Trabajo de Grado Especialización en Gestión Integrada QHSE

DISEÑO DEL SISTEMA INTEGRADO DE GESTIÓN NTC-ISO/IEC 27001:2013 E ISO 31000:2018, APLICADO A LA LEY ESTATUTARIA 1581 DE 2012 "POR LA CUAL SE DICTAN DISPOSICIONES GENERALES PARA LA PROTECCIÓN DE DATOS PERSONALES", PARA LA EMPRESA PAVIMENTACIONES MORALES S.L. SUCURSAL EN COLOMBIA.

Autora:
Natalia Brijaldo Valderrama

Director Trabajo de Grado:
M.Sc. Ing. Claudia Patricia Santiago Cely

Escuela Colombiana de Ingeniería Julio Garavito
Programa de Ingeniería Industrial
Especialización en Gestión Integrada QHSE
Cohorte XXXIX
Bogotá D.C., Colombia, julio 2018

Publicado en 2018 por la Escuela Colombiana de Ingeniería “Julio Garavito”. Avenida 13 No 205-59 Bogotá. Colombia
TEL: +57 – 1 668 36 00, e-mail: espeqhse@escuelaing.edu.co

Reconocimiento o Agradecimientos

Mi principal y mayor agradecimiento es a Dios, quien me concedió la oportunidad de realizar la especialización y cumplirla a cabalidad.

También doy gracias a mi familia por todo su apoyo, a la Escuela Colombiana de Ingeniería en especial al ingeniero Ricardo Augusto Vásquez, al ingeniero Jairo Raúl Chacón, a la ingeniera Claudia Patricia Santiago Cely, y a los docentes que compartieron sus conocimientos y experiencias con relación a la especialización.

Sinopsis

El presente trabajo de grado realiza el diseño de un sistema integrado de gestión basado en las normas NTC-ISO/IEC 27001:2013 e ISO 31000:2018, para dar cumplimiento a la Ley Estatutaria 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales", para la empresa Pavimentaciones Morales S.L. Sucursal en Colombia. Teniendo en cuenta que desde la vigencia de la Ley 1581 de 2012, al que debe estar comprometido la compañía, no se tiene evidencia de gestión en protección de datos personales, lo cual puede acarrear una multa a la empresa de hasta 2.000 SMMLV.

Resumen Ejecutivo

Por medio del presente proyecto se estableció el diseño de un sistema integrado de gestión basado en las normas NTC-ISO/IEC 27001:2013 e ISO 31000:2018, aplicado al cumplimiento de la Ley Estatutaria 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales", para la sucursal en Colombia de Pavimentaciones Morales.

Durante el desarrollo de la metodología se encontraron los siguientes hallazgos de interés para la empresa:

- Se encontraron cuarenta y cinco (45) artículos legales de protección de datos, aplicables a la empresa.

- Del cien porciento (100 %) de los riesgos hallados; el setenta y siete porciento (77%) de los riesgos son considerados críticos, según la escala establecida de evaluación y el veintitrés porciento (23%) restante es considerado significativo.

- Se determinaron los controles para los riesgos identificados, teniendo en cuenta que en este momento la empresa no se encuentra interesada en realizar inversiones en hardware y/o software.

De acuerdo a lo anterior, se recomienda a la empresa que se gestione los riesgos identificados y de esta manera mitigar considerablemente multas de hasta 2.000 SMMLV., sanciones, o cierre de la empresa por el no cumplimiento de la legislación en Colombia.

Tabla de contenido

Lista de Figuras

Lista de Tablas

1. INTRODUCCIÓN

1.1 PROBLEMÁTICA (JUSTIFICACIÓN)

Pavimentaciones Morales S.L. Sucursal en Colombia es una sucursal de una empresa de construcción vial española, radicada en Colombia desde el año 2012. Actualmente los activos de la sucursal superan los 100.000 UVT (Unidad de Valor Tributario); Lo anterior aplicándole el cumplimiento de la Ley Estatutaria 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales", teniendo que generar y adoptar un programa integral de gestión de datos personales.

Desde la vigencia de la Ley 1581 de 2012, al que debe estar comprometido la compañía, no se tiene evidencia ni gestión alguna del programa integral de gestión de datos personales, lo cual puede acarrear una multa a la empresa de hasta 2.000 SMMLV.

De las principales exigencias de la Ley Estatutaria 1581, se encuentran:

- Manual interno de políticas y procedimientos; la política del tratamiento de la información debe ser suministrada al RNBD que se encuentra a cargo de la Superintendencia de Industria y Comercio.

- Medidas de seguridad para proteger los datos personales y sensibles, evitando la adulteración, pérdida, consulta, uso o acceso fraudulento sobre la información.

A raíz de lo anterior, se genera la necesidad de crear en la empresa un sistema integrado de gestión para el tratamiento de datos personales, que dé cumplimiento a lo solicitado y establecido en la Ley 1581 de 2012. Por lo cual se decidió realizar el Sistema Integrado de gestión con las normas:

- ✓ NTC-ISO/IEC 27001:2013 Tecnología de la Información. Técnicas de Seguridad Sistemas de Gestión de la Seguridad de la Información.

- ✓ ISO 31000:2018. Gestión del Riesgo. Directrices.

1.2 OBJETIVOS Y PREGUNTA DE INVESTIGACIÓN

1.2.1 Objetivo general

Proporcionar directrices para la valoración y el tratamiento de los riesgos en la seguridad en los datos personales en *Pavimentaciones Morales S.L. Sucursal en Colombia* a través de un Sistema Integrado de Gestión NTC-ISO/IEC 27001:2013 e ISO 31000:2018, que permitan reducir el riesgo hasta un nivel aceptable y garantizar el cumplimiento de la Ley Estatutaria 1581 del 2012 Ley de protección de datos personales.

1.2.2 Objetivos específicos

1. Diseñar un Sistema Integrado de Gestión de las normas NTC-ISO/IEC 27001:2013 e ISO 31000:2018.

2. Analizar los posibles riesgos para la protección de datos de los afectados y valoración de la probabilidad que sucedan.

3. Diseñar Política y manuales de acuerdo con el diagnóstico, donde se trazarán los procesos, procedimientos, formatos y documentos necesarios para cumplir los requisitos de las normas y leyes de referencia.

1.2.3 Pregunta de investigación

¿Puede la organización mitigar, controlar o eliminar los riesgos expuestos a los que están sometidos los datos personales en la compañía, a través de un Sistema Integrado de Gestión de las normas NTC-ISO/IEC 27001:2013 e ISO 31000:2018?

1.3 ALCANCE Y LIMITACIONES

1.3.1 Alcance

El presente proyecto tendrá un alcance únicamente del diseño del S.I.G NTC-ISO/IEC 27001:2013 e ISO 31000:2018, aplicado únicamente al proceso de protección de datos personales según Ley Estatutaria 1581 de 2012, para la empresa Pavimentaciones Morales S.L. Sucursal en Colombia.

NOTA: El proyecto no contempla la implementación del sistema en ninguna de sus fases, ni la aprobación del mismo por parte de la empresa Pavimentaciones Morales S.L. Sucursal en Colombia.
Es importante resaltar que para el establecimiento de los objetivos del S.I.G., se debe realizar la identificación de los riesgos.

1.3.2 Limitaciones

Una de las principales limitaciones para el desarrollo del proyecto, es no contar con el apoyo a tiempo de los directivos de la empresa, en el suministro y/o ampliación de la información requerida.

1.4 METODOLOGÍA

Para el desarrollo del presenta trabajo de grado, se emplearán los siguientes métodos de investigación, para el desarrollo satisfactorio del proyecto:

INVESTIGACION Y DESARROLLO
Investigación, documentación y desarrollo de la metodología

APLICACIÓN DE LA METODOLOGIA

FASE 1 Creación del S.I.G.

- Analizar Compatibilidad de las normas NTC-ISO/IEC 27001:2013 e ISO 31000:2018.
- Documento consolidado S.I.G NTC-ISO/IEC 27001:2013 e ISO 31000:2018

FASE 2 Desarrollo del diseño del S.I.G.

Análisis
- Documentos requeridos por la norma integral.
- Contexto de la empresa.
- Requisitos legales.
- Activos de Información.

Valoración
- Nivel del Riesgo.

Tratamiento
- Medidas de Seguridad.

Plan de Acción
- Políticas
- Procedimientos

2. CAPÍTULO: MARCO TEÓRICO

2.1 LEY DE PROTECCIÓN DE DATOS

La normatividad de protección de datos inicialmente en Colombia se manejaba mediante la declaración de los Derechos Humanos en el Art 12 donde dice "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques". De esta manera se inicia un proceso normativo para garantizar el derecho de la protección de datos, después de esta declaración se empezaron a generar una cierta cantidad de resoluciones a nivel internacional en donde se realizaba la protección de los datos personales en países como México, Uruguay, Argentina, Perú, Nicaragua y Colombia.

En México se crea la Ley independiente de Protección de Datos Personales en Posesión de Particulares, denominada "Ley Federal de Protección de Datos Personales en Posesión De Los Particulares" (LFPDPPP) en el año 2010; en donde se manifiesta o se define como dato personal a "cualquier información concerniente a una persona identificada o identificable"[1], para ello cualquier información que se entregue por cualquier medio será respaldada por la Ley y las entidades privadas o gubernamentales deberán acatar esta normatividad.

Uruguay es uno de los países en los cuales mediante la Ley No. 18.331 de 2008, donde se explica en la legislación que "El derecho a la protección de datos personales es Inherente a la persona humana"[2] y está comprendida en el artículo 72 de la Constitución de la República Oriental del Uruguay. En el artículo 37 se consagra la acción del Habeas Data, con el artículo 31 de la Ley No. 18.331 de 2008, se crea la Unidad Regulada y de Control de Datos Personales (URCDP). Adicionalmente Uruguay ha sido reconocido como un país adecuado en materia de datos personales por la Unión Europea, y también ha sido el primer país en América Latina en ser invitado a adherir al Convenio 108 del Consejo de Europa.

---

[1] Congreso General de los Estados Unidos Mexicanos. (2010). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares.* Publicado *Diario Oficial de la Federación,* el 5 de julio de 2010. Mexico.

[2] Senado y Cámara de Representantes de la República Oriental del Uruguay. (2008). *Ley 18.331. Protección de Datos Personales y Acción de "Habeas Data".* Publicada *Diario Oficial* No. 27549, del 18 de agosto de 2008. Uruguay.

Ahora en Argentina se crea la Ley 25.326 en el año 2000, denominada "Protección de Datos Personales", en su primer artículo menciona "La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional. Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal. En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas"[3]. Esto los llevo a ser un país pionero en américa latina creando la Dirección Nacional de protección de Datos Personales (DNPDP).

Finalmente en Colombia el 17 de Octubre del 2012 se expide la ley 1581 que es la ley estatutaria de protección de datos personales en su artículo 1 menciona lo siguiente "La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma."

Una vez conociendo que en varios países de Latinoamérica tienen una ley o un decreto que protege los datos personales de todas las personas en entidades públicas o privadas, se quiere dar a conocer la aplicación de estas leyes en especial en Colombia con la ley 1581 de 2012 y para ello se tendrá en cuenta las normas ISO 27001 e ISO 31000 para la resolución de este proyecto.

2.2 NORMA ISO/IEC 27001

Esta norma certificable de la Organización Internacional de Normalización (ISO), describe como se debe gestionar la seguridad de la información, estableciendo las medidas para una implementación efectiva. Su origen y trascendencia se describe a continuación:

[3] Senado y Cámara de Diputados de la Nación de Argentina. (2000). *Ley 25.326. Protección de los Datos Personales.* Publicada *Boletín Oficial*, del 02 de noviembre de 2000. Argentina.

Tabla 2–1 Historia ISO/IEC 27001

AÑO	NORMA	NOMBRE	DESCRIPCIÓN
1995	BS 7799-1:1995	Gestión de seguridad de la información. Código de prácticas para los sistemas de gestión de la seguridad de la información.	Consistía únicamente en recomendaciones para administrar la Seguridad de la Información, no era certificable.
1999	Bs 7799-2:1999	Gestión de seguridad de la información. Especificación para sistemas de gestión de seguridad de la información.	Requisitos de implementación de un SGSI certificable.
2000	ISO/IEC 17799:2000	Tecnología de la información - Código de prácticas para la gestión de la seguridad de la información.	La norma Bs 7799-2:1999, fue tomada por La Organización Internacional para la Estandarización.
2005	ISO/IEC 27001:2005	Tecnología De la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos.	Nueva versión de la norma internacional certificable. Enfocado en el ciclo PHVA.
2013	ISO/IEC 27001:2013	Tecnología De la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos.	Se generan cambios significativos en su estructura evaluación y tratamiento de riesgos. Está enfocado a la alta dirección.

Fuente: Elaboración Propia.

Siendo de esta manera el estándar más usado en las empresas para la seguridad de la información; según informe estadístico de ISO Survey al año 2016, se encontraban certificadas 33.290 empresas en 150 países a nivel mundial. Generando un incremento del 20% con respecto al año 2015. Colombia hasta el año 2016 se encuentra con 163 empresas certificadas en la norma ISO/IEC 27001. El país pionero con empresas certificadas en esta norma es Japón con 8.945 certificaciones al año 2016.

La norma NTC ISO/IEC 27001:2013 (norma que aplica al desarrollo del presente proyecto) es una norma certificable, dirigida a todas las organizaciones independientemente de su naturaleza, tamaño u objeto social, y su estructura es de alto nivel.

La "estructura de alto nivel" es un elemento normativo definido en el Apéndice SL del documento ISO/IEC Directivas, Parte 1, que establece que las normas deben llevar la misma estructura de referencia (capítulos), texto básico idéntico, términos y definiciones comunes. Con el objetivo de consolidar con mayor veracidad la integración de las normas que estén bajo esta misma estructura. La estructura de referencia establecida es la siguiente:

4. Contexto de la organización.
5. Liderazgo.
6. Planificación.
7. Soporte.
8. Operación.
9. Evaluación del desempeño.
10. Mejora.

