001	27001:2013	NOTA 1 El Anexo A contiene una lista amplia de objetivos de control y controles. Se invita a los usuarios de esta Norma a consultar el Anexo A, para asegurar que no se pasen por alto los controles necesarios.
NOTA 2	NO LO TIENE	27001	27001:2013	NOTA 2 Los objetivos de control están incluidos implícitamente en los controles escogidos. Los objetivos de control y los controles enumerados en el Anexo A no son exhaustivos, y pueden ser necesarios objetivos de control y controles adicionales.
d)	NO LO TIENE	27001	ISO/IEC 27001:2013/Cor.2:2015	d) producir una declaración de aplicabilidad que contenga
Primera Viñeta	NO LO TIENE	27001	ISO/IEC 27001:2013/Cor.2:2015	1) los controles necesarios (véanse el numeral 6.1.4.1 b) y c));
Segunda Viñeta	NO LO TIENE	27001	ISO/IEC 27001:2013/Cor.2:2015	2) la justificación de las inclusiones;
Tercera Viñeta	NO LO TIENE	27001	ISO/IEC 27001:2013/Cor.2:2015	3) si los controles necesarios están implementados o no; y
Cuarta Viñeta	NO LO TIENE	27001	ISO/IEC 27001:2013/Cor.2:2015	4) la justificación para las exclusiones de los controles del Anexo A;
e)	Segunda Viñeta	31000 + 27001 Incluyendo S.I.G.	31000:2018	e) planificar e implementar un plan de tratamiento de riesgos del S.I.G.;
NO LO TIENE	Tercera Viñeta	31000	31000:2018	f) evaluar la eficacia de ese tratamiento;
NO LO TIENE	Cuarta Viñeta	31000	31000:2018	g) decidir si el riesgo residual es aceptables;
NO LO TIENE	Quinta Viñeta	31000	31000:2018	h) si no es aceptable, efectuar tratamiento adicional.
NO LO TIENE	**6.5.2 Selección de las opciones para el tratamiento del riesgo** (Primer Parráfo)	31000	31000:2018	**6.1.4.2 Selección de las opciones para el tratamiento del riesgo** La selección de las opciones más apropiadas para el tratamiento del riesgo implica hacer un balance entre los beneficios potenciales, derivados del logro de los objetivos contra costos, esfuerzo o desventajas de la implementación.
NO LO TIENE	Segundo Parráfo	31000	31000:2018	Las opciones de tratamiento del riesgo no necesariamente son mutuamente excluyentes o apropiadas en todas las circunstancias. Las opciones para tratar el riesgo pueden implicar una o más de las siguientes:
NO LO TIENE	Primera Viñeta	31000	31000:2018	a) evitar el riesgo decidiendo no iniciar o continuar con la actividad que genera el riesgo;
NO LO TIENE	Segunda Viñeta	31000	31000:2018	b) aceptar o aumentar el riesgo en busca de una oportunidad;
NO LO TIENE	Tercera Viñeta	31000	31000:2018	c) eliminar la fuente de riesgo;
NO LO TIENE	Cuarta Viñeta	31000	31000:2018	d) modificar la probabilidad;
NO LO TIENE	Quinta Viñeta	31000	31000:2018	e) modificar las consecuencias;
NO LO TIENE	Sexta Viñeta	31000	31000:2018	f) compartir el riesgo (por ejemplo: a través de contratos, compra de seguros);
NO LO TIENE	Séptima Viñeta	31000	31000:2018	g) retener el riesgo con base en una decisión informada.
NO LO TIENE	Tercer Parráfo	31000	31000:2018	La justificación para el tratamiento del riesgo es más amplia que las simples consideraciones económicas y debería tener en cuenta todas las obligaciones de la organización, los compromisos voluntarios y los puntos de vista de las partes interesadas. La selección de las opciones para el tratamiento del riesgo debería realizarse de acuerdo con los objetivos de la organización, los criterios del riesgo y los recursos disponibles.

NO LO TIENE	Cuarto Parráfo	31000	31000:2018	Al seleccionar opciones para el tratamiento del riesgo, la organización debería considerar los valores, las percepciones, el involucrar potencialmente a las partes interesadas y los medios más apropiados para comunicarse con ellas y consultarlas. A igual eficacia, algunas partes interesadas pueden aceptar mejor que otras los diferentes tratamientos del riesgo.
