Artículo de Investigación. Revista Killkana Técnica. Vol. 1, No. 2, pp. 31-42, Mayo-Agosto, 2017.
p-ISSN 2528-8024 / e-ISSN 2588-0888. Universidad Católica de Cuenca

Metodología Ágil para la Gestión de Riesgos Informáticos

Agile Methodology for Computer Risk Management

F. M. Arévalo*[1], I. P. Cedillo[1] y S. A. Moscoso[2]
[1]Facultad de Ingeniería, Universidad de Cuenca, Cuenca, Ecuador
[2]Facultad de Ingeniería, Industria y Construcción, Universidad Católica de Cuenca
Cuenca, Ecuador
mauriarevalom@gmail.com

Resumen

El presente artículo presenta una metodología integral para la gestión de riesgos informáticos basándose en los estándares mundialmente aceptados como son ISO 31000 e ISO/IEC 27005, los mismos que indican los requerimientos para una gestión adecuada de riesgos; sin embargo no indican, al menos de manera clara, como se puede realizar dicha gestión. Por ello se incluyen recomendaciones y buenas prácticas de otros estándares y guías internacionales para el manejo de riesgos. Con la aplicación de la metodología planteada en una empresa industrial de alimentos, se comprueba su validez; además, el equipo de trabajo que aplicó la metodología tuvo a su disposición herramientas sugeridas que ayudaron a valorar técnicamente los riesgos según su probabilidad de ocurrencia, sus consecuencias y dimensiones de seguridad afectadas.

Palabras clave: seguridad de la información, análisis de riesgos, gestión de riesgos, ISO 31000, ISO 27005.

Abstract

This article presents a comprehensive methodology for IT risk management based on globally accepted standards such as ISO 31000 and ISO / IEC 27005, which states the requirements for an adequate risk management; however, they do not indicate, at least in a clear manner, the way in which such management can be carried out. Recommendations and good practices from other international risk management standards and guidelines are therefore included. Its validity is verified through the application of the proposed methodology in an industrial food company; Furthermore, the work team that applied the methodology had at its disposal the suggested tools that helped to technically assess the risks according to their occurrence probability, their consequences, and safety dimensions affected.

Key words: information security, risk analysis, risk management, ISO 31000, ISO 27005.

I. Introducción

Hoy en día, la información ha llegado a ser uno de los activos más importantes para la operación de las organizaciones, independientemente de su naturaleza o actividad. Si dicha información es bien usada y explotada se convierte en una ventaja competitiva y en una herramienta de soporte en la toma de decisiones y cumplimiento de los objetivos estratégicos para una organización.

Con la creciente disponibilidad de dispositivos móviles y computadores en todo el mundo, más datos se procesan en cortos períodos de tiempo y debido al desarrollo de nuevas plataformas tecnológicas y la cambiante interacción entre ellas, la superficie de exposición de las empresas ha aumentado de manera significativa. Esto implica que existe un mayor número de vectores de ataque que pueden ser utilizados para comprometer la seguridad de los datos [1].

La masificación de las Tecnologías de Información (TI) y su adopción en las empresas, las han convertido también en blanco de ataques, con los riesgos asociados que aumentan y se transforman; por ello, se hace necesario crear y adaptar constantemente los medios y métodos utilizados en la seguridad de la información, para conservar la información crítica o sensible que las organizaciones actualmente necesitan proteger.

En un estudio reciente de seguridad de la información en América Latina realizado por la empresa de seguridad informática Eset [1], se muestran los resultados de un universo de 4500 empresas de todos los tamaños encuestadas en el año 2016, donde el 49 % sufrió ataques por malware, el 16 % por ransomware, el 15 % por pishing y el 10 % por explotación de vulnerabilidades entre las amenazas más importantes. También se indica que el 31 % de empresas encuestadas afirmaron no haber sufrido incidentes de seguridad, sin embargo el restante 69 % si los tuvo. En nuestro país Ecuador, el estudio indica que de las empresas encuestadas el 45.6 % tuvo ataques por malware y el 20.9 % tuvo ataques por pishing. Los datos arrojados de este estudio también demuestran que los controles de seguridad más implementados en Latinoamérica son el antivirus con el 83 %, el firewall con el 75 % y el respaldo de la información

con el 67 %.

De estos datos se puede inferir que, a pesar de que en Latinoamérica existen empresas que destinan una parte de su presupuesto a la seguridad de la información y disponen de ciertos controles, todavía se tiene un porcentaje considerable de empresas que tienen problemas de seguridad, por lo que, la seguridad de la información ha sido en realidad un gran desafío para la mayoría de las organizaciones en nuestro medio y debe ser tratada de manera íntegra. De hecho, la seguridad de la información es un proceso continuo de gestión de riesgos que cubre toda la información que necesita ser protegida [2].

Existen algunos trabajos relacionados con el planteamiento de metodologías de gestión de riesgos como el de Bojanc & Jerman-Blažič [3] donde se da a conocer un enfoque que permite el modelado económico de la gestión de riesgos de seguridad de la información para empresas contemporáneas y se propone un método para la identificación de los activos, amenazas y vulnerabilidades de los sistemas con un procedimiento que permite seleccionar la inversión óptima en tecnología de seguridad necesaria basada en la cuantificación de los valores de los sistemas que se necesitan proteger.

Se pueden mencionar también trabajos de titulación como el de Molina [4], donde se aplica la metodología Magerit [5] para gestionar riesgos en una institución de educación superior, o como el de Crespo [6], en el que se propone una metodología de gestión de riesgos llamada Ecu@Risk, basada en otras metodologías como Magerit [5], Octave-S [7], CRAMM [8] y Microsoft Risk Management [9]. El autor [6] indica que la metodología propuesta es aplicable a las Micro, Pequeñas y Medianas Empresas (MPYMES) del país en general.

En las empresas en general, la seguridad de la información es un tema crítico dado que de ella depende la seguridad de los datos de sus clientes, proveedores, transacciones diarias, las características principales que definen los productos en el caso de empresas industriales, o la reputación de la empresa en el caso de instituciones financieras; siendo necesario que esta información esté a buen resguardo. Considerando entonces la naturaleza de cada empresa, se necesita un método adecuado para la gestión de riesgos.

Por lo expuesto, el desarrollo y uso de metodologías integradas para gestionar riesgos, en especial el tecnológico, es importante con el fin de asegurar en una empresa el cumplimiento de las dimensiones y pilares fundamentales de la seguridad de la información: la confidencialidad, integridad y disponibilidad [10].

Hasta el momento, el marco existente para la gestión de riesgos y aceptado mundialmente por ISO (International Organization for Standardization, por sus siglas en inglés) lo conforman los estándares ISO 31000 (Risk management) [11] e ISO/IEC 27005 (*Information security risk management*) [12]. Estos estándares proveen los lineamientos generales sobre la gestión de riesgos pero hace falta una guía más precisa que ofrezca pautas sobre la forma de lograr los aspectos de seguridad requeridos.