A lo cual esta versión 2013 se acoge a lo establecido en el Apéndice SL del documento ISO/IEC Directivas y la distribución de sus capítulos está establecido de la siguiente manera:

Introducción.
0.1 Generalidades.
0.2 Compatibilidad con otras normas.
1. Objeto y campo de aplicación.
2. Referencias normativas.
3. Términos y definiciones.
4. Contexto de la organización.
5. Liderazgo.
6. Planificación.
7. Soporte.
8. Operación.
9. Evaluación del desempeño.
10. Mejora.

A través de su secuencia estructural, se va ejecutando el ciclo P.H.V.A.

El Ciclo P.H.V.A (Planificar, Hacer, Verificar, Actuar) o ciclo Deming, es una herramienta metodológica que permite cíclicamente realizar la mejora continua del sistema.

"La principal característica de un ciclo PHVA es que no tiene un punto y final en el momento en que se obtenga un determinado resultado, sino que se crea una rueda continua en la que el ciclo se reinicia una y otra vez de manera periódica"[4], como se explica en la Figura 3-1.

A continuación, se realiza la definición de las cuatro fases de ciclo:

Planificar: Corresponde a todo el diseño del sistema para conseguir los resultados esperados teniendo en cuenta los requisitos de la norma.

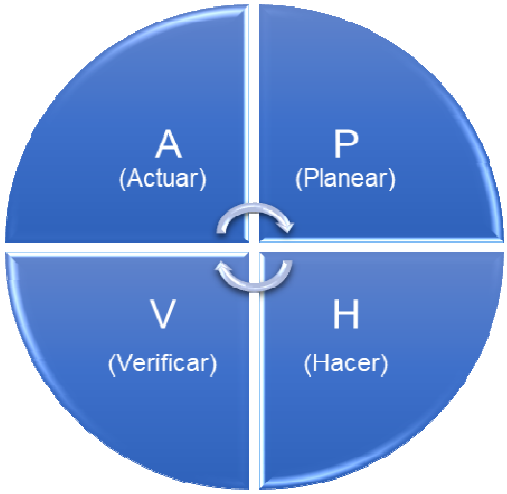
Hacer: Corresponde a la implementación del sistema planeado.

Verificar: Corresponde a la revisión y evaluación del avance del sistema, comparando el avance de los procesos con lo establecido en la planificación (políticas, objetivos, requisitos de la norma, requisitos legales, etc.).

Actuar: Teniendo en cuenta la revisión y evaluación en la fase anterior, se emprenden las acciones necesarias para corregir y/o mejorar continuamente el sistema y lograr los resultados esperados.

[4] ISOTools. (2015), *En que consiste el Ciclo PHVA de Mejora Continua.* 20 de febrero de 2015. Recuperado de https://www.isotools.org/2015/02/20/en-que-consiste-el-ciclo-phva-de-mejora-continua/

Figura 2–1 Ciclo P.H.V.A.



Fuente: Elaboración propia.

2.3 NORMA ISO 31000

El inicio de la norma ISO 31000 se da por la necesidad de evaluar y tratar cualquier tipo de riesgo que se presente en una empresa, para ello el comité de técnicos de ISO creó la norma estableciendo los principios y directrices para la gestión del riesgo en su primera versión en el año 2009 y de esta, manera que las empresas y organizaciones revalúen las metodologías de gestiones sobre cualquier tipo de riesgo que se pueda presentar.

La última versión de la norma se establece en del año 2018, en la que se realizan algunos cambios significativos con respecto a la norma que se había presentado hace 9 años; la nueva versión se enfoca a la alta dirección, y su lenguaje es más comprensible y conciso con respecto a la versión anterior. Esta norma se establece en 6 capítulos, y solamente definen 06 principios.

La última versión de esta norma ISO 31000 (norma que aplica al desarrollo del presente proyecto), está dirigida a las personas que gestionan riesgos en las organizaciones. Esta es una norma que no es certificable y tampoco tiene estructura de alto nivel, por lo tanto, su estructura de referencia está establecida de la siguiente manera:

Introducción.
1. Objeto y campo de aplicación.
2. Referencias normativas.

3. Términos y definiciones.
4. Principios.
5. Marco de referencia.
5.1 Generalidades.
5.2 Liderazgo y compromiso.
5.3 Integración.
5.4 Diseño.
5.4.1 Comprensión de la organización y de su contexto.
5.4.2 Articulación con el compromiso de la gestión del riesgo.
5.4.3 Asignación de roles, autoridades y obligaciones de rendir cuentas en la organización.
5.4.4 Asignación de recursos.
5.4.5 Establecimiento de la comunicación y consulta.
5.5 Implementación.
5.6 Valoración.
5.7 Mejora.
5.7.1 Adaptación.
5.7.2 Mejora continua.
6. Progreso.
6.1 Generalidades.
6.2 Comunicación y consulta.
6.3 Alcance, contexto y criterios.
6.3.1 Generalidades.
6.3.2 Definición del alcance.
6.3.3 Contextos externo e interno.
6.3.4 Definición de los criterios del riesgo.
6.4 Evaluación del riesgo.
6.4.1 Generalidades.
6.4.2 Identificación del riesgo.
6.4.3 Análisis del riesgo.
6.4.4 Valoración del riesgo.
6.5 Tratamiento del riesgo.
6.5.1 Generalidades.
6.5.2 Selección de las opciones para el tratamiento del riesgo.
6.5.3 Preparación e implementación de los planes de tratamiento del riesgo.
6.6 Seguimiento y revisión.
6.7 Registro e informe.

Dada la organización de sus capítulos, la integración con otras normas es un poco compleja.

3. CAPÍTULO: DESARROLLO DE LA METODOLOGÍA

3.1 MÓDULO 1: NATURALEZA DEL PROYECTO

3.1.1 Diseño de la Norma Integrada de Gestión NTC-ISO/IEC 27001:2013 e ISO 31000:2018

El diseño de la Norma Integrada de Gestión NTC-ISO/IEC 27001:2013 e ISO 31000:2018, está conformado por dos partes.

En la primera parte se analiza la compatibilidad de las normas NTC-ISO/IEC 27001:2013 e ISO 31000:2018. Y en la segunda parte dando continuidad al análisis de compatibilidad, se realiza el consolidado de las normas, generando un solo documento.

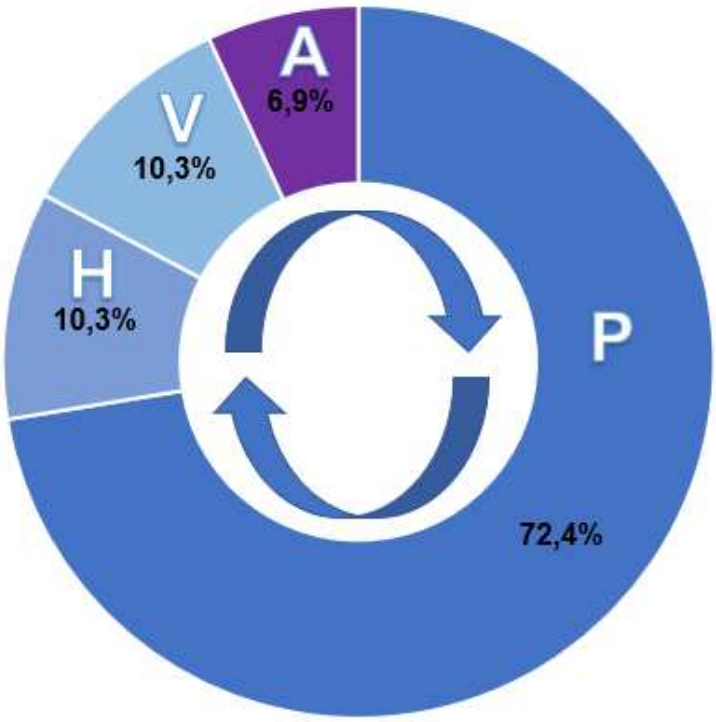
3.1.1.1 Análisis de Compatibilidad de las normas NTC-ISO/IEC 27001:2013 e ISO 31000:2018.

El análisis de compatibilidad se realizó a través de la asociación de los numerales entre las normas NTC-ISO/IEC 27001:2013 e ISO 31000:2018, tomando como base o referencia para la compatibilidad e integración, la norma NTC-ISO/IEC 27001:2013 (dado que esta norma es la que cuenta con estructura de alto nivel), asociando de esta manera los numerales de la norma ISO 31000:2018 a los numerales de la norma NTC-ISO/IEC 27001:2013.

Dada la compatibilidad de los numerales, se evidencio que gran porcentaje de la Norma Integrada está enfocada a la planificación del S.I.G., con un 72.4%, seguido de hacer, verificar y actuar (ver Figura 3-1).

Adicionalmente se realizó una comparación entre los documentos que se deben conservar o mantener de las normas en relación con los documentos que son solicitados para el cumplimiento de la Ley 1581 de 2012. Cabe resaltar que dado que en la norma ISO 31000:2018 se menciona "debería" en sus numerales, únicamente se hizo referencia con respecto a documentación, al numeral 6.7 que menciona de manera general las consideraciones con respecto a la información documentada.

Figura 3–1 Ciclo P.H.V.A. Norma Integral



Fuente: Elaboración propia.

En la Tabla 3-1 se muestra el resultado del análisis de compatibilidad entre las normas, que también puede ser consultado en el Anexo G.