NO LO TIENE	Quinto Parráfo	31000	31000:2018	Los tratamientos del riesgo, a pesar de un cuidadoso diseño e implementación, pueden no producir los resultados esperados y puede producir consecuencias no previstas. El seuimiento y la revisión nececsitan ser parte integral de la implementación del tratamiento del riesgo para segurar que las distintas maneras del tratamiento sean y permanezcan eficaces.
NO LO TIENE	Sexto Parráfo	31000	31000:2018	El tratamiento del riesgo a su vez puede introducir nuevos riesgos que necesiten gestionarse.
NO LO TIENE	Séptimo Parráfo	31000	31000:2018	Si no hay opciones disponibles para el tratamiento o si las opciones para el tratamiento no modifican suficientemente el riesgo, éste se debería registrar y mantener en continua revisión.
NO LO TIENE	Último Parráfo	31000	31000:2018	Las personas que toman decisiones y otras partes interesadas deberían ser conscientes de la naturaleza y el nivel del riesgo residual después del tratamiento del riesgo. El riesgo residual se debería documentar y ser objeto de seguimiento, revisión y, cuando sea apropiado, de tratamiento adicional.
NO LO TIENE	**6.5.3 Preparación e implementación de los planes de tratamiento del riesgo** (Primer Parráfo)	31000	31000:2018	**6.1.4.3 Preparación e implementación de los planes de tratamiento del riesgo** El propósito de los planes de tratamiento del riesgo es especificar la manera en la que se implementarán las opciones elegidas para el tratamiento, de manera tal que os involucrados comprendan las disposiciones, y que pueda realizarse el seguimiento del avance respecto de lo planificado. El plan de tratamiento debería identificar claramente el orden en el cual el tratamiento del riesgo se debería implemetar.
NO LO TIENE	Segundo Parráfo	31000	31000:2018	Los planes de tratamiento deberían integrarse en los planes y procesos de la gestión de la organización, en consulta con las partes interesadas apropiadas.
NO LO TIENE	Tercer Parráfo	31000	31000:2018	La información proporcionada en el plan del tratamiento debería incluir:
NO LO TIENE	Primera Viñeta	31000	31000:2018	a) el fundamento de la selección de las opciones para el tratamiento, incluyendo los beneficios esperados.
NO LO TIENE	Segunda Viñeta	31000	31000:2018	b) las personas que rinden cuentas y aquellas responsables de la aprobación e implementación del plan;
NO LO TIENE	Tercera Viñeta	31000	31000:2018	c) las acciones propuestas;
NO LO TIENE	Cuarta Viñeta	31000	31000:2018	d) los recursos necesarios, incluyendo las contingencias;
NO LO TIENE	Quinta Viñeta	31000	31000:2018	e) las medidas del desempeño;
NO LO TIENE	Sexta Viñeta	31000	31000:2018	f) las restricciones;
NO LO TIENE	Séptima Viñeta	31000	31000:2018	g) los informes y seguimiento requeridos;
NO LO TIENE	Octava Viñeta	31000	31000:2018	h) los plazos previstos para la realización y la finalización de las acciones;
f)	NO LO TIENE	27001 Incluyendo S.I.G.	27001:2013	i) obtener, de parte de los dueños de los riesgos, la aprobación del plan de tratamiento de riesgos del S.I.G., y la aceptación de los riesgos residuales del S.I.G.
Último Parráfo	NO LO TIENE	27001 Incluyendo S.I.G.	27001:2013	La organización debe conservar información documentada acerca del proceso de tratamiento de riesgos del S.I.G.
6.2 OBJETIVOS DE SEGURIDAD DE LA INFORMACION Y PLANES PARA LOGRARLOS (Primer Parráfo)	NO LO TIENE	27001 Incluyendo S.I.G.	27001:2013	**6.2 OBJETIVOS DEL S.I.G. Y PLANES PARA LOGRARLOS** La organización debe establecer los objetivos del S.I.G. en las funciones y niveles pertinentes.
Segundo Parráfo	NO LO TIENE	27001 Incluyendo S.I.G.	27001:2013	Los objetivos del S.I.G. deben:
a)	NO LO TIENE	27001 Incluyendo S.I.G.	27001:2013	a) ser coherentes con la política del S.I.G.;
b)	NO LO TIENE	27001	27001:2013	b) ser medibles (si es posible);
c)	NO LO TIENE	27001 Incluyendo S.I.G.	27001:2013	c) tener en cuenta los requisitos del S.I.G. aplicables, y los resultados de la valoración y del tratamiento de los riesgos;
d)	NO LO TIENE	27001	27001:2013	d) ser comunicados; y
e)	NO LO TIENE	27001	27001:2013	e) ser actualizados, según sea apropiado.