Estos antecedentes motivaron el desarrollo de la metodología propuesta en el presente artículo, que permite la gestión de riesgos de tipo tecnológico basándose en los estándares ISO 31000 [11] e ISO/IEC 27005 [12] de los cuales se realizaron las adaptaciones y especificaciones requeridas como aporte a la investigación; además se incorporaron recomendaciones, conceptos y buenas prácticas de otras guías y metodologías de seguridad como MAGERIT [5], ISO 27001 [10], ISO 27002 [13] y lo correspondiente a la seguridad en la gestión de servicios de ITILv3 2011 (*IT Infrastructure Library*) [14].

El presente artículo se encuentra estructurado de la siguiente manera: inicialmente se presenta una base tecnológica analizando conceptos respecto al riesgo informático, sus elementos, análisis, gestión, el modelo PDCA (Plan, Do, Check, Act por sus siglas en inglés) y algunas metodologías de gestión de riesgos existentes; a continuación se propone la metodología para la gestión de riesgos basada en los estándares ISO 31000 [11] e ISO/IEC 27005 [12] con las adaptaciones y especificaciones planteadas, indicando finalmente las conclusiones y resultados de la aplicación de esta metodología en el departamento de producción de una empresa industrial de alimentos de la ciudad de Cuenca - Ecuador, para demostrar así su validez.

II. Base Tecnológica

A. *El riesgo informático*

ISO indica que el riesgo es "la probabilidad de que una amenaza determinada se materialice explotando las vulnerabilidades de un activo o grupo de activos y por lo tanto causar daño o pérdidas a la organización" [15]. Los riesgos se pueden dividir en tres Categorías según el tipo de impacto ocasionado: daños a las operaciones, daños a la reputación y daños legales de la organización [16].

B. *Elementos del Riesgo*

1) *Activos de Información*: Hacen referencia a cualquier elemento que contenga información; los activos forman uno de los 14 dominios que trata el estándar ISO/IEC 27002, el mismo que contiene 3 objetivos de control y 10 controles, siendo uno de los objetivos de este dominio que la organización tenga conocimiento preciso sobre los activos que posee como parte importante de la gestión de riesgos. Según el estándar, los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información [13].
2) *Amenazas*: Son vulnerabilidades de un activo que pueden ser explotadas por una o más causas potenciales de un incidente, que puede resultar en daño a los activos y por consiguiente a la organización; las amenazas son

los elementos que pueden dañar o alterar la información de una u otra forma, estas generalmente pueden ser encontradas a partir de una vulnerabilidad existente. Las amenazas se pueden clasificar en varios tipos: de origen natural, del entorno, por defecto de aplicaciones, causadas por personas de forma accidental o de forma deliberada [4] [18].

3) *Vulnerabilidades*: Los activos se ven influidos por una serie de amenazas; la probabilidad de que se materialice una de dichas amenazas y la degradación que le supone a un activo es lo que se conoce como vulnerabilidad según la metodología MAGERIT [5] [4]. Las vulnerabilidades deben ser expresadas en una escala numérica para poder posteriormente cuantificar su impacto, se sugiere que éstas sean identificadas y valoradas individualmente [19] [6]. La vulnerabilidad se puede expresar mediante la fórmula (1) [20] [6]:

$$\text{Vulnerabilidad} = \frac{\text{Frecuencia estimada}}{\text{Días al año}}. \quad (1)$$

4) *Impacto*: Es un indicador de lo que puede suceder cuando ocurren las amenazas, siendo la medida del daño causado por una amenaza cuando la misma se materializa sobre un activo. El impacto se estima como en la fórmula (2) [4] conociendo el valor de los activos y su degradación causada por las amenazas:

$$\text{Impacto} = \text{Valor} \times \text{Degradación del activo}. \quad (2)$$

C. *Análisis de Riesgos*

El análisis de riesgos es conocido como el proceso sistemático para estimar la magnitud de los riesgos a los que está expuesta una organización y permite determinar la naturaleza, el costo y la protección que tiene un sistema [18]. Al implantar y operar este plan se debe satisfacer los objetivos propuestos con el nivel de riesgo aceptado por la dirección de la organización. Al conjunto de estas actividades se le denomina Proceso de Gestión de Riesgos [4] [18]. El riesgo se puede estimar mediante el producto entre la probabilidad de que ocurra y el impacto que causa dicho riesgo, como se indica en la fórmula (3) [18]:

$$\text{Riesgo} = \text{Probabilidad} \times \text{Impacto}. \quad (3)$$

D. *Gestión de Riesgos*

Todas las organizaciones se enfrentan diariamente a riesgos de un tipo u otro [16]. La Gestión de Riesgos se define como una disciplina que existe para hacer frente a los riesgos no especulativos, que son aquellos riesgos de los cuales sólo puede ocurrir una pérdida para la organización [16]. La gestión de riesgos suele tener los siguientes objetivos vinculados: Eliminar los riesgos, Reducir a niveles "aceptables" aquellos riesgos que no se pueden eliminar y entonces, Convivir con ellos, es decir, aceptarlos ejerciendo cuidadosamente los controles que los mantienen en niveles "aceptables" o transferirlos, por medio de aseguradoras por ejemplo, a alguna otra organización.

E. *El Modelo PDCA*

Para ejecutar el análisis y posterior gestión del riesgo, se tiene que seguir un modelo con cuatro etapas conocido por sus siglas en inglés como PDCA (Plan, Do, Check, Act) ó PHVA en español: Planificar, Hacer, Verificar, Actuar, (ilustrado en Fig. 1). Al igual que con otros estándares de TI, la familia de estándares ISO 27000 se refiere directamente al ciclo Plan-Do-Check-Act (ciclo PDCA), conocido por la gestión clásica de calidad de Deming, que enfatiza en la necesidad de la orientación al proceso, así como la integración del planeamiento de las operaciones y la