Tabla 3–1Compatibilidad de las normas NTC-ISO/IEC 27001:2013 e ISO 31000:2018

CICLO PHVA		NUMERALES ISO 27001:2013	NUMERALES ASOCIADOS	SE DEBE CONSERVAR O MANTENER INFORMACIÓN DOCUMENTADA?			LEY 1581 DE 2012		CONCLUSIÓN FINAL
			ISO 31000:2018	SI	DESCRIPCION ISO 27001:2013	DESCRIPCIÓN ISO 31000:2018	RELACIÓN NORMAS ISO CON LA LEY 1581 DE 2012	INFORMACIÓN DOCUMENTADA QUE SE DEBE CONSERVAR DE LA LEY 1581	
----------		0.1 GENERALIDADES							
		0.2 COMPATIBILIDAD CON OTRAS NORMAS DE SISTEMAS DE GESTION							
		1. OBJETO Y CAMPO DE APLICACIÓN	1. OBJETO Y CAMPO DE APLICACIÓN						
		2. REFERENCIAS NORMATIVAS	2. REFERENCIAS NORMATIVAS						
		3. TERMINOS Y DEFINICIONES	3. TERMINOS Y DEFINICIONES						
			4. PRINCIPIOS						
		4. CONTEXTO DE LA ORGANIZACIÓN	5.4.1 COMPRENSIÓN DE LA ORGANIZACIÓN Y DE SU CONTEXTO						
		4.1 CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO	6.3.3 CONTEXTOS EXTERNO E INTERNO						
		4.2 COMPRENSION DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS	----------						
		4.3 DETERMINACION DEL ALCANCE DEL SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION	6.3.2 DEFINICIÓN DEL ALCANCE	X	EL ALCANCE DEBE ESTAR DISPONIBLE COMO INFORMACIÓN DOCUMENTADA. TAMBIÉN SE DEBERÁN ESPECIFICAR LOS RECURSOS NECESARIOS, LAS RESPONSABILIDADES Y AUTORIDADES, Y LOS REGISTROS QUE SE DEBEN CONSERVAR.	EL ALCANCE DEBE ESTAR DISPONIBLE COMO INFORMACIÓN DOCUMENTADA			
		4.4 SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION	----------						
		5. LIDERAZGO	5.3 INTEGRACION						
		5.1 LIDERAZGO Y COMPROMISO	5.2 LIDERAZGO Y COMPROMISO						
		5.2 POLITICA	----------	X	LA POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN DEBE: E) ESTAR DISPONIBLE COMO INFORMACIÓN DOCUMENTADA.		AUNQUE EN LA LEY 1581 NO SE TIENE DESTINADO UN NUMERAL ESPECIFICO EL MISMO DICE QUE SE DEBE ELABORAR UNA QUE ES LA ELABORACIÓN DE ESTA, LA MENCIONADA IMPLICITAMENTE EN LOS DEBERES DE LOS RESPONSABLES Y ENCARGADOS DE LOS TRATAMIENTOS DE DATOS (ARTICULO 17 Y 18 DE LA LEY).		
		5.3 ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN	5.4.3 ASIGNACIÓN DE ROLES, AUTORIDADES, RESPONSABILIDADES Y OBLIGACIÓN DE RENDIR CUENTAS EN LA ORGANIZACIÓN				EN LOS ARTÍCULOS 17 Y 18 DE LA LEY 1581 DE 2012, EN EL QUE MENCIONAN LOS DEBERES DE LOS RESPONSABLES Y ENCARGADOS DE LOS TRATAMIENTOS DE DATOS, MENCIONA "ADOPTAR UN MANUAL INTERNO DE POLITICAS Y ***PROCEDIMIENTOS*** PARA GARANTIZAR EL ADECUADO CUMPLIMIENTO DE LA PRESENTE LEY Y, EN ESPECIAL, PARA LA ATENCIÓN DE CONSULTAS Y RECLAMOS POR PARTE DE LOS TITULARES. " AL IGUAL QUE LA POLITICA ESTA DESCRIBE IMPLICITAMENTE LA ELABORACIÓN DE PROCEDIMIENTOS PARA EL CARGO DE RESPONSABILIDAD.		
		----------	5.4.2 ARTICULACIÓN DEL COMPROMISO CON LA GESTIÓN DEL RIESGO						
		6. PLANIFICACIÓN	----------						
		6.1 ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES	----------						
		6.1.1 GENERALIDADES	6.1 GENERALIDADES 6.3.4 DEFINICIÓN DE LOS CRITERIOS DEL RIESGO						
		6.1.2 VALORACION DE RIESGOS DE LA SEGURIDAD DE LA INFORMACION	6.4 EVALUACIÓN DEL RIESGO	X	LA ORGANIZACIÓN DEBE CONSERVAR INFORMACIÓN DOCUMENTADA ACERCA DEL PROCESO DE VALORACIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN.				
			6.4.1 GENERALIDADES 6.4.2 IDENTIFICACIÓN DEL RIESGO 6.4.3 ANÁLISIS DEL RIESGO 6.4.4 VALORACIÓN DEL RIESGO						
72,4%	P	6.1.3 TRATAMIENTO DE RIESGOS DE LA SEGURIDAD DE LA INFORMACION	6.5 TRATAMIENTO DEL RIESGO	X	LA ORGANIZACIÓN DEBE CONSERVAR INFORMACIÓN DOCUMENTADA ACERCA DEL PROCESO DE TRATAMIENTO DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN.				AUNQUE LA LEY 1581 DE 2012 " POR EL CUAL SE DICTAN DISPOSICIONES GENERALES PARA LA PROTECCIÓN DE DATOS PERSONALES", COMO SU NOMBRE LO DESCRIBE ES PARA LA ***PROTECCIÓN DE DATOS PERSONALES*** ES DECIR ACOTA MUY SUPERFICIALMENTE EN LOS ARTÍCULOS DE LA LEY LA IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN EN LA PROTECCIÓN DE DATOS, LO QUE HA LLEVADO A GENERAR CREITOS VACÍOS EN LAS PERSONAS INVOLUCRADAS EN ESTOS PROCESOS, TENIENDO UNA IDEA VANA QUE EL CUMPLIMIENTO DE LA LEY ES ÚNICAMENTE SUBIR LA INFORMACIÓN A LA PAGINA DE LA S.I.C., Y "CREAR" UNA POLITICA Y PROCEDIMIENTOS PARA DAR CUMPLIMIENTO A LA LEY. SIN TENER EN CUENTA QUE LO REALMENTE IMPORTE NO ES CUMPLIR FORMATOS SINO GARANTIZAR LA PROTECCIÓN DE LOS DATOS PERSONALES A TRAVÉS DE GESTIÓN EN LA IDENTIFICACIÓN, ANÁLISIS Y EVALUACIÓN DE LOS RIESGOS A LOS QUE ESTAN SOMETIDOS LOS DATOS Y GARANTIZAR LA PROTECCIÓN DE DE LOS MISMOS. QUE ES LO QUE SE GESTIONA CON EL MODELO INTEGRADO.
			6.4.1 GENERALIDADES 6.5.2 SELECCION DE LAS OPCIONES PARA EL TRATAMIENTO DEL RIESGO						
			6.5.3 PREPARACIÓN E IMPLEMENTACIÓN DE LOS PLANES DE TRATAMIENTO DEL RIESGO	X	F) OBTENER, DE PARTE DE LOS DUEÑOS DE LOS RIESGOS, LA APROBACIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN, Y LA ACEPTACIÓN DE LOS RIESGOS RESIDUALES DE LA SEGURIDAD DE LA INFORMACIÓN.				
		6.2 OBJETIVOS DE SEGURIDAD DE LA INFORMACION Y PLANES PARA LOGRARLOS	----------	X	LA ORGANIZACIÓN DEBE CONSERVAR INFORMACIÓN DOCUMENTADA SOBRE LOS OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN				
		7. SOPORTE	----------						
		7.1 RECURSOS	5.4.4 ASIGNACIÓN DE RECURSOS						
		7.2 COMPETENCIA	----------	X	CONSERVAR LA INFORMACIÓN DOCUMENTADA APROPIADA, COMO EVIDENCIA DE LA COMPETENCIA.				
		7.3 TOMA DE CONCIENCIA	----------						
		7.4 COMUNICACIÓN	5.4.5 ESTABLECIMIENTO DE LA COMUNICACIÓN Y LA CONSULTA					ARTÍCULO 17. DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO. B) SOLICITAR Y CONSERVAR, EN LAS CONDICIONES PREVISTAS EN LA PRESENTE LEY, COPIA DE LA RESPECTIVA AUTORIZACIÓN OTORGADA POR EL TITULAR.	
			6.2 COMUNICACIÓN Y CONSULTA					ARTÍCULO 12. DEBER DE INFORMAR AL TITULAR. EL RESPONSABLE DEL TRATAMIENTO, AL MOMENTO DE SOLICITAR AL TITULAR LA AUTORIZACIÓN, DEBERÁ INFORMARLE DE MANERA CLARA Y EXPRESA LO SIGUIENTE: A) EL TRATAMIENTO AL CUAL SERÁN SOMETIDOS SUS DATOS PERSONALES Y LA FINALIDAD DEL MISMO. B) EL CARÁCTER FACULTATIVO DE LA RESPUESTA A LAS PREGUNTAS QUE LE SEAN HECHAS, CUANDO ESTAS VERSEN SOBRE DATOS SENSIBLES O SOBRE LOS DATOS DE LAS NIÑAS, NIÑOS Y ADOLESCENTES. C) LOS DERECHOS QUE LE ASISTEN COMO TITULAR. D) LA IDENTIFICACIÓN, DIRECCIÓN FÍSICA O ELECTRÓNICA Y TELÉFONO DEL RESPONSABLE DEL TRATAMIENTO. **PARÁGRAFO.** EL RESPONSABLE DEL TRATAMIENTO DEBERÁ CONSERVAR PRUEBA DEL CUMPLIMIENTO DE LO PREVISTO EN EL PRESENTE ARTÍCULO Y, CUANDO EL TITULAR LO SOLICITE, ENTREGARLE COPIA DE ESTA.	
		7.5 INFORMACION DOCUMENTADA	----------						
		7.5.1 GENERALIDADES	----------	X	LA INFORMACIÓN DOCUMENTADA QUE LA ORGANIZACIÓN HA DETERMINADO QUE ES NECESARIA PARA LA EFICACIA DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.				
		7.5.2 CREACION Y ACTUALIZACION	6.7 REGISTRO E INFORME	X		LAS DECISIONES CON RESPECTO A LA CREACIÓN, CONSERVACIÓN Y TRATAMIENTO DE LA INFORMACIÓN DOCUMENTADA DEBERÁN TENER EN CUENTA, PERO NO LIMITARSE A SU USO, LA SENSIBILIDAD DE LA INFORMACIÓN Y LOS CONTEXTOS EXTERNO E INTERNO.			
		7.5.3 CONTROL DE LA INFORMACION DOCUMENTADA	----------					ARTÍCULOS 17 Y 18. DEBERES DE LOS RESPONSABLES Y ENCARGADOS DE LOS TRATAMIENTOS DE DATOS. "ADOPTAR LAS MEDIDAS NECESARIAS PARA GARANTIZAR LAS CONDICIONES DE SEGURIDAD NECESARIAS PARA IMPEDIR SU ADULTERACIÓN, PÉRDIDA, CONSULTA, USO O ACCESO NO AUTORIZADO O FRAUDULENTO."	
		8. OPERACIÓN	----------						
10,3%	H	8.1 PLANIFICACION Y CONTROL OPERACIONAL	5.5 IMPLEMENTACIÓN	X	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.				
		8.2 VALORACION DE RIESGOS DE LA SEGURIDAD DE LA INFORMACION	----------	X	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 INFORMACION	----------	X	LA ORGANIZACIÓN DEBE CONSERVAR INFORMACIÓN DOCUMENTADA DE LOS RESULTADOS DEL TRATAMIENTO DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN				
		9. EVALUACIÓN DEL DESEMPEÑO	----------						
10,3%	V	9.1 SEGUIMIENTO, MEDICION, ANÁLISIS Y EVALUACION	5.6 VALORACIÓN	X	LA ORGANIZACIÓN DEBE CONSERVAR INFORMACIÓN DOCUMENTADA APROPIADA COMO EVIDENCIA DE LOS RESULTADOS DEL MONITOREO Y DE LA MEDICIÓN.				
			6.6 SEGUIMIENTO Y REVISIÓN						
		9.2 AUDITORIA INTERNA	----------	X	CONSERVAR INFORMACIÓN DOCUMENTADA COMO EVIDENCIA DE LA IMPLEMENTACIÓN DEL PROGRAMA DE AUDITORÍA Y DE LOS RESULTADOS DE ESTA.				
		9.3 REVISION POR LA DIRECCION	----------	X	LA ORGANIZACIÓN DEBE CONSERVAR INFORMACIÓN DOCUMENTADA COMO EVIDENCIA DE LOS RESULTADOS DE LAS REVISIONES POR LA DIRECCIÓN.				
		10. MEJORA	5.7 MEJORA						
6,9%	A	10.1 NO CONFORMIDADES Y ACCIONES CORRECTIVAS	----------	X	LA ORGANIZACIÓN DEBE CONSERVAR INFORMACIÓN DOCUMENTADA ADECUADA, COMO EVIDENCIA DE: F) LA NATURALEZA DE LAS NO CONFORMIDADES Y CUALQUIER ACCIÓN POSTERIOR TOMADA, Y G) LOS RESULTADOS DE CUALQUIER ACCIÓN CORRECTIVA				
		10.2 MEJORA CONTINUA	5.7.2 MEJORA CONTINUA						

Fuente: Elaboración Propia.

3.1.1.2 Documento consolidado S.I.G NTC-ISO/IEC 27001:2013 e ISO 31000:2018

Posteriormente al estudio de compatibilidad de los numerales de las normas, se realizó un estudio minucioso de compatibilidad e integración de aproximadamente 350 párrafos (su integración se puede verificar en el Anexo A Tabla de Integración Norma Integral) entre las normas NTC-ISO/IEC 27001:2013 e ISO 31000:2018, permitiendo como resultado la "Norma Integral de Gestión NTC-ISO/IEC 27001:2013 e ISO 31000:2018".

Con la metodología implementada para la integración de los párrafos, la norma integral está diseñada a través de párrafos combinados entre las normas, párrafos textuales de las normas, y adición a los párrafos de las normas, según su análisis de integración. En el Anexo A, se encuentra de manera explícita, la integración de los párrafos, especificando que hace parte de cada norma, que se combinó y qué es adicional.

Teniendo en cuenta que los numerales 0.1, 0.2, 1, 2 y 3 de la norma NTC-ISO/IEC 27001:2013, corresponden a la parte introductoria de la norma, la integración se realizó a partir del numeral 4. "Contexto de la organización" (para mayor información dirigirse al Anexo A.), razón por la cual la Norma Integral comienza numerada en 4 (numeral donde se da comienzo al ciclo P.H.V.A.). Cabe resaltar que es de suma importancia mencionar los principios de la ISO 31000:2018, lo que se consideró como parte introductoria en la Norma Integral.

NORMA INTEGRAL DE GESTIÓN
NTC-ISO/IEC 27001:2013 e ISO 31000:2018

PRINCIPIOS

El propósito de la gestión del riesgo es la creación y la protección del valor. Mejora el desempeño, fomenta la innovación y contribuye al logro de objetivos.
Los principios descritos en la Figura 3-2 proporcionan orientación sobre las características de una gestión del riesgo eficaz y eficiente, comunicando su valor y explicando su intención y propósito. Los principios son el fundamento de la gestión del riesgo y se deberían considerar cuando se establece el marco de referencia y los procesos de la gestión del riesgo de la organización. Estos principios deberían habilitar a la organización para gestionar los efectos de la incertidumbre sobre sus objetivos.

Figura 3–2 Principios

Fuente: Elaboración Propia.

La gestión del riesgo eficaz requiere los elementos de la Figura 3-2 y puede explicarse como sigue:

a) Integrada

La gestión del riesgo es parte integral de todas las actividades de la organización.

b) Estructurada y exhaustiva

Un enfoque estructurado y exhaustivo hacia la gestión del riesgo contribuye a resultados coherentes y comparables.

c) Adaptada

El marco de referencia y el proceso de la gestión del riesgo se adaptan y son proporcionales a los contextos externo e interno de la organización relacionados con sus objetivos.

d) Inclusiva

La participación apropiada y oportuna de las partes interesadas permite que se consideren su conocimiento, puntos de vista y percepciones. Esto resulta en una mayor toma de conciencia y una gestión del riesgo informada.

e) Dinámica

Los riesgos pueden aparecer, cambiar o desaparecer con los cambios de los contextos externo e interno de la organización. La gestión del riesgo anticipa, detecta, reconoce y responde a esos cambios y eventos de una manera apropiada y oportuna.

f) Mejor información disponible

Las entradas a la gestión del riesgo se basan en información histórica y actualizada, así como en expectativas futuras. La gestión del riesgo tiene en cuenta explícitamente cualquier limitación e incertidumbre asociada con tan información y expectativas. La información debería ser oportuna, clara y disponible para las partes interesadas pertinentes.

g) Factores humanos y disponibles

El comportamiento humano y la cultura influyen considerablemente en todos los aspectos de la gestión del riesgo en todos los niveles y etapas.

h) Mejora continua

La gestión del riesgo mejora continuamente mediante aprendizaje y experiencia.

4. CONTEXTO DE LA ORGANIZACIÓN

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.

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 reflejar 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.

La comprensión de contexto es importante porque:

a) la gestión del riesgo y seguridad de la información, tiene lugar en el contexto de los objetivos y las actividades de la organización;

b) los factores organizacionales pueden ser una fuente de riesgo;

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 organización como un todo.

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:

a) los factores sociales, culturales, políticos, legales, reglamentarios, financieros, tecnológicos, económicos y ambientales ya sea a nivel internacional, nacional, regional o local;

b) los impulsores clave y las tendencias que afectan a los objetivos de la organización;

c) las relaciones, percepciones, valores, necesidades y expectativas de las partes interesadas externas;

d) las relaciones contractuales y los compromisos;

e) la complejidad de las redes y dependencias.