Tercer Parráfo	NO LO TIENE	27001 Incluyendo S.I.G.	27001:2013	La organización debe conservar información documentada sobre los objetivos del S.I.G.
Cuarto Parráfo	NO LO TIENE	27001 Incluyendo S.I.G.	27001:2013	Cuando se hace la planificación para lograr sus objetivos del S.I.G., la organización debe determinar:
f)	NO LO TIENE	27001	27001:2013	f) lo que se va a hacer;
g)	NO LO TIENE	27001	27001:2013	g) que recursos se requerirán;
h)	NO LO TIENE	27001	27001:2013	h) quién será responsable;
i)	NO LO TIENE	27001	27001:2013	i) cuándo se finalizará; y
j)	NO LO TIENE	27001	27001:2013	j) cómo se evaluarán los resultados.

7. SOPORTE	NO LO TIENE	27001	27001:2013	**7. SOPORTE**
7.1 RECURSOS (Primer Parráfo)	**5.4.4 ASIGNACIÓN DE RECURSOS** (Primer Parráfo)	31000 + 27001 Incluyendo S.I.G.	31000:2018	**7.1 ASIGNACIÓN DE RECURSOS** La alta direción y los órganos de supervisión, cuando sea aplicable, debe determinar, proporcionar y asegurar la asignación de los recursos necesarios y apropiados para el establecimiento, implementación, mantenimiento y mejora continua del S.I.G., que puede incluir, pero no limitarse a:
NO LO TIENE	Primera Viñeta	31000	31000:2018	a) las personas, las habilidades, la experiencia y las competencias;
NO LO TIENE	Segunda Viñeta	31000	31000:2018	b) los procesos, los métodos y las herramientas de la organización a utilizar para gestionar el riesgo;
NO LO TIENE	Tercera Viñeta	31000	31000:2018	c) los procesos y procedimientos documentados;
NO LO TIENE	Cuarta Viñeta	31000	31000:2018	d) los sistemas de gestión de la información y del conocimiento;
NO LO TIENE	Quinta Viñeta	31000	31000:2018	e) el desarrollo profesional y las necesidades de formación.
NO LO TIENE	Último Parráfo	31000	31000:2018	La organización debería considerar las competencias y limitaciones de los recursos existentes.
7.2 COMPETENCIA (Primer Parráfo)	NO LO TIENE	27001	27001:2013	**7.2 COMPETENCIA** La organización debe:
a)	NO LO TIENE	27001 Incluyendo Gestión del riesgo	27001:2013	a) determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta su desempeño de la seguridad de la información y la gestión del riesgo, y
b)	NO LO TIENE	27001	27001:2013	b) asegurarse de que estas personas sean competentes, basándose en la educación, formación o experiencia adecuadas;
c)	NO LO TIENE	27001	27001:2013	c) cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones tomadas; y
d)	NO LO TIENE	27001	27001:2013	d) conservar la información documentada apropiada, como evidencia de la competencia.
NOTA	NO LO TIENE	27001	27001:2013	NOTA Las acciones aplicables pueden incluir, por ejemplo: la formación, la tutoría o la reasignación de las personas empleadas actualmente; o la contratación de personas competentes.
7.3 TOMA DE CONCIENCIA (Primer Parráfo)	NO LO TIENE	27001	27001:2013	**7.3 TOMA DE CONCIENCIA** Las personas que realizan el trabajo bajo el control de la organización deben tomar conciencia de:
a)	NO LO TIENE	27001 Incluyendo S.I.G.	27001:2013	a) la política del S.I.G.;
b)	NO LO TIENE	27001 Incluyendo Gestión del riesgo	27001:2013	b) su contribución a la eficacia del S.I.G., incluyendo los beneficios de una mejora del desempeño de la seguridad de la información y gestión del riesgo; y
c)	NO LO TIENE	27001 Incluyendo S.I.G.	27001:2013	c) las implicaciones de la no conformidad con los requisitos del S.I.G.