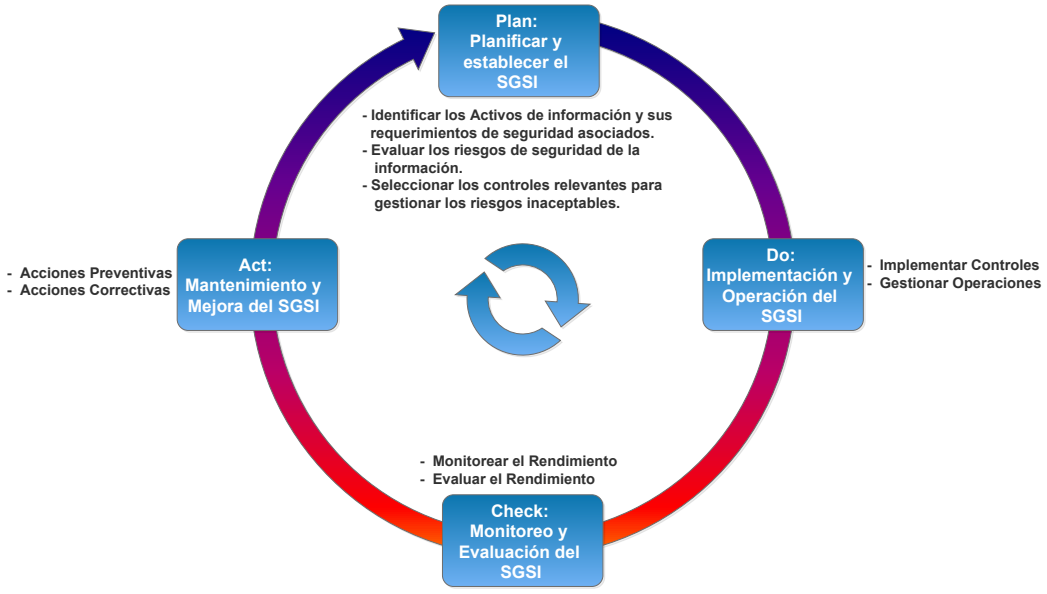

FIG. 1. Modelo PDCA [17].

verificación constante de la implementación conforme a la planificación [17].

La metodología propuesta utiliza como base el modelo PDCA [17], con la finalidad de establecer un proceso de gestión que se enfoque en la mejora continua, siguiendo los siguientes pasos:

1) *Planificar*: Se establecen los objetivos, procesos y procedimientos para la gestión de riesgos tecnológicos. La finalidad de esta etapa es la entrega de resultados acordes con las políticas y objetivos globales de la organización. Además se establece el plan de comunicaciones y el análisis del contexto organizacional actual para definir el alcance de la gestión de riesgos tecnológicos.
2) *Hacer*: Se realiza la implementación y operación de los controles, procesos y procedimientos e incluye además la operación e implementación de las políticas definidas y la valoración y tratamiento de los riesgos.
3) *Verificar*: En esta etapa se evalúa y se mide el desempeño de los procesos contra la política y los objetivos de seguridad. Además se debe informar los resultados obtenidos.
4) *Actuar*: En esta etapa se establece la política para la gestión de riesgos tecnológicos y se implementan los cambios requeridos para la mejora de los procesos. En las etapas verificar y actuar, se incluye el monitoreo y la mejora continua, donde se verifican los cambios y el cumplimientos de indicadores establecidos en la etapa de planificación.

F. Guías y Metodologías utilizadas

La metodología propuesta además de basarse principalmente en las normas ISO 31000 e ISO 27005, agrega mejoras y recomendaciones de otras guías y metodologías como:

1) *ISO/IEC 27001*: Esta norma técnica especifica los requerimientos para la implementación de controles de seguridad acordes al planteamiento de un Sistema de Gestión de Seguridad de la Información (SGSI) [10].
2) *ISO/IEC 27002*: Establece las pautas y principios generales para la implementación, mantenimiento y mejora de la gestión de seguridad. Cuenta con un amplio listado de objetivos de control y controles para un SGSI. Posee 14 dominios cada uno con sus objetivos de control y controles específicos [13].
3) *MAGERIT*: Metodología de gestión de riesgos creada por el Consejo Superior de Administración Electrónica del Ministerio de Hacienda y Administraciones Públicas de España para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información siguiendo la terminología de la norma ISO 31000. En el año 2012 se actualizó a la versión 3 [4]. En la metodología propuesta sirve como fuente de revisión de definiciones y lo correspondiente a la estimación de riesgos. MAGERIT consiste en 3 libros en versiones inglés, español e italiano: Libro 1: Método, libro 2: Catálogo de Elementos, libro 3: Guía de Técnicas [5].
4) *ITIL® v3 2011*: "Librería de Infraestructura de Tecnologías de la Información" (ITIL por sus siglas en inglés) es un estándar internacional importante que describe un conjunto de buenas prácticas para gestionar los servicios de TI. La presente metodología aplica

TABLA I
RELACIÓN DE LAS NORMAS ISO 31000 / ISO 27005 CON EL MODELO PDCA.

<table>
<tr><th>PHVA</th><th colspan="3">ISO 27005</th><th colspan="2">ISO 31000</th></tr>
<tr><td rowspan="12">Planear</td><td colspan="3"></td><td colspan="2">Mandato y compromiso de la dirección</td></tr>
<tr><td colspan="3">Definir Plan de gestión de riesgos</td><td colspan="2">Diseño del marco de trabajo para gestión de riesgos</td></tr>
<tr><td colspan="2">Establecimiento del contexto</td><td rowspan="11">Proceso de gestión del riesgo</td><td colspan="2">Entender la organización y su contenido</td></tr>
<tr><td colspan="2" rowspan="2"></td><td colspan="2">Definir responsabilidades</td></tr>
<tr><td colspan="2">Recursos</td></tr>
<tr><td colspan="2" rowspan="2"></td><td colspan="2">Integración con procesos</td></tr>
<tr><td colspan="2">Establecer mecanismos de comunicación</td></tr>
<tr><td>Identificación del riesgo</td><td rowspan="3">Valoración del Riesgo</td><td colspan="2" rowspan="3"></td></tr>
<tr><td>Estimación del riesgo</td></tr>
<tr><td>Evaluación del riesgo</td></tr>
<tr><td colspan="2">Desarrollar el plan de tratamiento del riesgo</td></tr>
<tr><td colspan="2">Aceptación del riesgo</td></tr>
<tr><td rowspan="3">Hacer</td><td colspan="2"></td><td colspan="2">Establecer políticas para la gestión del riesgo</td></tr>
<tr><td colspan="2">Implementar el plan de tratamiento</td><td>Implemnetación del marco de trabajo para la gestión de riesgos</td><td>Implementar el proceso de gestión de riesgos</td></tr>
<tr><td colspan="2">Implementar el plan de comunicación del riesgo</td><td colspan="2"></td></tr>
<tr><td>Verificar</td><td colspan="2">Monitoreo y revisión del riesgo</td><td colspan="2">Monitoreo y revisión del marco de trabajo</td></tr>
<tr><td>Actuar</td><td colspan="2">Mantener y mejorar el proceso de gestión</td><td colspan="2">Mejora continua del marco de trabajo</td></tr>
</table>

los procesos concernientes a la gestión de incidentes, gestión de problemas, gestión de acceso y el proceso de mejora continua de esta librería [14].