El análisis del contexto interno de la organización puede incluir, pero no limitarse a:

f) la visión, la misión y los valores;

g) la gobernanza, la estructura de la organización, los roles y la rendición de cuentas;

h) la estrategia, los objetivos y las políticas;

i) la cultura de la organización;

j) las normas, las directrices y los modelos adoptados por la organización;

k) las capacidades, entendidas en términos de recursos y conocimiento (por ejemplo, capital, tiempo, personas, propiedad intelectual, procesos, sistemas y tecnologías);

l) los datos, los sistemas de información y los flujos de información;

m) las relaciones con partes interesadas internas, teniendo en cuenta sus percepciones y valores;

n) las relaciones contractuales y los compromisos;

o) las interdependencias e interconexiones.

4.2 COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS

La organización debe determinar:

a) las partes interesadas que son pertinentes al S.G.I.; y

b) los requisitos de estas partes interesadas pertinentes a seguridad de la información y gestión del riesgo.

NOTA Los requisitos de las partes interesadas pueden incluir los requisitos legales y reglamentarios, y las obligaciones contractuales.

4.3 DETERMINACIÓN DEL ALCANCE DEL S.I.G.

La organización debe determinar los límites y la aplicabilidad del S.I.G. para establecer su alcance.

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.

Cuando se determina este alcance, la organización debe considerar:

a) las cuestiones externas e internas referidas en el numeral 4.1, y

b) los requisitos referidos en el numeral 4.2;

c) las interfaces y dependencias entre las actividades realizadas por la organización, y las que realizan otras organizaciones;

d) los objetivos y las decisiones que se necesitan tomar;

e) los resultados esperados de las etapas a ejecutar en el proceso;

f) el tiempo, la ubicación, las inclusiones y las exclusiones especificas;

g) las herramientas y las técnicas apropiadas de evaluación del riesgo;

h) los recursos requeridos, responsabilidades y registros a conservar;

i) las relaciones con otros proyectos, procesos y actividades.

El alcance debe estar disponible como información documentada.

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.

4.4.1 Integración

La integración de la gestión del riesgo y la seguridad de la información, depende de la compresión de las estructuras y el contexto de la organización. Las estructuras difieren dependiendo del propósito, las metas y la complejidad de la organización. El riesgo se gestiona en cada parte de la estructura de la organización. Todos los miembros de una organización tienen la responsabilidad de gestionar el riesgo y la seguridad de la información.

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.

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

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) 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) asegurando la integración de los requisitos del S.I.G. en los procesos de la organización;

c) asegurando que los recursos necesarios para el S.I.G. estén disponibles;

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) asegurando que el S.I.G. logre los resultados previstos;

f) asignando autoridad, responsabilidad y obligación de rendir cuentas en los niveles apropiados dentro de la organización;

g) dirigiendo y apoyando a las personas, para contribuir a la eficacia del S.I.G.;

h) promoviendo el seguimiento sistemático y la mejora continua, y

i) apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidad.

Esto ayudará a la organización a:

j) reconocer y acordar todas las obligaciones, así como sus compromisos voluntarios;

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.

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:

l) se aseguren de que los riesgos se consideran apropiadamente cuando se establezcan los objetivos de la organización;

m) comprendan los riesgos a los que hace frente la organización en la búsqueda de sus objetivos;

n) se aseguren de que los sistemas para gestionar estos riesgos se implementen y operen eficazmente;

o) se aseguren de que estos riesgos sean apropiados en el contexto de los objetivos de la organización;

p) se aseguren de que la información sobre estos riesgos y su gestión se comunique de la manera apropiada.

5.2 POLÍTICA

La alta dirección debe establecer una política de la seguridad de la información y la gestión del riesgo que:

a) sea adecuada al propósito de la organización;

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) incluya el compromiso de cumplir los requisitos aplicables relacionados con la seguridad de la información y la gestión del riesgo; y

d) incluya el compromiso de mejora continua del S.I.G.

La política de la seguridad de la información y la gestión del riesgo debe:

e) estar disponible como información documentada;

f) comunicarse dentro de la organización; y

g) estar disponible para las partes interesadas, según sea apropiado.

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 y gestión del riesgo se asignen y comuniquen a todos los niveles de la organización.

La alta dirección debe asignar la responsabilidad y autoridad para:

a) asegurarse de que el S.I.G sea conforme con los requisitos de esta Norma Integral;

b) informar a la alta dirección sobre el desempeño del S.I.G.

c) enfatizar que la gestión del riesgo es una responsabilidad principal;

d) identificar a las personas que tienen asignada la obligación de rendir cuentas y la autoridad para gestionar el riesgo (dueños del riesgo).

NOTA La alta dirección también puede asignar responsabilidades y autoridades para informar sobre el desempeño del S.I.G. dentro de la organización.

5.4 ARTICULACIÓN 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:

a) el propósito de la organización para gestionar el riesgo y la seguridad de la información, y los vínculos con sus objetivos y otras políticas;

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;

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;

d) las autoridades, las responsabilidades y la obligación de rendir cuentas;

c) la disponibilidad de los recursos necesarios;

d) la manera de manejar los objetivos en conflicto;

e) la medición e informe como parte de los indicadores de desempeño de la organización;

f) la revisión y la mejora.

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

6.1 ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES

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 del riesgo, con el fin de:

a) asegurarse de que el S.I.G. pueda lograr sus resultados previstos;

b) prevenir o reducir efectos indeseados; y

c) lograr la mejora continua.

La organización debe planificar:

d) las acciones para tratar estos riesgos y oportunidades; y

e) la manera de:

1) integrar e implementar estas acciones en sus procesos del S.I.G.,

2) evaluar la eficacia de estas acciones.

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.

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.

Para establecer los criterios del riesgo, se debería considerar lo siguiente:

a) la naturaleza y los tipos de las incertidumbres que pueden afectar a los resultados y objetivos (tanto tangibles como intangibles);

b) cómo se van a definir y medir las consecuencias (tanto positivas como negativas) y la probabilidad;

c) los factores relacionados con el tiempo;

d) la coherencia en el uso de las mediciones;

e) cómo se va a determinar el nivel de riesgo;

f) cómo se tendrán en cuenta las combinaciones y las secuencias de múltiples riesgos;

g) la capacidad de la organización.

6.1.3 Evaluación del riesgo

6.1.3.1 Generalidades

La evaluación del riesgo es el proceso global de identificación del riesgo, análisis del riesgo y valoración del riesgo.

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.

La organización debe definir y aplicar un proceso de valoración de riesgos de la seguridad de la información que:

a) establezca y mantenga criterios de riesgo de la seguridad de la información que incluyan:

1) Los criterios de aceptación de riesgos; y

2) los criterios para realizar valoraciones de riesgos de la seguridad de la información;

b) asegure que las valoraciones repetidas de riesgos de la seguridad de la información produzcan resultados consistentes, válidos y comparables;

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.

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:

a) los riesgos asociados con la pérdida de la confidencialidad de integridad y de disponibilidad de información dentro del alcance del S.I.G.

b) las fuentes de riesgo tangibles e intangibles;

c) las causas y los eventos;

d) las amenazas y las oportunidades;

e) las vulnerabilidades y las capacidades;

f) los cambios en los contextos externo e interno;

g) los indicadores de riesgo emergentes;

h) la naturaleza y el valor de los activos y recursos;

i) las consecuencias y sus impactos en los objetivos;

j) las limitaciones de conocimiento y la confiabilidad de la información;

k) los factores relacionados con el tiempo;

l) identificar a los dueños de los riesgos;

m) los sesgos, los supuestos y las creencias de las personas involucradas.

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.

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.

El análisis del riesgo se puede realizar con diferentes grados de detalle y complejidad, dependiendo 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.

El análisis del riesgo debería considerar factores tales como:

a) la probabilidad de los eventos y de las consecuencias;

b) la naturaleza y la magnitud de las consecuencias;

c) la complejidad y la interconexión;

d) los factores relacionados con el tiempo y la volatilidad;

e) la eficacia de los controles existentes;

f) los niveles de sensibilidad y de confianza;

g) valorar las consecuencias potenciales que resultarán si se materializan los riesgos identificados en 6.1.3.2 a);

h) valorar la probabilidad realista de que ocurran los riesgos identificados en 6.1.3.2 a); y

i) determinar los niveles de riesgo.

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.

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.

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 tipos y niveles de riesgo.

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:

a) no hacer nada más;

b) considerar opciones para el tratamiento del riesgo;

c) realizar un análisis adicional para comprender mejor el riesgo;

d) mantener los controles existentes;

e) reconsiderar los objetivos.

f) priorizar los riesgos analizados para el tratamiento de los riesgos.

Las decisiones deberían tener en cuenta un contexto más amplio y las consecuencias reales y percibidas por las partes interesadas externas e internas.

Los resultados de la valoración del riesgo se deberían registrar, comunicar y luego validar a los niveles apropiados de la organización.

La organización debe conservar información documentada acerca del proceso de valoración de riesgos del S.I.G.

6.1.4 Tratamiento del riesgo

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.

El tratamiento del riesgo implica un proceso iterativo de:

a) formular y seleccionar opciones apropiadas para el tratamiento del riesgo teniendo en cuenta los resultados de la valoración de riesgos;

b) determinar todos los controles que sean necesarios para implementar las opciones escogidas para el tratamiento de riesgos del S.I.G.;

NOTA Las organizaciones pueden diseñar los controles necesarios, o identificarlos de cualquier fuente.

c) comparar los controles determinados en 6.1.4.1 b) con los del Anexo A (norma NTC-ISO/IEC 27001:2013) y verificar que no se han omitidos controles necesarios;

NOTA 1 El Anexo A (norma NTC-ISO/IEC 27001:2013) 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 Los objetivos de control están incluidos implícitamente en los controles escogidos. Los objetivos de control y los controles enumerados en el Anexo A (norma NTC-ISO/IEC 27001:2013) no son exhaustivos, y pueden ser necesarios objetivos de control y controles adicionales.

d) producir una declaración de aplicabilidad que contenga

1) los controles necesarios (véanse el numeral 6.1.4.1 b) y c));

2) la justificación de las inclusiones;

3) si los controles necesarios están implementados o no; y

4) la justificación para las exclusiones de los controles del Anexo A (norma NTC-ISO/IEC 27001:2013);

e) planificar e implementar un plan de tratamiento de riesgos del S.I.G.;

f) evaluar la eficacia de ese tratamiento;

g) decidir si el riesgo residual es aceptable;

h) si no es aceptable, efectuar tratamiento adicional.

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.

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:

a) evitar el riesgo decidiendo no iniciar o continuar con la actividad que genera el riesgo;

b) aceptar o aumentar el riesgo en busca de una oportunidad;

c) eliminar la fuente de riesgo;

d) modificar la probabilidad;

e) modificar las consecuencias;

f) compartir el riesgo (por ejemplo: a través de contratos, compra de seguros);

g) retener el riesgo con base en una decisión informada.

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.

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.

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 seguimiento y la revisión necesitan ser parte integral de la implementación del tratamiento del riesgo para asegurar que las distintas maneras del tratamiento sean y permanezcan eficaces.

El tratamiento del riesgo a su vez puede introducir nuevos riesgos que necesiten gestionarse.

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.

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.

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 implementar.

Los planes de tratamiento deberían integrarse en los planes y procesos de la gestión de la organización, en consulta con las partes interesadas apropiadas.

La información proporcionada en el plan del tratamiento debería incluir:

a) el fundamento de la selección de las opciones para el tratamiento, incluyendo los beneficios esperados.

b) las personas que rinden cuentas y aquellas responsables de la aprobación e implementación del plan;

c) las acciones propuestas;

d) los recursos necesarios, incluyendo las contingencias;

e) las medidas del desempeño;

f) las restricciones;

g) los informes y seguimiento requeridos;

h) los plazos previstos para la realización y la finalización de las acciones;

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.

La organización debe conservar información documentada acerca del proceso de tratamiento de riesgos del S.I.G.

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.

Los objetivos del S.I.G. deben:

a) ser coherentes con la política del S.I.G.;

b) ser medibles (si es posible);

c) tener en cuenta los requisitos del S.I.G. aplicables, y los resultados de la valoración y del tratamiento de los riesgos;

d) ser comunicados; y

e) ser actualizados, según sea apropiado.

La organización debe conservar información documentada sobre los objetivos del S.I.G.

Cuando se hace la planificación para lograr sus objetivos del S.I.G., la organización debe determinar:

f) lo que se va a hacer;

g) qué recursos se requerirán;

h) quién será responsable;

i) cuándo se finalizará; y

j) cómo se evaluarán los resultados.

7. SOPORTE

7.1 ASIGNACIÓN DE RECURSOS

La alta dirección 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:

a) las personas, las habilidades, la experiencia y las competencias;

b) los procesos, los métodos y las herramientas de la organización a utilizar para gestionar el riesgo;

c) los procesos y procedimientos documentados;

d) los sistemas de gestión de la información y del conocimiento;

e) el desarrollo profesional y las necesidades de formación.

La organización debería considerar las competencias y limitaciones de los recursos existentes.

7.2 COMPETENCIA

La organización debe:

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) asegurarse de que estas personas sean competentes, basándose en la educación, formación o experiencia adecuadas;

c) cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones tomadas; y

d) conservar la información documentada apropiada, como evidencia de la competencia.

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

Las personas que realizan el trabajo bajo el control de la organización deben tomar conciencia de:

a) la política del S.I.G.;

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) las implicaciones de la no conformidad con los requisitos del S.I.G.

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 dé 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.

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 información, así como el derecho a la privacidad de las personas.

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.

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) el contenido de la comunicación;

b) cuándo comunicar;

c) a quién comunicar;

d) quién debe comunicar; y

e) los procesos para llevar a cabo la comunicación.

La comunicación y consulta pretende:

f) reunir diferentes áreas de experiencia para cada etapa del proceso de la gestión del riesgo;

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;

h) proporcionar suficiente información para facilitar la supervisión del riesgo y la toma de decisiones;

i) construir un sentido de inclusión y propiedad entre las personas afectadas por el riesgo.