7.4 COMUNICACIÓN (Primer Parráfo)	**5.4.5 ESTABLECIMIENTO DE LA COMUNICACIÓN Y CONSULTA** (Primer Parráfo)	31000 + 27001 Incluyendo S.I.G.	31000:2018	**7.4 COMUNICACIÓN Y CONSULTA** La organización debe determinar y establecer un enfoque apropiado con relación a la necesidad de la comunicación y la consulta, internas y externas pertinentes al S.I.G. La comunicación implica compartir información con el público objetivo. La consulta además implica que los participantes proporcionen retroalimentación con la expectativa de que ésta contribuya y de forma a las decisiones u otras actividades. Los métodos y el contenido de la comunicación y la consulta deberían reflejar las expectativas de las partes interesadas, cuando sea pertinente.
NO LO TIENE	**6.2 COMUNICACIÓN Y CONSULTA** (Primer Parráfo)	31000	31000:2018	El propósito de la comunicación y la consulta es asistir a las partes interesadas pertinentes a comprender el riesgo, las bases con las que se toman decisiones y las razones por las que son necesarias acciones específicas. La comunicación busca promover la toma de conciencia y la comprensión del riesgo, mientras que la consulta implica obtener retroalimentación e información para apoyar la toma de decisiones. Una coordinación cercana entre ambas debería facilitar un intercambio de información basado en hechos, oportuno, pertinente, exacto y comprensible, teniendo en cuenta la confidencialidad e integridad de la infromación, así como el derecho a la privacidad de las personas.
NO LO TIENE	5.4.5 ESTABLECIMIENTO DE LA COMUNICACIÓN Y CONSULTA (Segundo Parráfo)	31000	31000:2018	La comunicación y la consulta deberían ser oportunas y asegurar que se recopile, consolide, sintetice y comparta la información pertinente, cuando sea apropiado, y que se proporcione retroalimentación y se lleven a cabo mejoras.
Primer Parráfo	6.2 COMUNICACIÓN Y CONSULTA (Segundo Parráfo)	31000	31000:2018	La comunicación y consulta con las partes interesadas apropiadas, externas e internas, se debería realizar en todas y cada una de las etapas del proceso de la gestión del riesgo, que incluyan:
a)	NO LO TIENE	27001	27001:2013	a) el contenido de la comunicación;
b)	NO LO TIENE	27001	27001:2013	b) cuándo comunicar;

c)	NO LO TIENE	27001	27001:2013	c) a quién comunicar;
d)	NO LO TIENE	27001	27001:2013	d) quién debe comunicar; y
e)	NO LO TIENE	27001	27001:2013	e) los procesos para llevar a cabo la comunicación.
NO LO TIENE	Tercer Parráfo	31000	31000:2018	La comunicación y consulta pretende:
NO LO TIENE	Primera Viñeta	31000	31000:2018	f) reunir diferentes áreas de experiencia para cada etapa del proceso de la gestión del riesgo;
NO LO TIENE	Segunda Viñeta	31000	31000:2018	g) asegurar que se consideren de manera apropiada los diferentes puntos de vista cuando se definen los criterios del riesgo y cuando se valoran los riesgos;
NO LO TIENE	Tercera Viñeta	31000	31000:2018	h) proporcionar suficiente información para facilitar la supervisión del riesgo y la toma de decisiones;
NO LO TIENE	Cuarta Viñeta	31000	31000:2018	i) construir un sentido de inclusión y propiedad entre las personas afectadas por el riesgo.
7.5 INFORMACIÓN DOCUMENTADA	NO LO TIENE	27001	27001:2013	**7.5 INFORMACIÓN DOCUMENTADA**
7.5.1 GENERALIDADES (Primer Parráfo)	NO LO TIENE	27001	27001:2013	**7.5.1 GENERALIDADES** El S.I.G. de la organización debe incluir:
a)	NO LO TIENE	27001	27001:2013	a) la información documentada requerida por esta Norma Integral; y
b)	NO LO TIENE	27001	27001:2013	b) la información documentada que la organización ha determinado que es necesaria para la eficacia del S.I.G.
NOTA	NO LO TIENE	27001	27001:2013	NOTA El alcance de la información documentada para un S.I.G. puede ser diferente de una organización a otra, debido a:
a)	NO LO TIENE	27001	27001:2013	a) el tamaño de la organización y a su tipo de actividades, procesos, productos y servicios,
b)	NO LO TIENE	27001	27001:2013	b) la complejidad de los procesos y sus interacciones, y
c)	NO LO TIENE	27001	27001:2013	c) la competencia de las personas.