Se muestra a continuación la relación entre los estándares ISO 31000 e ISO 27005, ajustándolos a la metodología diseñada junto al modelo PDCA (tabla I).

III. Metodología de investigación

El trabajo de investigación propuesto se estructuró siguiendo una extensión del modelo para la transferencia de tecnología propuesto por Gorschek [21], el mismo que se encuentra basado en las necesidades de la industria. Este modelo incluye actividades de evaluación y observación (ver Fig. 2).

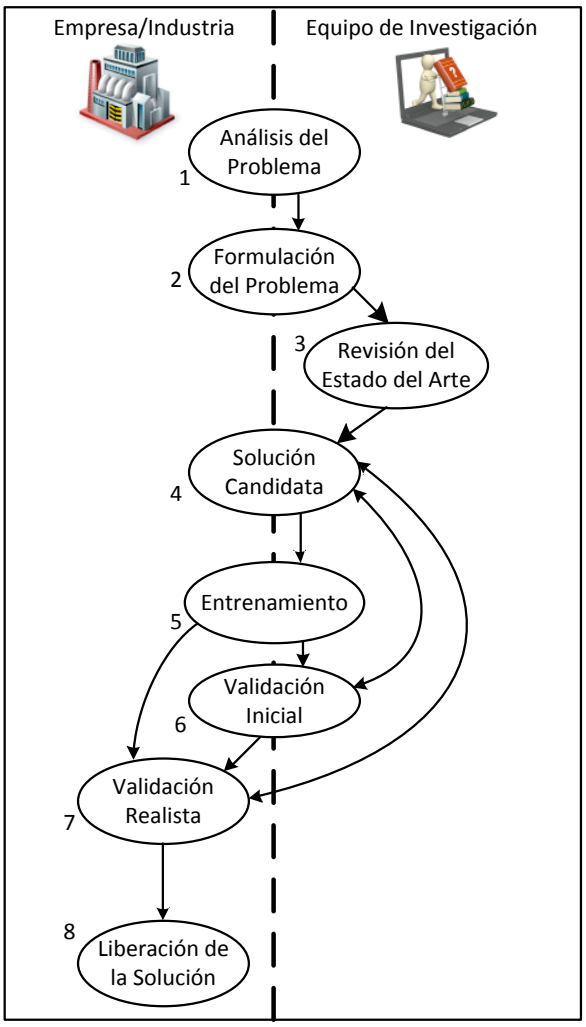

FIG. 2. Modelo de Transferencia Tecnológica de Gorschek [21].

Este modelo de investigación y transferencia de tecnología, se basa en ocho actividades relacionadas (Fig. 2), donde la búsqueda de soluciones adecuadas se realiza en un proceso iterativo por medio de la formulación de soluciones candidatas y la correspondiente validación empírica que permite dirigir los esfuerzos a una solución realista. Para la validación de la solución se utilizó la aplicación de la metodología propuesta como un caso de estudio al personal de TI en una empresa industrial de alimentos de la ciudad de Cuenca-Ecuador; de esta manera se aplica la metodología con varios individuos realizando la validación de una solución candidata llegando a obtener así una solución definitiva.

IV. Propuesta metodológica

La metodología planteada sigue los pasos del proceso de gestión de riesgos de la norma ISO 27005 [12], la cual contempla las siguientes etapas (Fig. 3):

- Establecimiento del plan de comunicación.
- Establecimiento del contexto organizacional.
- Valoración de los riesgos.
- Tratamiento de los riesgos.
- Monitoreo y mejora continua del proceso de gestión.

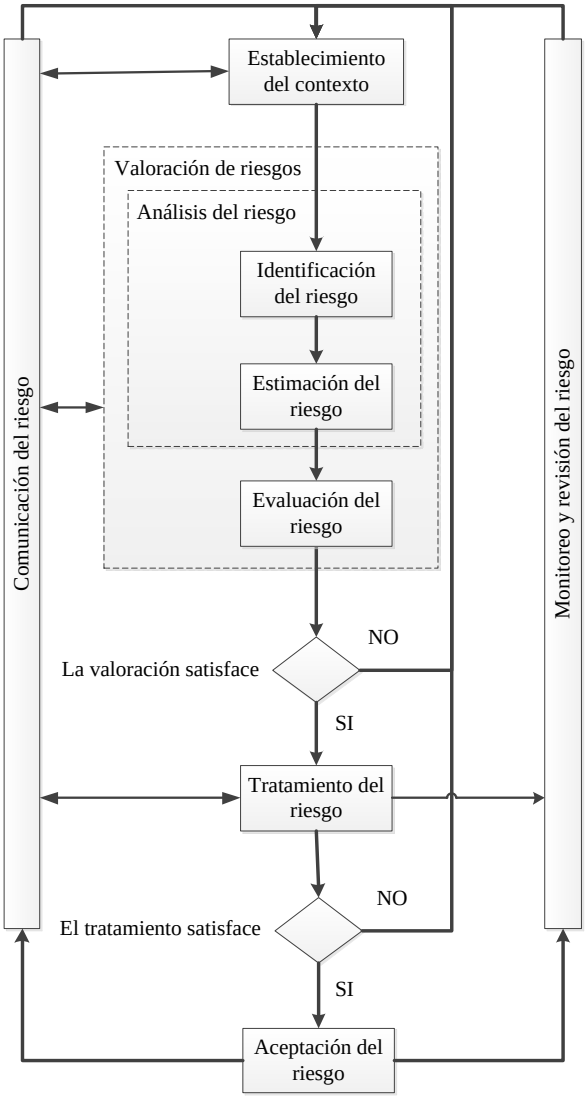

FIG. 3. Procesos de Gestión de Riesgos según la norma ISO/IEC 27005 [12].

A. *Establecimiento del Plan de Comunicación*

El plan de comunicación debe ser realizado a nivel interno (con los empleados, directivos, socios de la organización) y externo (con los clientes, proveedores, entes reguladores), considerando las definiciones sobre la existencia del riesgo, los objetivos de la gestión, el informe de los avances del proceso y todo aquello que se considere necesario. Los medios que se utilizan para comunicar el proceso de gestión dependen de las necesidades y disponibilidad de la organización, sin embargo como herramientas se sugieren: circulares, capacitaciones, presentaciones, guías o manuales, campañas de concientización que son de fácil desarrollo y permiten llegar a todo el personal objetivo; cabe señalar que la consideración de otros medios depende de la organización [12].