7.5 INFORMACIÓN DOCUMENTADA

7.5.1 GENERALIDADES

El S.I.G. de la organización debe incluir:

a) la información documentada requerida por esta Norma Integral; y

b) la información documentada que la organización ha determinado que es necesaria para la eficacia del S.I.G.

NOTA El alcance de la información documentada para un S.I.G. puede ser diferente de una organización a otra, debido a:

a) el tamaño de la organización y a su tipo de actividades, procesos, productos y servicios,

b) la complejidad de los procesos y sus interacciones, y

c) la competencia de las personas.

7.5.2 CREACIÓN Y ACTUALIZACIÓN

Cuando se crea y actualiza información documentada, la organización debe asegurarse de que lo siguiente sea apropiado:

a) la identificación y descripción (por ejemplo, título, fecha, autor o número de referencia);

b) el formato (por ejemplo, idioma, versión del software, gráficos) y sus medios de soporte (por ejemplo, papel, electrónico);

c) la revisión y aprobación con respecto a la idoneidad y adecuación.

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:

a) comunicar las actividades de la gestión del riesgo y seguridad de la información, y sus resultados a lo largo de la organización;

b) proporcionar información para la toma de decisiones;

c) mejorar las actividades de la gestión del riesgo y seguridad de la información;

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.

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.

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 informe incluyen, pero no se limitan a:

e) las diferentes partes interesadas, sus necesidades y requisitos específicos de información;

f) el costo, la frecuencia y los tiempos del informe;

g) el método del informe;

h) la pertinencia de la información con respecto a los objetivos de la organización y la toma de decisiones.

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) esté disponible y adecuada para su uso, dónde y cuándo se necesite; y

b) esté protegida adecuadamente (por ejemplo, contra pérdida de la confidencialidad, uso inadecuado, o pérdida de integridad).

Para el control de la información documentada, la organización debe tratar las siguientes actividades, según sea aplicable:

c) distribución, acceso, recuperación y uso;

d) almacenamiento y preservación, incluida la preservación de la legibilidad;

e) control de cambios (por ejemplo, control de versión); y

f) retención y disposición.

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 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

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:

a) el desarrollo de un plan apropiado incluyendo plazos y recursos;

b) la identificación de dónde, cuándo, cómo y quién toma diferentes tipos de decisiones en toda la organización;

c) la modificación de los procesos aplicables para la toma de decisiones, cuando sea necesario;

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.

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 incertidumbre en la toma de decisiones, al tiempo que se asegura que cualquier incertidumbre nueva o subsiguiente se pueda tener en cuenta cuando surja.

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 captaran de manera adecuada.

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.

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.

La organización debe asegurar que los procesos contratados externamente estén controlados.

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.

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

La organización debe implementar el plan de tratamiento de riesgos de la seguridad de la información.

La organización debe conservar información documentada de los resultados del tratamiento de riesgos de la seguridad de la información.

9. EVALUACIÓN DEL DESEMPEÑO

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.

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 parte planificada del proceso de la gestión del riesgo y seguridad de la información, con responsabilidades claramente definidas.

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.

La organización debe determinar:

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) los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos;

NOTA Para ser considerados válidos, los métodos seleccionados deberían producir resultados comparables y reproducibles

c) cuándo se deben llevar a cabo el seguimiento y la medición;

d) quién debe llevar a cabo el seguimiento y la medición;

e) cuándo se deben analizar y evaluar los resultados del seguimiento y de la medición; y

f) quién debe analizar y evaluar estos resultados.

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.

La organización debe conservar información documentada apropiada como evidencia de los resultados del monitoreo y de la medición.

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) es conforme con:

1) los propios requisitos de la organización para su S.I.G.; y

2) los requisitos de esta Norma Integral;

b) está implementado y mantenido eficazmente.

La organización debe:

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) para cada auditoría, definir los criterios y el alcance de ésta;

e) seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría;

f) asegurarse de que los resultados de las auditorías se informan a la dirección pertinente; y

g) conservar información documentada como evidencia de la implementación del programa de auditoría y de los resultados de ésta.

NOTA Para mayor información consultar las normas NTC-ISO 19011 y NTC-ISO 27007

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.

La revisión por la dirección debe incluir consideraciones sobre:

a) el estado de las acciones con relación a las revisiones previas por la dirección;

b) los cambios en las cuestiones externas e internas que sean pertinentes al S.I.G.;

c) retroalimentación sobre el desempeño de la seguridad de la información y gestión del riesgo, incluidas las tendencias relativas a:

1) no conformidades y acciones correctivas;

2) seguimiento y resultados de las mediciones;

3) resultados de la auditoría; y

4) cumplimiento de los objetivos de la seguridad de la información y gestión del riesgo;

d) retroalimentación de las partes interesadas;

e) resultados de la valoración de riesgos y estado del plan de tratamiento de riesgos; y

f) las oportunidades de mejora continúa.

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.

La organización debe conservar información documentada como evidencia de los resultados de las revisiones por la dirección.

10. MEJORA

10.1 NO CONFORMIDADES Y ACCIONES CORRECTIVAS

Cuando ocurra una no conformidad, la organización debe:

a) reaccionar ante la no conformidad, y según sea aplicable

1) tomar acciones para controlarla y corregirla, y

2) hacer frente a las consecuencias;

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) la revisión de la no conformidad

2) la determinación de las causas de la no conformidad, y

3) la determinación de si existen no conformidades similares, o que potencialmente podrían ocurrir;

c) implementar cualquier acción necesaria;

d) revisar la eficacia de las acciones correctivas tomadas, y

e) hacer cambios al S.I.G., si es necesario.

Las acciones correctivas deben ser apropiadas a los efectos de las no conformidades encontradas.

La organización debe conservar información documentada adecuada, como evidencia de:

f) la naturaleza de las no conformidades y cualquier acción posterior tomada; y

g) los resultados de cualquier acción correctiva.

10.2 MEJORA CONTINUA

La organización debe mejorar continuamente la conveniencia, idoneidad, adecuación y eficacia del S.I.G.

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 implementadas, estas mejoras deberían contribuir al fortalecimiento del S.I.G.

ANEXO A - ISO 27001
(Normativo)

OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA

El Anexo A de la norma, puede ser consultado directamente en la norma NTC-ISO/IEC 27001:2013.

3.2 MÓDULO 2: MARCO DE REFERENCIA

3.2.1 Revisión de documentos requeridos por la norma

Después de realizar el documento integrado de las normas NTC-ISO/IEC 27001:2013 e ISO 31000:2018, a continuación, se mencionan los documentos

requeridos para el cumplimiento de la norma Integral, aplicado al cumplimiento de la Ley Estatutaria 1581 de 2012.

Tabla 3–2 Documentos y registros exigidos por la Norma Integral.

CLASIFICACIÓN	DESCRIPCIÓN	NUMERAL
DOCUMENTOS	Establecer el contexto	4.1
	Alcance del S.I.G.	4.3
	Política del S.I.G.	5.2
	Objetivos del S.I.G.	6.2
	Definición de los criterios del riesgo	6.1.2
	Metodología de evaluación y tratamiento de riesgos	6.1.3
	Declaración de aplicabilidad	6.1.4.1 d)
	Plan de tratamiento de riesgo	6.1.4
	Obtener, de parte de los dueños de los riesgos, la aprobación del plan de tratamiento de riesgos	6.1.4.3 i)
	Informe sobre resultados de evaluación de riesgos	7.5.3 Y 8.2
	Informe sobre resultados de tratamiento de riesgos	7.5.3 Y 8.3
	Definición de roles y responsabilidades de seguridad	5.3, A.6.1.1 y A.7.1.2
	Inventario de activos	A.8.1.1
	Uso aceptable de los activos	A.8.1.3
	Política de control de acceso	A.9.1.1
	Política de transferencia de información	A.13.2.1, A.13.2.2, A.13.2.3
	Política de seguridad para proveedores	A.15.1.1
	Procedimiento para gestión de incidentes	A.16.1.5
	Requerimientos legales, regulatorios y contractuales	A.18.1.1
REGISTROS	Registros de formación, habilidades, experiencia y calificaciones	7.2
	Seguimiento y resultados de medición	9.1
	Programa de auditoria interna	9.2
	Resultados de auditorías internas	9.2
	Resultados de la Revisión por Dirección	9.3
	Resultados de acciones correctivas	10.1

Fuente: Elaboración Propia.

3.3 MÓDULO 3: Diseño del Sistema Integrado de Gestión

3.3.1 Evaluación del contexto de la empresa en protección de datos.

Actualmente en la empresa Pavimentaciones Morales S.L Sucursal en Colombia, no se maneja una protección de los datos obtenidos; a continuación, se realiza una descripción de las diferentes áreas que componen el contexto interno y externo de la organización, con relación a la protección de datos.

3.3.1.1 Análisis contexto interno.

El análisis del contexto interno de la sucursal en Colombia, se enfocó en la gestión que se realiza con respecto a la protección de datos personales y las relaciones con la cultura, principios, procesos, comunicaciones y la estructura organizacional.

- **Capacidad Directiva:** actualmente la empresa directivamente está co[redacted] el

Información Reservada.

ad[redacted]

- **Capacidad Competitiva:** Considerando que la competitividad es uno de [redacted]

Información Reservada.

[redacted]

Otros aspectos relevantes a tener en cuenta referente a la protección de datos en la empresa internamente, son:

- Información Reservada.

- **Capacidad Financiera:** Teniendo en cuenta que el pasado 19 de enero de 2018 la SIC Superintendencia de Industria y Comercio) expidió el Decreto

Información Reservada.

- **Capacidad Tecnológica:** Actualmente la sucursal no cuenta con tecnología referente a protección de datos.

- **Capacidad Del Talento Humano:** Actualmente en la sucursal, se cuenta

Información Reservada.

Información Reservada.

Según lo anterior las actividades subcontratadas serán analizadas en el contexto externo.

3.3.1.2 Análisis contexto externo.

El análisis del contexto externo de la sucursal en Colombia, se realizó en relación de las áreas subcontratadas, socios de los consorcios y ámbito jurídico, con respecto a la gestión que se realiza de protección de datos personales, de los documentos que la empresa les entrega.

- **Ámbito Socio-Cultural:** Actualmente en el sector, con las empresas con la[illegible]s re[illegible]

Información Reservada.

- **Servicios Contratados:** Como se mencionó en el análisis del contexto interno, las áreas como asesoría jurídica, contabilidad y revisoría fiscal, son áreas que no son manejadas o controladas por la empresa, a lo cual se realiza una descripción de estas áreas y cómo funciona la transferencia de datos entre las mismas:

  - **Área contable:** Con respecto a esta área, todos los documentos

Información Reservada.

- **Ámbito Legal:** Con respecto al ámbito legal en relación a protección de datos, aplica ley 1581 de 2012, modificada recientemente por el Decreto el pasado 19 de enero de 2018 por la SIC Superintendencia de Industria y Comercio); el cual como se mencionó anteriormente se redujo la población obligada a registrar las bases de datos ante la SIC, exigiendo este registro únicamente a las sociedades y entidades sin ánimo de lucro que sus activos superen los 100.000 UVT, teniendo plazo para cumplimiento de la Ley hasta el 30 de septiembre de 2018, el no cumplimiento de la Ley, puede acarrearle a la empresa multas hasta de 2.000 SMMLV.

3.3.2 Requisitos legales y contractuales

La matriz elaborada con las especificaciones de los requisitos legales aplicables, se encuentra en el Anexo B "Matriz legal aplicable de protección de datos personales".

3.3.3 Alcance

El Alcance del S.I.G. NTC-ISO/IEC 27001:2013 e ISO 31000:2018 de la organización Pavimentaciones Morales S.L. Sucursal en Colombia, aplica únicamente al cumplimiento de la protección de datos personales según Ley Estatutaria 1581 de 2012, "Por la cual se dictan disposiciones generales para la protección de datos personales", en el área administrativa de la empresa en Colombia.

3.3.4 Política

Teniendo en cuenta el alcance del S.I.G., la política se encuentra establecida para la protección de datos personales. De acuerdo a los requerimientos de la Ley Estatutaria 1581 de 2012, la política está basada en el modelo establecido por la S.I.C, en su "Guía de Formatos Modelo para El Tratamiento de Datos Personales -Ley 1581 De 2012", en el que se encuentran párrafos literales al modelo, e inclusiones para dar cumplimiento a la Norma Integral.

POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

Pavimentaciones Morales S.L. Sucursal en Colombia, sociedad comercial legalmente constituida el 20 de enero de 2012, identificada con el NIT 900.492.601-1, y matricula comercial No. 02174189, es una empresa dedicada a la construcción de carreteras y vías férreas con domicilio principal en la Carrera 47 A # 95 – 56 Oficina 605, de la ciudad de Bogotá D.C, Colombia.

Pavimentaciones Morales S.L. Sucursal en Colombia, siendo el responsable de la protección de datos personales en la empresa, está comprometida con el cumplimiento de la norma Integrada y la legislación vigente. Así mismo está comprometida con la mejora continua del S.I.G.

OBJETIVO:

Establecer los criterios para la recolección, almacenamiento, uso, circulación, supresión y gestión de los riesgos, de los datos personales tratados por ***Pavimentaciones Morales S.L. Sucursal en Colombia***.

ALCANCE:

Esta política aplica para toda la información personal (proveniente de postulantes, colaboradores, proveedores, clientes, socios y accionistas) registrada en las bases de datos de ***Pavimentaciones Morales S.L. Sucursal en Colombia,*** quien actúa en calidad de responsable del tratamiento de los datos personales.

TRATAMIENTO Y FINALIDAD:

El tratamiento que realizará ***Pavimentaciones Morales S.L. Sucursal en Colombia*** con la información personal será el siguiente:

La recolección, almacenamiento, uso, circulación, supresión y gestión de los riesgos, para temas de misión licitatoria, contractual, contable, financiera, fiscal y de recursos humanos.