7.5.2 CREACIÓN Y ACTUALIZACIÓN (Primer Parráfo)	NO LO TIENE	27001	27001:2013	**7.5.2 CREACIÓN Y ACTUALIZACIÓN** Cuando se crea y actualiza información documentada, la organización debe asegurarse de que lo siguiente sea apropiado:
a)	NO LO TIENE	27001	27001:2013	a) la identificación y descripción (por ejemplo, título, fecha, autor o número de referencia);
b)	NO LO TIENE	27001	27001:2013	b) el formato (por ejemplo, idioma, versión del software, gráficos) y sus medios de soporte (por ejemplo, papel, electrónico);
c)	NO LO TIENE	27001	27001:2013	c) la revisión y aprobación con respecto a la idoneidad y adecuación.
NO LO TIENE	**6.7 REGISTRO E INFORME** (Primer Parráfo)	31000 Incluyendo Seguridad de la información	31000:2018	**7.5.3 REGISTRO E INFORME** El proceso de la gestión del riesgo y seguridad de la información, y sus resultados se deberían documentar e informar a través de los mecanismos apropiados. El registro e informe pretenden:
NO LO TIENE	Primera Viñeta	31000 Incluyendo Seguridad de la información	31000:2018	a) comunicar las actividades de la gestión del riesgo y seguridad de la información, y sus resultados a lo largo de la organización;
NO LO TIENE	Segunda Viñeta	31000	31000:2018	b) proporcionar información para la toma de decisiones;
NO LO TIENE	Tercera Viñeta	31000 Incluyendo Seguridad de la información	31000:2018	c) mejorar las actividades de la gestión del riesgo y seguridad de la información;
NO LO TIENE	Cuarta Viñeta	31000 Incluyendo Seguridad de la información	31000:2018	d) asistir la interacción con las partes interesadas, incluyendo a las personas que tienen la responsabilidad y la obligación de rendir cuentas de las actividades de la gestión del riesgo y seguridad de la información.
NO LO TIENE	Segundo Parráfo	31000	31000:2018	Las decisiones con respecto a la creación, conservación y tratamiento de la información documentada deberían tener en cuenta, pero no limitarse a su uso, la sensibilidad de la información y los contextos externo e interno.
NO LO TIENE	Tercer Parráfo	31000	31000:2018	El informe es una parte integral de la gobernanza de la organización y debería mejorar la calidad del diálogo con las partes interesadas, y apoyar a la alta dirección y a los órganos de supervisión a cumplir sus responsabilidades. Los factores a considerar en el infrome incluyen, pero no se limitan a:
NO LO TIENE	Quinta Viñeta	31000	31000:2018	e) las diferentes partes interesadas, sus necesidades y requisitos específicos de información;
NO LO TIENE	Sexta Viñeta	31000	31000:2018	f) el costo, la frecuencia y los tiempos del informe;
NO LO TIENE	Séptima Viñeta	31000	31000:2018	g) el método del informe;
NO LO TIENE	Octava Viñeta	31000	31000:2018	h) la pertinencia de la información con respecto a los objetivos de la organización y la toma de decisiones.
7.5.3 CONTROL DE LA INFORMACIÓN DOCUMENTADA (Primer Parráfo)	NO LO TIENE	27001 Incluyendo S.I.G.	27001:2013	**7.5.4 CONTROL DE LA INFORMACIÓN DOCUMENTADA** La información documentada requerida por el S.I.G. y por esta Norma Integral se debe controlar para asegurarse de que:
a)	NO LO TIENE	27001	27001:2013	a) esté disponible y adecuada para su uso, donde y cuando se necesite; y
b)	NO LO TIENE	27001	27001:2013	b) esté protegida adecuadamente (por ejemplo, contra pérdida de la confidencialidad, uso inadecuado, o pérdida de integridad).

Segundo Parráfo	NO LO TIENE	27001	27001:2013	Para el control de la información documentada, la organización debe tratar las siguientes actividades, según sea aplicable:
c)	NO LO TIENE	27001	27001:2013	c) distribución, acceso, recuperación y uso;
d)	NO LO TIENE	27001	27001:2013	d) almacenamiento y preservación, incluida la preservación de la legibilidad;
e)	NO LO TIENE	27001	27001:2013	e) control de cambios (por ejemplo, control de versión); y
f)	NO LO TIENE	27001	27001:2013	f) retención y disposición.