El plan de comunicación debe contener una capacitación adecuada a los diferentes tipos de usuarios que utilizan tecnología en la organización en la empresa, ya que frecuentemente se tienen equipos de trabajo multidiciplinarios y heterogéneos donde no siempre están personas expertos en TI que entienden los conceptos de seguridad de la información y los procesos de gestión del riesgo; considerando que esta es una amenaza que puede afectar a la aplicación de la metodología, se debe capacitar al equipo de trabajo antes de aplicar la metodología de gestión de riesgos. El plan de comunicación debe ser diseñado de manera que permita concientizar en lo que a seguridad informática se refiere y que evidencie la existencia de riesgos tecnológicos; si está bien estructurado permitirá lograr los objetivos de la gestión de forma satisfactoria, obtener información correcta para el análisis y contribuir así con la planificación del proceso de gestión de riesgos. La propuesta presentada para estructurar el plan de comunicación se la ha dividido en tres etapas:

1) *Comunicación inicial*: donde se incluyen conceptos generales sobre riesgos, sus implicaciones y las ventajas de la gestión entre otros aspectos revisados en la sección de base tecnológica del presente artículo.
2) *Comunicación en la marcha*: Durante esta etapa se busca mostrar avances del proceso de gestión de riesgos para obtener una retroalimentación y conseguir el apoyo y participación de las partes interesadas (stakeholders en inglés) de la organización (ver Fig.4).
3) *Comunicación de los resultados*: Esta etapa pretende compartir y difundir los resultados obtenidos teniendo en cuenta los debidos filtros de información de acuerdo al público objetivo (confidencialidad de la información).

Estas etapas de comunicación se aplican tanto a nivel interno como externo dependiendo de la estructura de la organización.

B. *Establecimiento del Contexto Organizacional*

Las empresas tienen un contexto interno que contiene su misión, visión, políticas, objetivos, estrategias, metas, roles y responsabilidades, estructura, normativas internas y externas, entre otros. Además interactúa constantemente con su entorno ya que tiene un contexto externo en el cual deben considerarse aspectos como la competencia, regulaciones legales, economía, política, tecnología, cultura y otros aspectos que se consideren necesarios. Es importante conocer estos aspectos para comprender que es lo que necesita ser protegido y cuáles son las limitaciones existentes para lograr esta protección.

Como fuentes de información se recomienda emplear la documentación existente en la organización relacionada con la calidad, seguridad, planeación estratégica y continuidad que brinden información que permita conocer a la organización con respecto a su medio, entrevistas con altos mandos, encuestas con el personal, visitas a instalaciones que se consideren necesarias.

El objetivo de esta etapa es conocer totalmente la organización para lograr determinar qué es lo que pudiese afectar a nivel interno y externo, que se requiere proteger y de acuerdo a los recursos actuales como se podría dar esa protección para establecer el nivel de aceptación de riesgo al cual están dispuestos, determinando los alcances y limitaciones existentes.

Es importante conocer los procesos que tiene la empresa, teniendo en cuenta que esto facilita el entendimiento sobre el funcionamiento de la organización y la definición de interacciones existentes para la identificación de activos y riesgos asociados. Además, el analizar procesos permite obtener una visión global de la organización y con ello el apoyo requerido por parte de la alta gerencia al mostrar la necesidad de proteger y gestionar los procesos críticos de la organización.

Se sugieren herramientas como el organigrama interno de la empresa (Ver Fig. 5) y su cadena de valor (Ver Fig. 6) en una empresa industrial de alimentos con el objetivo de identificar las actividades a las que se dedica la empresa y los roles de sus colaboradores.

La Cadena de Valor es una forma sistemática de examinar todas las actividades que una empresa desempeña y cómo interactúan entre ellas, además de que, con esta herramienta, se disgrega a la empresa en sus actividades estratégicas relevantes para comprender su comportamiento.

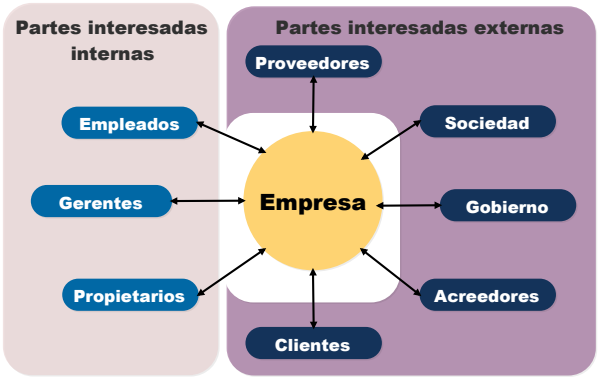

FIG. 4. Stakeholders (Partes Interesadas) en una organización [22].

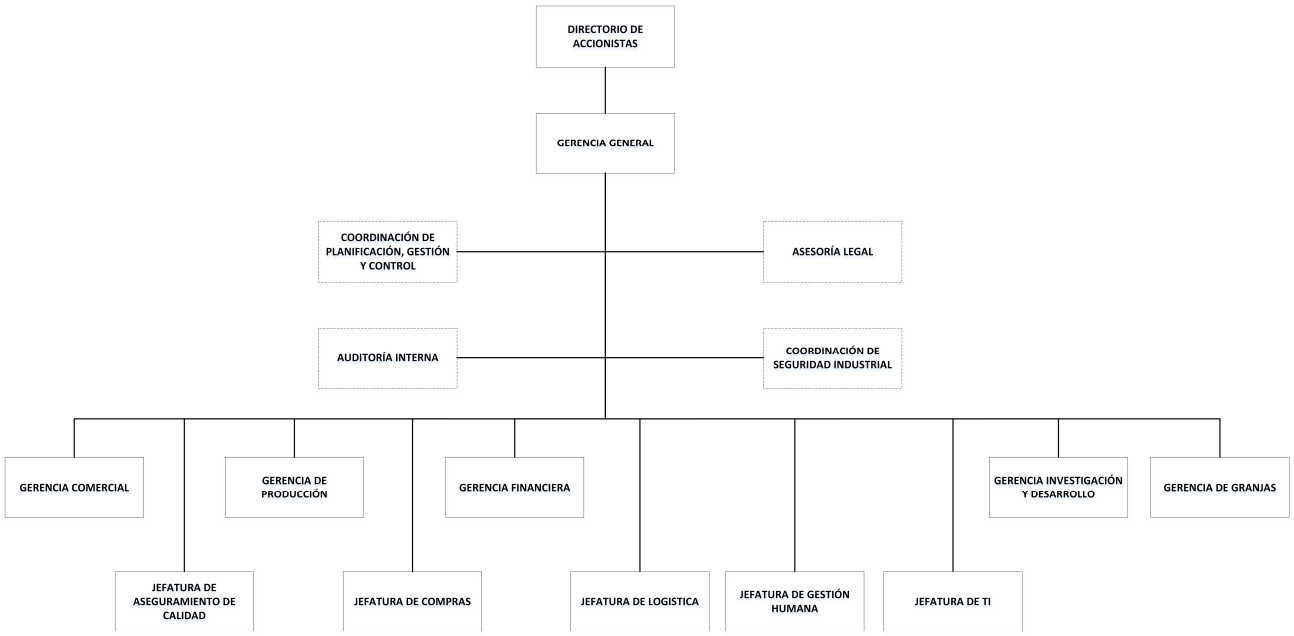

FIG. 5. Organigrama Interno de una empresa industrial de alimentos.