TRATAMIENTO DE DATOS SENSIBLES:

Los datos sensibles recolectados serán tratados con las siguientes finalidades:

- Gestión contable, fiscal y administrativa - Gestión fiscal
- Recursos humanos - Formación de personal
- Recursos humanos - Prestaciones sociales
- Recursos humanos - Prevención de riesgos laborales
- Recursos humanos - Promoción y selección de personal

CONTROL DE ACCESO:

El Control de acceso a las bases de datos y tratamiento de los mismos estará únicamente a cargo de ***Pavimentaciones Morales S.L. Sucursal en Colombia*** como responsable del tratamiento de datos y la persona encargada del tratamiento de los datos dentro de la organización.

TRANSFERENCIA Y/O TRANSMISIÓN DE DATOS A PROVEEDORES, SUBCONTRATISTAS Y SOCIOS Y CONFIDENCIALIDAD DE LOS MISMOS:

Tanto los proveedores, subcontratistas y socios, deben garantizar el tratamiento y protección de datos suministrados por **Pavimentaciones Morales S.L. Sucursal en Colombia**, dando cumplimiento al Art. 2.2.2.25.5.2 del Decreto Único Reglamentario 1074 de 2015, y artículo 26 de la Ley 1581 de 2012. Acoplándose a los procedimientos de la organización en caso de requerir documentación que haga parte de los activos de la empresa, garantizando el buen uso y finalidad de los mismos.

El incumplimiento del Art 2.2.2.25.5.2 del Decreto Único Reglamentario 1074 de 2015, artículo 26 de la Ley 1581 de 2012 y/o la finalidad por lo cual se solicita un documento será considerado como falta grave, que podrá dar lugar a:

- sanciones, teniendo en cuenta los daños (multas, sanciones, cierre, etc.) que se pueden ocasionar, por parte de las autoridades competentes, y/o

- terminación de la relación contractual, sin perjuicio de las acciones legales adicionales a que haya lugar.

DERECHOS DE LOS TITULARES:

Como titular de sus datos personales Usted tiene derecho a:

(i) Acceder de forma gratuita a los datos proporcionados que hayan sido objeto de tratamiento.

(ii) Conocer, actualizar y rectificar su información frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté prohibido o no haya sido autorizado.

(iii) Solicitar prueba de la autorización otorgada.

(iv) Presentar ante la Superintendencia de Industria y Comercio (SIC) quejas por infracciones a lo dispuesto en la normatividad vigente.

(v) Revocar la autorización y/o solicitar la supresión del dato, siempre que no exista un deber legal o contractual que impida eliminarlos.

(vi) Abstenerse de responder las preguntas sobre datos sensibles. Tendrá carácter facultativo las respuestas que versen sobre datos sensibles o sobre datos de las niñas y niños y adolescentes.

ATENCIÓN DE PETICIONES, CONSULTAS Y RECLAMOS:

El área de administración, es la dependencia que tiene a cargo dar trámite a las solicitudes de los titulares para hacer efectivos sus derechos.

Los datos de contacto, son los mencionados a continuación:

Domicilio principal y dirección de correspondencia: Carrera 47 A # 95 – 56 Oficina 605. Bogotá D.C.
Teléfono: (571) 8059532.

PROCEDIMIENTO PARA EL EJERCICIO DEL DERECHO DE HABEAS DATA:

En cumplimiento de las normas sobre protección de datos personales, ***Pavimentaciones Morales S.L. Sucursal en Colombia*** presenta el procedimiento y requisitos mínimos para el ejercicio de sus derechos:

Para la radicación y atención de su solicitud le solicitamos suministrar la siguiente información:

- ✓ Nombre completo y apellidos.
- ✓ Datos de contacto (Dirección física y/o electrónica y teléfonos de contacto).
- ✓ Medios para recibir respuesta a su solicitud.
- ✓ Motivo(s)/hecho(s) que dan lugar al reclamo con una breve descripción del derecho que desea ejercer (conocer, actualizar, rectificar, solicitar prueba de la autorización otorgada, revocarla, suprimir, acceder a la información).
- ✓ Firma (si aplica) y número de identificación.

El término máximo previsto por la ley para resolver su reclamación es de quince (15) días hábiles, contado a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, ***Pavimentaciones Morales S.L. Sucursal en Colombia*** informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

Una vez cumplidos los términos señalados por la Ley 1581 de 2012 y las demás normas que la reglamenten o complementen, el Titular al que se deniegue, total o parcialmente, el ejercicio de los derechos de acceso, actualización, rectificación, supresión y revocación, podrá poner su caso en conocimiento de la Superintendencia de Industria y Comercio –Delegatura para la Protección de Datos Personales-.

VIGENCIA:

La presente Política para el Tratamiento de Datos Personales rige a partir del 01 de agosto de 2018.

Las bases de datos en las que se registrarán los datos personales tendrán una vigencia igual al tiempo en que se mantenga y utilice la información para las finalidades descritas en esta política. Una vez se cumpla(n) esa(s) finalidad(es) y siempre que no exista un deber legal o contractual de conservar su información, sus datos serán eliminados de nuestras bases de datos.

Esta política es de obligatorio y estricto cumplimiento para ***Pavimentaciones Morales S.L. Sucursal en Colombia.***

_____
Representante Legal.
Pavimentaciones Morales S.L. Sucursal en Colombia.

3.3.5 Objetivos del S.I.G.

Teniendo en cuenta el análisis de los riesgos, y el nivel de riesgo hallado, se establecerá principalmente el siguiente objetivo para el Sistema Integrado de gestión:

1. Reducir en un sesenta porciento (60%) el nivel promedio de los riesgos, durante el primer mes de ejecución del mismo, a través del control del 61% de las principales amenazas (falta de conocimiento en la normatividad aplicable, la entrega de información en original a entidades o personas externas y los ataques cibernéticos), con el fin de evitar consecuencias legales.

NOTA. Se selecciona el 60% de reducción en el nivel promedio de los riesgos, dado que al tratar y controlar el 61% de las amenazas, se mitiga que se materialice el 80% de los riesgos críticos. Este análisis puede ser consultado en el Anexo C. en su pestaña Análisis riesgos y amenazas.

3.3.6 Definición de roles, competencia y responsabilidades.

Para el desarrollo del S.I.G, teniendo en cuenta el alcance del mismo, se definen los siguientes roles, competencias y responsabilidades.

3.3.6.1 Roles.

Los roles necesarios para el cumplimiento de la norma integral y teniendo en cuenta lo establecido en La ley 1581 de 2012, son:

> **Responsable del Tratamiento:** Persona natural o jurídica que toma las decisiones con respecto al tratamiento de los datos.
>
> **Encargado del Tratamiento:** Persona(s) natural(es) o jurídica, que, a través de delegación por el Responsable del tratamiento, realiza únicamente la ejecución del tratamiento de los datos.

3.3.6.2 Competencia

Es importante que tanto el Responsable como el Encargado tengan conocimientos acerca de:

- ✓ Legislación de protección de datos.
- ✓ Tener conocimientos y/o haber manejado norma ISO 27001 y norma ISO 31000.
- ✓ Tener los conocimientos para la ejecución y monitoreo del S.I.G.

Como evidencia de lo anterior, se deben conservar los soportes de las competencias establecidas y/o el registro de capacitaciones para adquirir los conocimientos y competencias necesarias.

3.3.6.3 Responsabilidades:

Dando cumplimiento a la normatividad aplicable a protección de datos, se menciona literalmente los artículos que establecen los deberes del responsable y encargado de tratamiento de datos personales:

> **ARTÍCULO 17. Deberes de los Responsables del Tratamiento.** Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular.

c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.

d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.

f) Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a éste se mantenga actualizada.

g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.

h) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley.

i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.

j) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley.

k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos.

l) Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.

m) Informar a solicitud del Titular sobre el uso dado a sus datos.

n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Adicionalmente a los deberes establecidos por la Ley 1581 de 2012. El responsable del tratamiento de datos debe:

p) informar a la alta dirección sobre el desempeño del S.I.G.

a) Dar cumplimiento a los Procedimientos y Formatos establecidos por la organización (Ver Anexo E. Procedimientos y Formatos para protección de datos personales).

ARTÍCULO 18. Deberes de los Encargados del Tratamiento. Los Encargados del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

b) Garantizar al Titular, en todo momento, el pleno y efectivo ejercicio del derecho de hábeas data.

c) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración. pérdida, consulta, uso o acceso no autorizado o fraudulento.

d) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley.

e) Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo.

f) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente ley.

g) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los Titulares.

h) Registrar en la base de datos la leyenda "reclamo en trámite" en la forma en que se regula en la presente ley.

i) Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.

j) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.

k) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.

l) Informar a la Superintendencia de Industria y Comercio cuando se le presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

m) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Adicionalmente a los deberes establecidos por la Ley 1581 de 2012. El encargado del tratamiento de datos debe:

n) Informar al responsable del tratamiento de datos sobre el desempeño del S.I.G.

o) Dar cumplimiento a los Procedimientos y Formatos establecidos por la organización (Ver Anexo E. Procedimientos y Formatos para protección de datos personales).

3.3.7 Identificación de activos.

Para proceder con la identificación de los activos, es importante definir las clases de datos personales que están establecidas en Colombia.

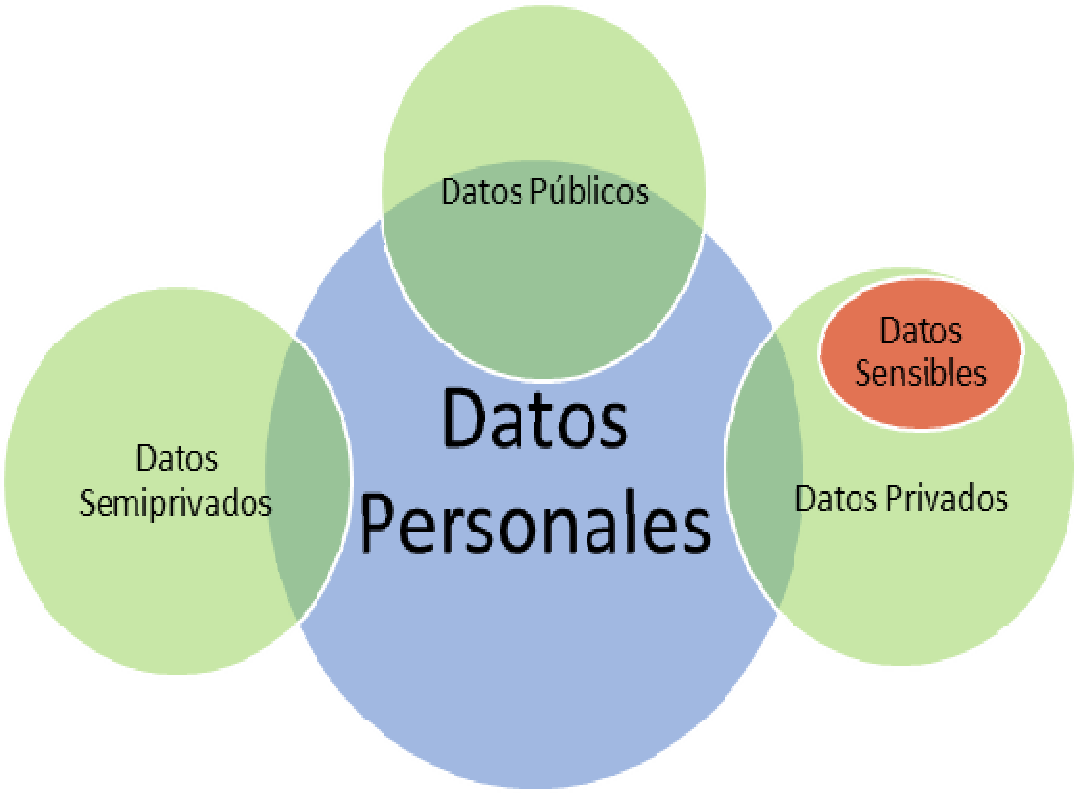
Para temas legales y para no generar contrariedad en la definición de los términos de la clasificación de los datos personales, se tomará textualmente de la normatividad colombiana, la definición de los diferentes tipos de datos.

De acuerdo con La Ley 1266 de 2008, se definen los siguientes tipos de datos:

> **Dato personal:** "Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente ley se haga referencia a un dato, se presume que se trata de uso personal. Los datos personales pueden ser públicos, semiprivados o privados".
>
> **Dato público:** "Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas".
>
> **Dato semiprivado:** "Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la presente ley".
>
> **Dato privado: "**Es el dato que por su naturaleza íntima o reservada solo es relevante para el titular".

En Ley Estatutaria 1581 de 2012 se establece la definición de **datos sensibles** como "aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos".

Figura 3–3 Clasificación de Datos Personales.



Fuente: Elaboración Propia.

Posterior al conocimiento previo de la clasificación de datos personales en Colombia, se procede a identificar los activos de empresa.

Los diferentes activos de Información que son manejados en la empresa son: Información Física e Información Digital. Teniendo en cuenta la descripción de la clase datos personales (ver Figura 3-3 Clasificación de Datos Personales), en la Tabla 3-3, se realiza la representación de los activos que se tienen de forma física como digital con relación a datos personales.

Tabla 3–3 Identificación y Clasificación de Activos.