Tercer Parráfo	NO LO TIENE	27001 Incluyendo S.I.G.	27001:2013	La información documentada de origen externo, que la organización ha determinado que es necesaria para la planificación y operación del S.I.G., se debe identificar y controlar, según sea adecuado.
NOTA	NO LO TIENE	27001	27001:2013	NOTA El acceso implica una decisión concerniente al permiso solamente para consultar la información documentada, o el permiso y la autoridad para consultar y modificar la información documentada, etc.
8. OPERACIÓN	**NO LO TIENE**	27001	27001:2013	**8. OPERACIÓN**
8.1 PLANIFICACIÓN Y CONTROL OPERACIONAL (Primer Parráfo)	**5.5 IMPLEMENTACIÓN** (Primer Parráfo)	27001 + 31000	27001:2013	**8.1 PLANIFICACIÓN Y CONTROL OPERACIONAL** La organización debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos de seguridad de la información y para implementar las acciones determinadas en el numeral 6.1. La organización también debe implementar planes para lograr los objetivos de la seguridad de la información determinados en el numeral 6.2., mediante:
NO LO TIENE	Primera Viñeta	31000	31000:2018	a) el desarrollo de un plan apropiado incluyendo plazos y recursos;
NO LO TIENE	Segunda Viñeta	31000	31000:2018	b) la identificación de dónde, cuándo, cómo y quién toma diferentes tipos de decisiones en toda la organización;
NO LO TIENE	Tercera Viñeta	31000	31000:2018	c) la modificación de los procesos aplicables para la toma de decisiones, cuando sea necesario;
NO LO TIENE	Cuarta Viñeta	31000	31000:2018	d) el aseguramiento de que las disposiciones de la organización para gestionar el riesgo y la seguridad de la información, son claramente comprendidas y puestas en práctica.
NO LO TIENE	Segundo Parráfo	31000	31000:2018	La implementación con éxito del marco de referencia requiere el compromiso y la toma de conciencia de las partes interesadas. Esto permite a las organizaciones abordar explícitamente la incertifumbre en la toma de decisiones, al tiempo que se asegura que cualquier incertidumbre nueva o subsiguiente se pueda tener en cuenta cuando surja.
NO LO TIENE	Tercer Parráfo	31000	31000:2018	Si se diseña e implementa correctamente, el marco de referencia de la gestión del riesgo asegurará que el proceso de la gestión el riesgo y la seguridad de la información, sea parte de todas actividades en toda la organización, incluyendo la toma de decisiones, y que los cambios en los contextos externo e interno se captáran de manera adecuada.
Segundo Parráfo	NO LO TIENE	27001	27001:2013	La organización debe mantener información documentada en la medida necesaria para tener la confianza en que los procesos se han llevado a cabo según lo planificado.
Tercer Parráfo	NO LO TIENE	27001	27001:2013	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.
Último Parráfo	NO LO TIENE	27001	27001:2013	La organización debe asegurar que los procesos contratados externamente estén controlados.
8.2 VALORACIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN (Primer Parráfo)	NO LO TIENE	27001	27001:2013	**8.2 VALORACIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN** La organización debe llevar a cabo valoraciones de riesgos de la seguridad de la información a intervalos planificados o cuando se propongan u ocurran cambios significativos, teniendo en cuenta los criterios establecidos en el numeral 6.1.3.1.
Segundo Parráfo	NO LO TIENE	27001	27001:2013	La organización debe conservar información documentada de los resultados de las valoraciones de riesgos de la seguridad de la información.
8.3 TRATAMIENTO DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN (Primer Parráfo)	NO LO TIENE	27001	27001:2013	**8.3 TRATAMIENTO DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN** La organización debe implementar el plan de tratamiento de riesgos de la seguridad de la información.
Segundo Parráfo	NO LO TIENE	27001	27001:2013	La organización debe conservar información documentada de los resultados del tratamiento de riesgos de la seguridad de la información.