Para tener claros los procesos y su interrelación en el entorno de la empresa se sugiere el modelamiento de procesos mediante notación BPMN (Business Process Model and Notation) [23].

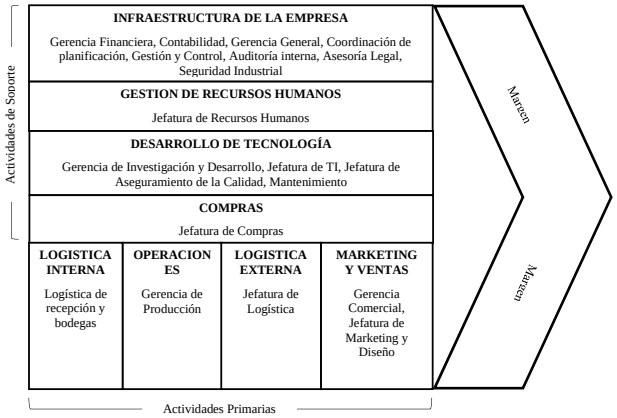

FIG. 6. Cadena de Valor en una empresa industrial de alimentos.

En la ilustración de la Fig. 7 se muestran los procesos en notación BPMN de la empresa industrial de alimentos donde se aplicó esta herramienta.

C. *Valoración de los Riesgos*

En esta etapa se identifican inicialmente los activos que se quieren proteger y sus debilidades, así como las amenazas a las cuales están expuestos. Se recomiendan también posibles controles para mitigar sus riesgos. Al realizar una valoración de activos se deben tener en cuenta los posibles activos que sean relevantes, incluyendo procesos, información, datos y activos de soporte. La valoración para activos de soporte incluye costos por adquisición, renovación o reposición, mantenimiento y toma en cuenta los factores de depreciación. Se muestra en la tabla II un ejemplo de escalas de criterios para valorar los activos [5].

TABLA II
ESCALAS DE CRITERIOS PARA VALORACIÓN DE ACTIVOS

Valor	Criterio	Impacto sobre el activo
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efector prácticos

Luego de establecer el listado de activos es posible validar si el alcance preliminar es correcto o debe ser ajustado para cumplir con los propósitos. Además se debe considerar los tipos de amenazas que pueden presentarse: físicas, lógicas o estratégicas; su origen que puede ser: natural, técnico, humano accidental o intencional; los daños o impacto que pueden implicar las amenazas, la determinación sobre las pérdidas causadas por los riesgos en términos de impacto.

Posteriormente se procede a determinar los controles y priorizar los riesgos. Los controles a usar se clasifican en: preventivos, detectivos y correctivos. Así mismo dependiendo de si se usa o no una base tecnológica para la implementación, los controles pueden ser técnicos o no técnicos. Es importante tener en cuenta las dependencias entre activos y procesos, la cadena de valor y el valor mismo

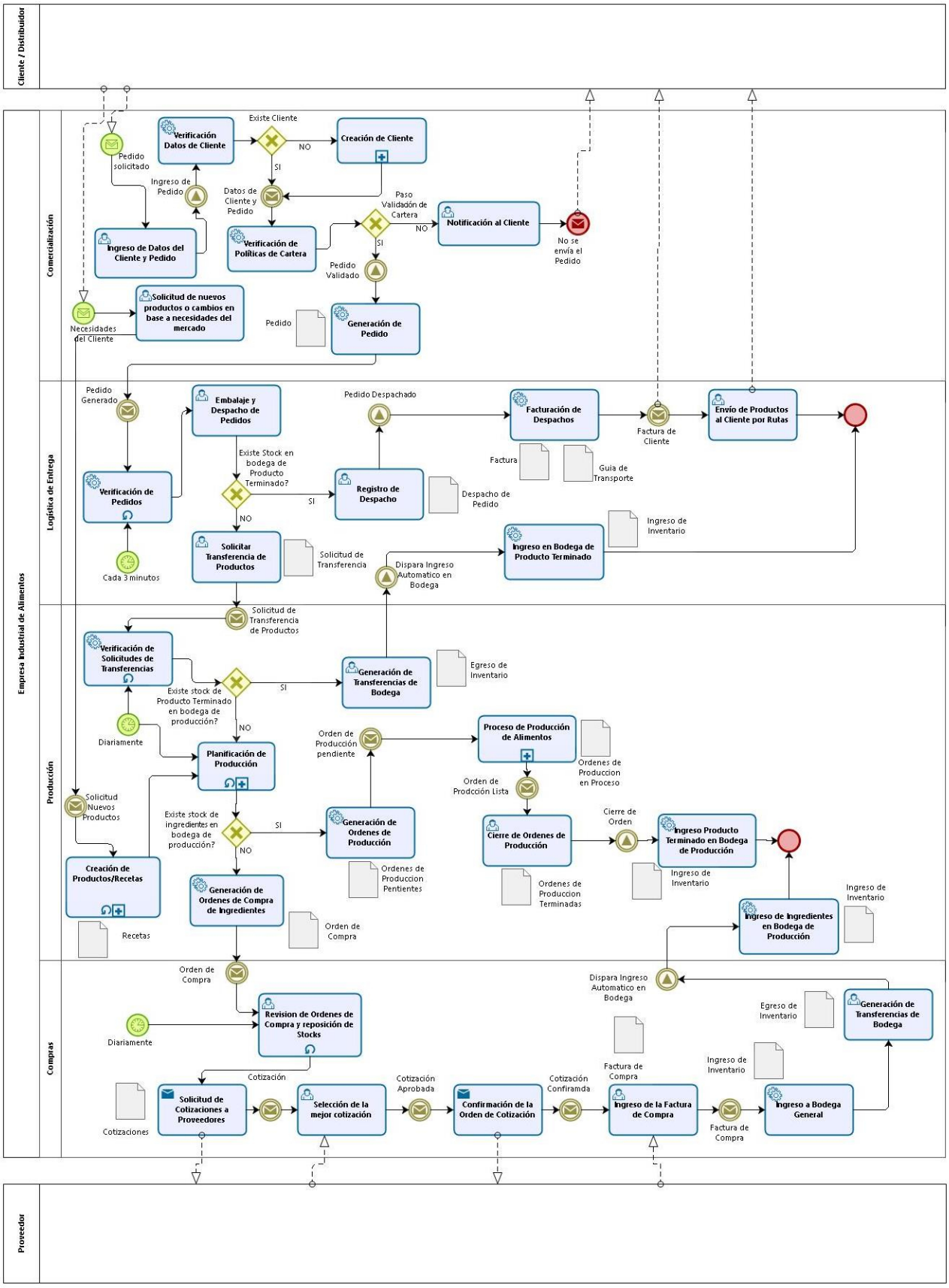

FIG. 7. Modelo de procesos con notación BPMN de una empresa industrial de alimentos.

del activo y del proceso. Los procesos deben ser priorizados con el fin de determinar niveles de criticidad de los mismos.