CLASIFICACIÓN DE DATOS PERSONALES	DESCRIPCIÓN DEL DATO	OBTENCIÓN DEL DATO	TIPO DE INFORMACIÓN		REQUIERE AUTORIZACIÓN PARA TRATAMIENTO?	RESPONSABLE DEL TRATAMIENTO
			FÍSICA	DIGITAL		
DATOS PÚBLICOS	Número de celular empresarial	➢ Tarjetas de presentación	✓	✓		Encargado del tratamiento de datos.
		➢ Correos electrónicos.		✓		
		➢ Suministro verbal.				
	Número de teléfono fijo empresarial	➢ Tarjetas de presentación	✓	✓		Encargado del tratamiento de datos.
		➢ Correos electrónicos.		✓		
		➢ Suministro verbal.				
	Correos empresariales	➢ Tarjetas de presentación	✓	✓		Encargado del tratamiento de datos.
		➢ Correos electrónicos.		✓		
		➢ Suministro verbal.				
	Dirección empresarial	➢ Tarjetas de presentación	✓	✓		Encargado del tratamiento de datos.
		➢ Correos electrónicos.		✓		
		➢ Suministro verbal.				
	Profesión	➢ Hoja de vida.	✓	✓		Encargado del tratamiento de datos.
		➢Contrato laboral	✓	✓		
		➢ Copia tarjeta profesional	✓	✓		
	Números de identificación	➢ Hoja de vida.	✓	✓		Encargado del tratamiento de datos.
		➢Contrato laboral	✓	✓		
		➢ Copia cédula de ciudadanía	✓	✓		
		➢ Copia tarjeta profesional	✓	✓		
	Nombre Completo	➢ Hoja de vida.	✓	✓		Encargado del tratamiento de datos.
		➢Contrato laboral	✓	✓		
		➢ Copia cédula de ciudadanía.	✓	✓		
		➢ Copia tarjeta profesional	✓	✓		
		➢ Tarjetas de presentación	✓	✓		
		➢ Correos electrónicos.	✓	✓		
		➢ Suministro verbal.	✓	✓		
	Lugar y fecha de expedición del documento de identificación	➢ Hoja de vida.	✓	✓		Encargado del tratamiento de datos.
		➢ Copia cédula de ciudadanía.	✓	✓		
DATOS SEMIPRIVADOS	Números de cuentas bancarias de los colaboradores	➢ Cuentas de Cobro.	✓	✓	✓	Encargado del tratamiento de datos.
		➢ Certificaciones Bancarias.	✓	✓	✓	
		➢ correos con datos bancarios.	✓	✓	✓	
	Fecha y lugar de nacimiento	➢ Copia cédula de ciudadanía.	✓	✓	✓	Encargado del tratamiento de datos.
DATOS PRIVADOS	Correos electrónicos personales	➢ Hoja de vida.	✓	✓	✓	Encargado del tratamiento de datos.
		➢Contrato laboral	✓	✓	✓	
		➢ correos con información.	✓	✓	✓	
	Dirección de Residencia	➢ Cuentas de Cobro.	✓	✓	✓	Encargado del tratamiento de datos.
		➢Contrato laboral	✓	✓	✓	
	Número de celular personal	➢ Hoja de vida.	✓	✓	✓	Encargado del tratamiento de datos.
		➢Contrato laboral	✓	✓	✓	
	Número de teléfono fijo	➢ Hoja de vida.	✓	✓	✓	Encargado del tratamiento de datos.
		➢Contrato laboral	✓	✓	✓	
	Fotografía	➢ Hoja de vida.	✓	✓	✓	Encargado del tratamiento de datos.
		➢ Copia cédula de ciudadanía	✓	✓	✓	
		➢ Copia tarjeta profesional	✓	✓	✓	
DATOS SENSIBLES	Datos biométricos	➢ Copia cédula de ciudadanía	✓	✓	✓	Encargado del tratamiento de datos.

Fuente: Elaboración Propia.

3.3.8 Uso aceptable de los activos

La disposición y adecuado uso de los activos están destinados únicamente para las siguientes finalidades, teniendo en cuenta las personas autorizadas para el acceso y disposición de los mismos.

Finalidades de los activos:

- Gestión contable, fiscal y administrativa; en procesos de gestión de cobros, pagos, facturación, clientes, proveedores.
- Gestión administrativa; Gestión de nómina, procedimientos bancarios.
- Recursos humanos; Promoción, Selección y formación de personal, contratación, trabajo temporal, prestaciones sociales, prevención de riesgos laborales.
- Socio – Cultural; gestión licitatoria y contractual.

3.3.9 Definición de metodología de evaluación y tratamiento de riesgos.

Teniendo en cuenta la Norma Integral, la metodología diseñada para la evaluación y tratamiento de los riesgos para los datos personales, constará de tres fases, que se mencionan a continuación.

Fase 1:

1. Definición de los criterios del riesgo.

Fase 2: Evaluación del riesgo

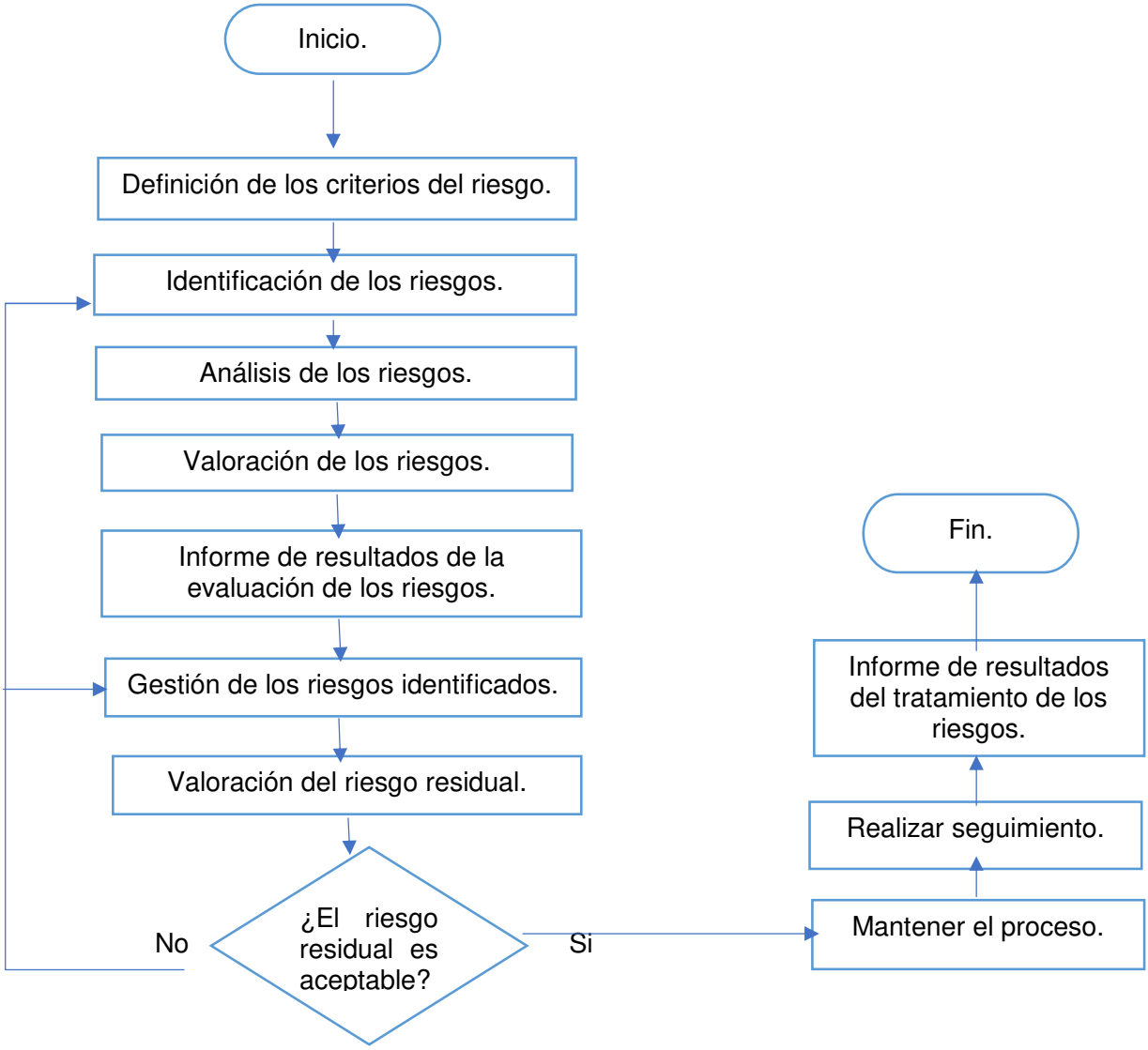
2. Identificación de los riesgos.
3. Análisis de los riesgos.
4. Valoración del riesgo.
5. Informe de resultado de evaluación de riesgos.

Fase 3: Tratamiento del riesgo

6. Autorización del titular para el tratamiento de datos.
7. Gestión de los riesgos identificados.
8. Valoración del riesgo residual.
9. Informe de resultado de tratamiento de riesgos.

NOTA. Cada una de las fases se explicará con el desarrollo de la metodología.

Figura 3–4 Diagrama de flujo de metodología de evaluación y tratamiento de datos personales.



Fuente: Elaboración Propia.

En el Apéndice A, se propone una matriz formulada para la evaluación y tratamiento de los riesgos de los datos personales.

3.3.10 Definición de los criterios del riesgo.

Los criterios de riesgos establecidos como aceptables, serán únicamente los riesgos que, al ser valorados, su nivel sea bajo y las consecuencias no generan violación a la privacidad de los datos personales.

3.3.11 Evaluación de los riesgos.

3.3.11.1 Identificación de los riesgos.

Teniendo en cuenta el contexto de la empresa analizado anteriormente y el inventario de datos que se maneja en la organización, se procede a realizar la identificación de riesgos a los que se encuentra expuesta la información.

En la cual se identifica la fuente, las amenazas y los riesgos que se pueden generar si se materializa la amenaza.

A continuación, se realiza la definición de los elementos que se deben analizar en esta fase:

- **Fuente:** Espacio en el que se está originando la amenaza, puede ser externo o interno.

- **Amenaza:** Situación, acto y/o elemento capaz de alterar la protección de los datos personales, dando origen a los riesgos.

- **Riesgo:** Efectos negativos que se pueden generar si la amenaza se materializa.

De acuerdo a la matriz propuesta para evaluación y tratamiento de los riesgos, en el Anexo C, se realiza la identificación de los riesgos.

3.3.11.2 Análisis de los riesgos.

En esta fase de la evaluación del riesgo, se analiza:

- Si existen controles para los riesgos anteriormente identificados.

- En cada de ser positivo el ítem anterior, especificar que controles existen.

- Determinar cuantitativamente el nivel de probabilidad que se materialice el riesgo.

- Determinar cuantitativamente el nivel de consecuencia si se materializa el riesgo.

- Calcular el nivel del riesgo.

Entiéndase como:

- **Probabilidad:** Posibilidad que el riesgo suceda, dependiendo de la frecuencia con la que se repite la amenaza.

- **Consecuencia:** Grado de perjuicio que se puede generar si el riesgo se materializa.

- **Nivel de Riesgo:** nivel de probabilidad que se materialice el riesgo por el nivel de consecuencia si el riesgo se materializa.

A continuación, se definen las escalas determinadas para el desarrollo del análisis de los riesgos:

- Escala de valores para el cálculo de la probabilidad:

  Probabilidad baja: La frecuencia con la que se presenta la amenaza es poco recurrente, por lo tanto, la posibilidad que se materialice el riesgo es mínima. Su valoración cuantitativa es 1.

  Probabilidad media: La frecuencia con la que se presenta la amenaza es recurrente, por lo tanto, la posibilidad que se materialice el riesgo es media. Su valoración cuantitativa es 2.

  Probabilidad alta: La frecuencia con la que se presenta la amenaza es muy recurrente, por lo tanto, la posibilidad que se materialice el riesgo es alta o muy elevada. Su valoración cuantitativa es 3.

- Escala de valores para el cálculo de la consecuencia:

  Consecuencia baja: El nivel de perjuicio que se puede generar es mínimo, y su impacto no generaría consecuencias. Su valoración cuantitativa es 1.

  Consecuencia media: Se puede generar perjuicios, y su impacto puede ocasionar sanciones legales. Su valoración cuantitativa es 2.

  Consecuencia alta: El nivel de perjuicio que se puede generar es elevado, y su impacto puede ocasionar el cierre de la empresa. Su valoración cuantitativa es 3.

- Nivel del riesgo:

  El nivel del riesgo se determinará con la siguiente matriz de calor:

Tabla 3–4 Matriz de nivel del riesgo

			NIVEL DE CONSECUENCIA		
			BAJA 1	**MEDIA** 2	**ALTA** 3
NIVEL DE PROBABILIDAD	**BAJO**	1	1	2	3
	MEDIO	2	2	4	6
	ALTO	3	3	6	9

Fuente: Elaboración Propia.

Tabla 3–5 Definición de los niveles del riesgo.

1	**MÍNIMO**	Continuar con las medidas de control implementadas, y en lo posible establecer mejoras. Es importante realizar seguimiento para comprobar la aceptabilidad del riesgo.
2-4	**SIGNIFICATIVO**	Se deben tomar medidas de control, y realizar seguimiento periódico con frecuencia.
6-9	**CRÍTICO**	Se deben tomar medidas de control inmediatas y con prioridad, es importante realizar seguimiento con frecuencia alta.

Fuente: Elaboración Propia.

De acuerdo a la matriz propuesta para evaluación y tratamiento de los riesgos, en el Anexo C, se realiza el análisis de riesgos a los que se encuentra expuesta la información.

3.3.11.3 Valoración de los riesgos.

En la valoración del riesgo se realiza el siguiente procedimiento:

- Se describe el valor cualitativo del nivel del riesgo (ver Tabla 3-4).
- Determinar si el riesgo es aceptable o no, teniendo en cuenta el criterio de aceptabilidad del riesgo comparado con el nivel del riesgo.
- Decidir qué medidas se deben tomar con el riesgo (si se debe tomar medidas con prioridad, si es necesario realizar un análisis adicional, si se debe mantener los controles).

De acuerdo a la matriz propuesta para evaluación y tratamiento de los riesgos, en el Anexo C, se realiza la valoración de los riesgos.