9. EVALUACIÓN DEL DESEMPEÑO	NO LO TIENE	27001	27001:2013	**9. EVALUACIÓN DEL DESEMPEÑO**
9.1 SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN (Primer Parráfo)	**6.6 SEGUIMIENTO Y REVISIÓN**	27001 + 31000 Incluyendo S.I.G.	27001:2013	**9.1 SEGUIMIENTO, REVISIÓN, MEDICIÓN, ANÁLISIS Y EVALUACIÓN** La organización debe evaluar el desempeño de la seguridad de la información y la gestión del riesgo, y la eficacia del S.I.G.

NO LO TIENE	Primer Parráfo	31000 Incluyendo Seguridad de la información.	31000:2018	El propósito del seguimiento y la revisión es asegurar y mejorar la calidad y la eficacia del diseño, la implementación y los resultados del proceso. El seguimiento continuo y la revisión periódica del proceso de la gestión del riesgo y seguridad de la información, y sus resultados debería ser una pate planificada del proceso de la gestión del riesgo y seguridad de la información, con responsabilidades claramente definidas.
NO LO TIENE	Segundo Parráfo	31000	31000:2018	El seguimiento y la revisión deberían tener un lugar en todas etapas del proceso. El seguimiento y la revisión incluyen planificar, recopilar y analizar información, registrar resultados y proporcionar retroalimentación.
Segundo Parráfo	NO LO TIENE	27001	27001:2013	La organización debe determinar:
a)	NO LO TIENE	27001 Incluyendo Gestión del riesgo	27001:2013	a) a qué es necesario hacer seguimiento y qué es necesario medir, incluidos los procesos y controles de la seguridad de la información y la gestión del riesgo;
b)	NO LO TIENE	27001	27001:2013	b) los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos;
NOTA	NO LO TIENE	27001	27001:2013	NOTA Para ser considerados válidos, los métodos seleccionados deberían producir resultados comparables y reproducibles
c)	NO LO TIENE	27001	27001:2013	c) cuándo se deben llevar a cabo el seguimiento y la medición;
d)	NO LO TIENE	27001	27001:2013	d) quién debe llevar a cabo el seguimiento y la medición;
e)	NO LO TIENE	27001	27001:2013	e) cuándo se deben analizar y evaluar los resultados del seguimiento y de la medición; y
f)	NO LO TIENE	27001	27001:2013	f) quién debe analizar y evaluar estos resultados.
	Último Parráfo	31000	31000:2018	Los resultados del seguimiento y la revisión deberían incorporarse a todas las actividades de la gestión del desempeño, de medición y de informe de la organización.
Último Parráfo	NO LO TIENE	27001	27001:2013	La organización debe conservar información documentada apropiada como evidencia de los resultados del monitoreo y de la medición.
9.2 AUDITORÍA INTERNA (Primer Parráfo)	NO LO TIENE	27001 Incluyendo S.I.G.	27001:2013	**9.2 AUDITORÍA INTERNA** La organización debe llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si el S.I.G.:
a)	NO LO TIENE	27001	27001:2013	a) es conforme con:
1)	NO LO TIENE	27001 Incluyendo S.I.G.	27001:2013	1) los propios requisitos de la organización para su S.I.G.; y
2)	NO LO TIENE	27001 Incluyendo Integral	27001:2013	2) los requisitos de esta Norma Integral;
b)	NO LO TIENE	27001	27001:2013	b) está implementado y mantenido eficazmente.
Segundo Parráfo	NO LO TIENE			La organización debe:
c)	NO LO TIENE	27001	27001:2013	c) 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;
d)	NO LO TIENE	27001	27001:2013	d) para cada auditoría, definir los criterios y el alcance de ésta;
e)	NO LO TIENE	27001	27001:2013	e) seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría;
f)	NO LO TIENE	27001	27001:2013	f) asegurarse de que los resultados de las auditorías se informan a la dirección pertinente; y
g)	NO LO TIENE	27001	27001:2013	g) conservar información documentada como evidencia de la implementación del programa de auditoría y de los resultados de ésta.
NOTA	NO LO TIENE	27001	27001:2013	NOTA Para mayor información consultar las normas NTC-ISO 19011 y NTC-ISO 27007
9.3 REVISIÓN POR LA DIRECCIÓN (Primer Parráfo)	NO LO TIENE	27001 Incluyendo S.I.G.	27001:2013	**9.3 REVISIÓN POR LA DIRECCIÓN** La alta dirección debe revisar el S.I.G. de la organización a intervalos planificados, para asegurarse de su conveniencia, adecuación y eficacia continuas.