Se pueden determinar las vulnerabilidades con varias herramientas como la realización de pruebas y listas de chequeo, clasificándolas adecuadamente y analizando su impacto con respecto a la frecuencia de ocurrencia, identificando así correctamente los riesgos. Para valorar los riesgos se pueden usar técnicas cuantitativas y/o cualitativas para la estimación de riesgos con algunas formas de presentación de la información como vectores de ataque o matrices, dependiendo de los requerimientos, conocimientos, recursos y habilidades del equipo de trabajo de gestión de riesgos en la empresa.

D. Tratamiento de los Riesgos

En esta etapa se establecen e implementan las acciones a tomar para mitigar los riesgos encontrados y lograr riesgos residuales aceptables por la organización. Las acciones a tomar para mitigar los riesgos deben ser: reducir, aceptar, eliminar o transferir los riesgos.

Se establece un plan de tratamiento de riesgos según la priorización previa realizada. Este plan debe definir recursos, responsabilidades y actividades teniendo en cuenta las posibles restricciones a nivel económico, legal, temporal, técnico, operativo, político, cultural. Los controles que sean recomendados deben considerar un análisis costo-beneficio, teniendo en cuenta costos de implementación y mantenimiento.

El plan debe ser documentado y finalmente definir las políticas a seguir [13]. Con la definición de políticas de seguridad se establecen los lineamientos base requeridos para cumplir con las dimensiones de seguridad (confidencialidad, integridad y disponibilidad) [24]. En este punto es importante que el plan sea consistente con las metas y objetivos indicados en la planificación del proceso de gestión. Se debe considerar el tiempo acorde con lo definido al inicio y con el tiempo de vida útil de los activos, además de dar paso a la siguiente etapa de mejora continua. El plan de tratamiento define la gestión de riesgos sin dejar espacio a nuevos posibles riesgos que ocurran como consecuencia de errores en la implementación de las acciones del mismo tratamiento.

E. Monitoreo y Mejora Continua del Proceso de Gestión

El control de cambios es muy importante en esta etapa y el monitoreo debe realizarse sobre los activos, procesos, vulnerabilidades, amenazas, controles, documentación de políticas y procedimientos con el fin de establecer acciones a seguir frente a los cambios (agregar activos, riesgos o amenazas nuevas que pudieran surgir o también modificaciones o eliminaciones sobre los mismos) consiguiendo que la gestión este continuamente actualizada y evaluada mediante indicadores de cumplimiento de los planes.

El monitoreo y la mejora continua busca asegurar la constante revisión sobre la gestión de riesgos para dar cumplimiento a los procesos de mitigación definidos. También, permite agregar al análisis riesgos nuevos que pudiesen aparecer luego de la definición de los planes teniendo en cuenta posibles cambios internos y externos.

Las etapas de la metodología propuesta se ilustran de manera resumida en la figura 8 en un proceso secuencial claramente definido en cada una de sus etapas.

V. Conclusiones

La metodología de gestión de riesgos propuesta presenta una oportunidad para comprender mejor los conceptos definidos en los estándares ISO/IEC 27005 e ISO 31000 para la gestión de riesgos, ya que se basa en ellos y se centra concretamente en un enfoque a los riesgos tecnológicos. Se propone el uso de esta guía para la aplicación del proceso de gestión de riesgos evitando los vacíos y ambigüedades que tienen los estándares ISO, indicando con claridad cómo llevar a cabo las acciones que estos mencionan con las herramientas adecuadas y adaptadas para su uso en empresas de nuestro medio.

Como validación de la metodología se aplicó la misma realizando la evaluación y tratamiento de riesgos en una empresa industrial de alimentos con los siguientes resultados:

La organización en la que se aplicó la metodología es una empresa industrial de alimentos dedicada a la producción, comercialización y distribución de cárnicos y embutidos en la ciudad de Cuenca-Ecuador. Se trata de una empresa privada de tipo PYME (Pequeñas y Medianas Empresas) y tiene en total 350 empleados distribuidos entre la matriz y 2 sucursales en las ciudades de Quito y Guayaquil. Su organización se la puede evidenciar en su organigrama interno (Fig. 5) y su cadena de valor (Fig. 6). La metodología propuesta se aplicó específicamente en el departamento de producción e la empresa para identificar, analizar y gestionar los riesgos de esta área, y duró un total de 7 horas divididas en 2 días de labores. Los procesos a los que se dedica esta empresa se analizaron mediante un modelo con notación BPMN como indica la metodología (Fig. 7).

En la aplicación de la metodología, se obtuvieron un total de 201 activos identificados, la mayoría, un 59.20 %, tienen un valor calificado como Alto respecto a las dimensiones de seguridad; un 31.84 % tienen un valor Medio, un 6.47 % tiene un valor Muy Alto y un 2.49 tienen un valor Extremo; además, ningún activo tuvo una valoración de Bajo o Despreciable. Esto se debe a que la mayoría de tipos de activos como edificaciones, hardware, software, información electrónica, información en papel, e infraestructura de comunicaciones tienen un nivel crítico respecto a su confidencialidad, integridad y disponibilidad ya que en esta área los activos de información contienen o gestionan información crítica ya sea electrónica o en papel como las órdenes de producción, formulas o recetas de los productos que fabrica la empresa, datos de operación de la maquinaria, procesos y normas de calidad electrónicos o impresos, la documentación de los procesos de elaboración

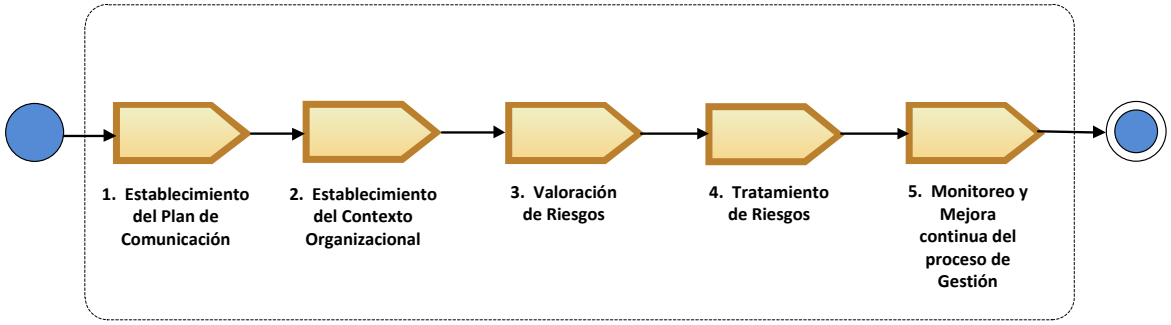

FIG. 8. Etapas de la metodologia propuesta.

de productos y sus recursos, el software que controla estos procesos y sus respectivas bases de datos, etc.