3.3.11.4 Informe de resultado de evaluación de riesgos.

Es importante que la gestión realizada en la evaluación de riesgos, quede documentada. A lo cual se establece que:

- La frecuencia de la presentación de informes a la alta dirección se realizará mensualmente.
- El lenguaje de comunicación, debe ser lo más sencillo y claro posible, permitiendo la comprensión del mismo.
- La revisión de los informes por parte de la alta dirección, se debe analizar mensualmente en las reuniones directivas.
- En la revisión mensual por parte de la dirección, se deben tomar decisiones con respecto a las conclusiones del informe, así mismo se debe realizar el seguimiento a las decisiones tomadas de los informes anteriores.

Se debe conservar evidencia de lo anterior.

NOTA. Teniendo en cuenta la frecuencia de presentación y revisión del informe, se debe presentar un solo informe en el cual también se comunique acerca de la gestión del tratamiento de los riesgos.

3.3.12 Tratamiento de los riesgos.

3.3.12.1 Autorización del titular para el tratamiento de datos.

Es importante contar con la autorización por parte del titular (cuando se requiera autorización) para proceder con el tratamiento de los datos y la aceptación de los riesgos residuales. El formato para solicitar autorización puede ser verificado en el Anexo E. Procedimientos y Formatos para protección de datos personales.

3.3.12.2 Gestión de los riesgos identificados.

En la gestión de los riesgos, se realiza el siguiente procedimiento:

- Describir las medidas de control propuestas para cada uno de los riesgos identificados y valorados.
- Determinar los recursos necesarios.
- Determinar la frecuencia de seguimiento que se debe realizar, a la implementación de las medidas de control propuestas.
- Después de implementar los controles necesarios y establecidos se debe evaluar nuevamente el nivel del riesgo. A lo que se catalogara este valor como nivel del riesgo residual.

De acuerdo a la matriz propuesta para evaluación y tratamiento de los riesgos, en el Anexo C, se realiza las medidas de control y los elementos necesarios para la gestión de los riesgos identificados.

3.3.12.3 Declaración de aplicabilidad.

Con base a los riesgos evaluados, la declaración de aplicabilidad puede ser consultada en el Anexo F.

3.3.12.4 Valoración del riesgo residual.

La valoración del riesgo residual, está comprendido por el siguiente proceso:

- Se describe el valor cualitativo del nivel del riesgo residual (ver Tabla 3-4).
- Determinar si el riesgo es aceptable o no, teniendo en cuenta el criterio de aceptabilidad del riesgo comparado con el nivel del riesgo.

- Decidir qué medidas se deben tomar con el riesgo (si se debe tomar medidas con prioridad, si es necesario realizar un análisis adicional, si se debe mantener los controles).

- Determinar la frecuencia de seguimiento que se debe realizar, a la implementación de las medidas de control propuestas.

- Determinar el responsable de la identificación y actualización de los riesgos, e implementación del tratamiento.

De acuerdo a la matriz propuesta para evaluación y tratamiento de los riesgos, en el Anexo C, se encuentra la opción para realizar la valoración de los riesgos residuales.

3.3.12.5 Informe de resultado de evaluación de riesgos.

Es importante que la gestión realizada en el tratamiento de riesgos, quede documentado. A lo cual se establece que:

- La frecuencia de la presentación de informes a la alta dirección se realizará mensualmente.

- El lenguaje de comunicación, debe ser lo más sencillo y claro posible, permitiendo la comprensión del mismo.

- La revisión de los informes por parte de la alta dirección, se debe analizar mensualmente en las reuniones directivas.

- En la revisión mensual por parte de la dirección, se deben tomar decisiones con respecto a las conclusiones del informe, así mismo se debe realizar el seguimiento a las decisiones tomadas de los informes anteriores.

Se debe conservar evidencia de lo anterior.

NOTA. Teniendo en cuenta la frecuencia de presentación y revisión del informe, se debe presentar un solo informe en el cual también se comunique acerca de la gestión de la valoración de los riesgos.

A continuación, se establecen los ítems mínimos que debe contener el informe de evaluación y tratamiento de riesgos:

1. Fecha de presentación.
2. Periodo que abarca el informe.

3. Introducción (resumen ejecutivo).
4. Análisis por parte de la dirección con respecto al informe anterior, y gestión del mismo.
5. Identificación de riesgos.
6. Nivel del riesgo.
7. Decisión adoptada para cada riesgo y medidas propuestas.
8. Riesgos residuales.
9. Análisis y conclusiones.
10. Nombre y cargo de quien elaboró, revisó y aprobó.

3.3.13 Evaluación del desempeño.

3.3.13.1 Seguimiento, medición y análisis.

Se realizará seguimiento y medición a:

- El tratamiento de los riesgos:

  De acuerdo a la matriz propuesta para evaluación y tratamiento de los riesgos, en el Anexo C, se realiza el indicador de gestión para evaluar el desempeño de la gestión de los riesgos tratados, así como la meta propuesta mensual dependiendo del nivel del riesgo residual.

  El proceso para la evaluación del desempeño de los riesgos, se describe a continuación:

  - La frecuencia con la que se realizará el seguimiento será mensual.
  - Definir el indicador de gestión, para calcular el desempeño de reducción de los riesgos.
  - Definir la meta de cumplimiento que se quiere lograr en máximo un semestre de ejecución.
  - Realizar el análisis del periodo que se esta estudiando (el mes de ejecución), según el % de cumplimiento del indicador con respecto a la meta.
  - Realizar resumen del promedio de cumplimiento del indicador y el seguimiento, con respecto a los periodos anteriores (en cas que aplique).

- Realizar análisis final del seguimiento; teniendo en cuenta el análisis del periodo actual y el análisis de los periodos anteriores.

La matriz se debe realizar mensualmente y conservar como registro para verificar el avance del desempeño.

- Los objetivos del S.I.G.

  En el Anexo D, se encuentra la ficha técnica de indicadores de gestión para los objetivos S.I.G. (modelo suministrado en el desarrollo académico de la especialización).

  Se debe conservar registro del seguimiento y alcance del objetivo..

3.3.13.2 Auditoria Interna.

Teniendo en cuenta que la auditoria es la referencia del seguimiento y diagnóstico de acciones preventivas y correctivas al S.I.G, y una herramienta para la toma de decisiones que promueve la mejora continua del sistema. Es importante determinar:

1. La frecuencia con la que se realizarán las auditorias: Teniendo en cuenta los niveles del riesgo, es importante que la primera auditoria se realice a los seis meses después de implementar el S.I.G., posteriormente realizar las auditorias con una frecuencia anual.

2. Definir el alcance y objetivos de la auditoria.

3. Seleccionar el equipo auditor.

4. La metodología a implementar para el desarrollo de la misma.

5. Los responsables.

6. El informe, con el resultado de hallazgos, el análisis de las fortalezas y debilidades del S.I.G. y las conclusiones.

Se debe conservar como información documentada:

- Resultados de auditorías internas.

- Resultados de la Revisión por Dirección.

- Resultados de acciones correctivas.

3.3.13.3 Revisión por la dirección.

Teniendo en cuenta que al igual que la auditoria, la revisión por la dirección también es una herramienta de gran valor para garantizar la eficacia del S.I.G., y en caso de ser necesario realizar cambios para la mejora del sistema. A lo cual es importante determinar:

1. La frecuencia con la que se realizarán las revisiones: Las revisiones del S.I.G., se alinearán con las reuniones mensuales directivas.

2. Aspectos a tener en cuenta, para la revisión:

   2.1 Observaciones, gestión y resultados de las revisiones anteriores.
   2.2 Resultados de la evaluación de los riesgos.
   2.3 Resultados del tratamiento de los riesgos.
   2.4 Resultado de los indicadores de gestión de los riesgos.
   2.5 Revisión de los objetivos y el grado de cumplimiento alcanzado.
   2.6 Revisión de solicitudes o quejas por parte de los titulares, las decisiones tomadas y su estado.
   2.7 Revisión de incidentes, las decisiones tomadas y su estado.
   2.8 Acciones correctivas y preventivas sobre el S.I.G.
   2.9 Resultados de auditorías internas y/o externas.

3. Teniendo en cuenta las revisiones anteriores, determinar el análisis general del sistema, las acciones a tomar para la mejora del S.I.G., los recursos necesarios y en caso de requerirse los cambios en el S.I.G.

Se debe conservar las actas de reuniones de revisión por parte de la dirección.

4. CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

La principal conclusión generada es que, con el diseño del modelo integrado de gestión, se concluye que la organización puede mitigar, controlar o eliminar los riesgos expuestos a los que están sometidos los datos personales en la compañía, a través del Sistema Integrado de Gestión de las normas NTC-ISO/IEC 27001:2013 e ISO 31000:2018, mitigando y evitando a un nivel máximo las medidas sancionarías por parte de la(s) entidad(es) reguladoras de la Ley 1581 de 2012.

Debido a que con el diseño de la norma integrada de las normas NTC-ISO/IEC 27001:2013 e ISO 31000:2018; se genera una norma muy completa para la protección de datos y en general la seguridad de la información, gracias a que mientras con la norma ISO 31000:2018 se evalúan y tratan los riesgos, con la norma NTC-ISO/IEC 27001 se generan los controles.

Por último, se concluye que es de vital importancia tener un buen y consolidado conocimiento, respecto a amenazas y riesgos con el fin que la evaluación de los mismos sea objetiva y no subjetivamente.

4.2 RECOMENDACIONES

1. Es muy importante que la empresa tenga en cuenta que el Decreto Único Reglamentario 1074 de 2015, se encuentran los estándares y amplia información acerca de los requerimientos de la Ley estatutaria 1581 de 2012.

2. Se le recomienda a la empresa realizar una inversión en infraestructura tecnológica, para tener un mayor control en la protección de los datos. Dado que a través de un servidor y por medio de accesos VPN (Virtual Access Network) se establece el acceso a usuarios específicos, mitigando grandemente el acceso no autorizado.

Bibliografía

Congreso de la Republica. (2012). Ley Estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Publicado *Diario Oficial No.* 48.587, del 18 de octubre de 2012. Colombia.

Ministerio de Comercio, Industria y Turismo. Decreto Único Reglamentario 1074 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Publicado *Diario Oficial No.* 49523, del 26 de mayo de 2015. Colombia.

Constitución Política de Colombia. 1991

NTC-ISO-IEC 27001:2013, *Tecnología de la Información. Técnicas de seguridad. Gestión del riesgo en la seguridad de la información*. Instituto Colombiano de Normas Técnicas y Certificación. Bogotá. ICONTEC. 2013.

ISO 31000:2018. *Gestión del Riesgo - Directrices* (2a. ed.). Secretaria central de ISO. Ginebra, Suiza. 2018.

Agencia Española de Protección de Datos. (2014). *Guía para una evaluación de impacto en la protección de datos personales*. España.

Superintendencia de Industria y Comercio. *Protección de datos personales: aspectos prácticos sobre el derecho de hábeas data.* Colombia.

Superintendencia de Industria y Comercio. *Guía de formatos modelo para el tratamiento de datos personales – Ley 1581 de 2012.* Colombia.

Superintendencia de Industria y Comercio. (2017). *Manual de usuario del registro nacional de bases de datos – RNBD.* Colombia.

Organización Internacional para la Estandarización, ISO. *ISO Survey 2016.* Recuperado de https://www.iso.org/the-iso-survey.html

Bureau Veritas. *ISO 31000:2018, la nueva versión para la gestión de riesgos.* Recuperado de http://www.bureauveritas.es/home/news/iso-31000-2018-renovada-gestion-riesgos

Congreso General de los Estados Unidos Mexicanos. (2010). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares.* Publicado *Diario Oficial de la Federación,* el 5 de julio de 2010. Mexico.

Senado y Cámara de Representantes de la República Oriental del Uruguay. (2008). *Ley 18.331. Protección de Datos Personales y Acción de "Habeas Data".* Publicada *Diario Oficial* No. 27549, del 18 de agosto de 2008. Uruguay.

Senado y Cámara de Diputados de la Nación de Argentina. (2000). *Ley 25.326. Protección de los Datos Personales.* Publicada *Boletín Oficial*, del 02 de noviembre de 2000. Argentina.

ISOTools. (2015), *En que consiste el Ciclo PHVA de Mejora Continua.* 20 de febrero de 2015. Recuperado de https://www.isotools.org/2015/02/20/en-que-consiste-el-ciclo-phva-de-mejora-continua/

Abreviaciones

ISO	Organización Internacional de Normalización.
P.H.V.A.	Planificar, hacer, verificar y actuar.
RNBD	Registro nacional de base de datos.
S.I.G.	Sistema Integrado de Gestión.
UVT	Unidad de Valor Tributario.
VPN	Virtual Access network.

Anexos

Anexo A. Tabla de Integración Norma Integral.

El anexo A. puede ser consultado en el archivo adjunto al trabajo de grado.

Anexo B. Matriz legal aplicable de protección de datos personales.

El anexo B. puede ser consultado en el archivo adjunto al trabajo de grado.

Anexo C. Matriz de evaluación y tratamiento de los riesgos.

El anexo C. puede ser consultado en el archivo adjunto al trabajo de grado.

Anexo D. Ficha técnica de indicadores de gestión para los objetivos S.I.G.

El anexo D. puede ser consultado en el archivo adjunto al trabajo de grado.

Anexo E. Procedimientos y Formatos para protección de datos personales.

El anexo E. puede ser consultado en el archivo adjunto al trabajo de grado.

Anexo F. Declaración de aplicabilidad.

El anexo F. puede ser consultado en el archivo adjunto al trabajo de grado.

Anexo G. Relación de normas ISO 27001 e ISO 31000.

El anexo G. puede ser consultado en el archivo adjunto al trabajo de grado.

Apéndices

Apéndice A. Matriz formulada para la evaluación y tratamiento de los riesgos de los datos personales.

El Apéndice A. puede ser consultado en el archivo adjunto al trabajo de grado.