Segundo Parráfo	NO LO TIENE	27001	27001:2013	La revisión por la dirección debe incluir consideraciones sobre:
a)	NO LO TIENE	27001	27001:2013	a) el estado de las acciones con relación a las revisiones previas por la dirección;
b)	NO LO TIENE	27001 Incluyendo S.I.G.	27001:2013	b) los cambios en las cuestiones externas e internas que sean pertinentes al S.I.G.;
c)	NO LO TIENE	27001 Incluyendo Gestión del riesgo	27001:2013	c) retroalimentación sobre el desempeño de la seguridad de la información y gestión del riesgo, incluidas las tendencias relativas a:
1)	NO LO TIENE	27001	27001:2013	1) no conformidades y acciones correctivas;
2)	NO LO TIENE	27001	27001:2013	2) seguimiento y resultados de las mediciones;
3)	NO LO TIENE	27001	27001:2013	3) resultados de la auditoría; y
4)	NO LO TIENE	27001 Incluyendo Gestión del riesgo	27001:2013	4) cumplimiento de los objetivos de la seguridad de la información y gestión del riesgo;

d)	NO LO TIENE	27001	27001:2013	d) retroalimentación de las partes interesadas;
e)	NO LO TIENE	27001	27001:2013	e) resultados de la valoración de riesgos y estado del plan de tratamiento de riesgos; y
f)	NO LO TIENE	27001	27001:2013	f) las oportunidades de mejora continúa.
Tercer Parráfo	NO LO TIENE	27001	27001:2013	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 S.I.G.
Último Parráfo	NO LO TIENE	27001	27001:2013	La organización debe conservar información documentada como evidencia de los resultados de las revisiones por la dirección.
10. MEJORA	**5.7 MEJORA**	27001 = 31000	27001:2013	**10. MEJORA**
10.1 NO CONFORMIDADES Y ACCIONES CORRECTIVAS (Primer Parráfo)	NO LO TIENE	27001	27001:2013	**10.1 NO CONFORMIDADES Y ACCIONES CORRECTIVAS** Cuando ocurra una no conformidad, la organización debe:
a)	NO LO TIENE	27001	27001:2013	a) reaccionar ante la no conformidad, y según sea aplicable
1)	NO LO TIENE	27001	27001:2013	1) tomar acciones para controlarla y corregirla, y
2)	NO LO TIENE	27001	27001:2013	2) hacer frente a las consecuencias;
b)	NO LO TIENE	27001	27001:2013	b) 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:
1)	NO LO TIENE	27001	27001:2013	1) la revisión de la no conformidad
2)	NO LO TIENE	27001	27001:2013	2) la determinación de las causas de la no conformidad, y
3)	NO LO TIENE	27001	27001:2013	3) la determinación de si existen no conformidades similares, o que potencialmente podrían ocurrir;
c)	NO LO TIENE	27001	27001:2013	c) implementar cualquier acción necesaria;
d)	NO LO TIENE	27001	27001:2013	d) revisar la eficacia de las acciones correctivas tomadas, y
e)	NO LO TIENE	27001 Incluyendo S.I.G.	27001:2013	e) hacer cambios al S.I.G., si es necesario.
Segundo Parráfo	NO LO TIENE	27001	27001:2013	Las acciones correctivas deben ser apropiadas a los efectos de las no conformidades encontradas.
Tercer Parráfo	NO LO TIENE	27001	27001:2013	La organización debe conservar información documentada adecuada, como evidencia de:
f)	NO LO TIENE	27001	27001:2013	f) la naturaleza de las no conformidades y cualquier acción posterior tomada; y
g)	NO LO TIENE	27001	27001:2013	g) los resultados de cualquier acción correctiva.
10.2 MEJORA CONTINUA (Primer Parráfo)	**5.7.2 MEJORA CONTINUA** (Primer Parráfo)	27001 + 31000 Incluyendo S.I.G.	27001:2013	**10.2 MEJORA CONTINUA** La organización debe mejorar continuamente la conveniencia, idoneidad, adecuación y eficacia del S.I.G..
NO LO TIENE	Segundo Parráfo	31000 Incluyendo S.I.G.	31000:2018	Cuando se identifiquen brechas u oportunidades de mejora pertinentes, la organización debería desarrollar planes y tareas y asignarlas a quienes tuviesen que rendir cuentas de su implementación. Una vez impementadas, estas mejoras deberían contribuir al fortalecimiento del S.I.G.