Se identificaron un total de 30 riesgos divididos en 7 riesgos de tipo provocados (no intencionados), 11 riesgos provocados (intencionados), 3 riesgos de comunicaciones, 6 riesgos lógicos y 3 riesgos naturales.

Otro punto relevante de la aplicación de la metodología fue que se llegó a la conclusión de que la mayoría de estos riesgos (56 %) fueron analizados y valorados con un nivel alto, pues la mayoría son riesgos provocados por error o deliberadamente, el 32 % de riesgos fueron catalogados como extremos, partiendo de que la mayoría afectan a las 3 dimensiones de seguridad: integridad, disponibilidad y confidencialidad, por lo que estos riesgos necesitarían medidas y acciones de gestión urgentes si no las hubiera en la empresa.

El restante 12 % fueron catalogados de nivel medio y específicamente caen en esta categoría los riesgos de comunicaciones, ya que se tienen equipos e infraestructura de contingencia para las comunicaciones en la empresa; sin embargo son riesgos de nivel medio porque afectan la disponibilidad de la información, ocasionando que ciertos procesos se detengan por un período de tiempo en la producción de la empresa hasta que se solucione el problema.

Ningún riesgo fue valorado como bajo o despreciable, pues todos tienen una probabilidad de ocurrencia y un nivel de consecuencias que afectan a una o varias de las dimensiones de seguridad (Disponibilidad, Integridad o Confidencialidad) de los activos de información en el departamento de producción que los hacen tener una valoración media, alta o extrema.

Para todos estos riesgos identificados y valorados, se planteó exitosamente un plan de tratamiento de riesgos, el cual se debe monitorear continuamente revisando su cumplimiento.

VI. DISCUSIÓN

Actualmente, uno de los marcos existentes para la gestión de riesgos y aceptado mundialmente por ISO (International Organization for Standardization, por sus siglas en inglés) lo conforman los estándares ISO 31000 (Risk management) [11] e ISO/IEC 27005 (*Information security risk management*) [12].

Existen también otras metodologías para gestionar riesgos como lo son Magerit [5], Octave-S [7], CRAMM [8] y Microsoft Risk Management [9]. Sin embargo estos estándares proveen lineamientos generales sobre la gestión de riesgos pero les hace falta una guía más sencilla y clara que ofrezca pautas sobre la forma de lograr los aspectos importantes de seguridad requeridos como identificar, evaluar, valorar y tratar los riesgos tecnológicos.

La motivación principal y objetivo que se cumplió en el presente trabajo fue contar con un método adecuado para la gestión de riesgos basado en la norma ISO/IEC 27005 y validar su aplicación en empresas industriales de alimentos; ya que si bien en la bibliografía consultada se indican estudios que proponen metodologías para gestionar riesgos y establecer así una cultura de seguridad de la información en las organizaciones, no establecen un método apropiado, con procesos claros y detallados para la gestión de riesgos en empresas industriales de alimentos. Se debe considerar que en este tipo de organizaciones se maneja información crítica como los datos de sus clientes, proveedores, transacciones diarias y las características principales que definen un producto como son sus recetas, proceso de fabricación, costos, etc. siendo necesario que toda esta información tenga la seguridad adecuada.

En el presente trabajo se detalló de una manera clara y sencilla el planteamiento de un método adecuado para la identificación, análisis, evaluación, tratamiento y monitoreo de riesgos. La metodología planteada sigue los pasos del proceso de gestión de riesgos de la norma ISO 27005 [12], la cual contempla las siguientes 5 etapas: establecimiento del plan de comunicación, establecimiento del contexto organizacional, valoración de los riesgos, tratamiento de los riesgos, monitoreo y mejora continua del proceso de gestión.

Se proponen además como contribución a la investigación y al estándar ISO/IEC 27005, herramientas e instrumentos para que la metodología sea ágil, eficiente y aplicable a las empresas industriales de alimentos. El modelo propuesto en este trabajo va más allá de las metodologías analizadas en la literatura, ya que describe un contexto

organizacional más amplio que incluye una visión global de la organización y de sus influencias externas e internas claves que pueden materializar el impacto de riesgos en los procesos organizacionales, mediante el análisis de procesos mediante notación BPMN, el organigrama funcional y la cadena de valor, entre otras herramientas o instrumentos que mejor se adaptan y describen las operaciones y estructura de las empresas industriales en general en nuestro medio.

En beneficio de la comunidad científica, se indica que la metodología propuesta en este estudio ofrece una oportunidad para hacer más avances en una importante y creciente temática como lo es la seguridad informática en determinados dominios, teniendo en consideración la identificación, evaluación y gestión de riesgos para una determinado tipo de organización, ya que se debe considerar que no todas las empresas u organizaciones tienen las mismas necesidades de seguridad, pues sus riesgos varían de acuerdo a su localización, su naturaleza, estructura y los procesos que se manejan así como los activos de información y controles que disponen; considerando además el enfoque e importancia que los directivos de una organización tienen respecto a la seguridad de su información y la situación o estado actual de una empresa en cuanto a seguridad informática se refiere.

Por lo tanto se podrían proponer otras metodologías y su aplicación basadas en esta propuesta, pues si bien la metodología de este trabajo se la realizó y evaluó en una empresa industrial de alimentos, también podría servir en empresas industriales de diversos tipos, realizando las validaciones correspondientes.

Referencias

[1] ESET, "Eset security report latinoamérica 2017." [Online]. Disponible en https://welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf, 2017.

[2] A. Barbosa Martins and C. Saibel, "A methodology to implement an information security management system," *Journal of Information Systems and Technology Management*, vol. 2, no. 2, pp. 121–136, 2005.

[3] R. Bojanc and B. Jerman-Blažič, "An economic modelling approach to information security risk management," *International Journal of Information Management*, vol. 28, no. 5, pp. 413–422, 2008.

[4] M. F. Molina, *Propuesta de un plan de gestión de riesgos de tecnología aplicado en la Escuela Superior Politécnica del Litoral*. PhD thesis, Universidad Politécnica de Madrid, 2015.

[5] Ministerio de Hacienda y Administraciones Públicas, "Magerit v.3 : Metodología de análisis y gestión de riesgos de los sistemas de información." [Online]. Disponible en https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WaeCb7LyjIU.

[6] P. E. Crespo, "Metodología de seguridad de la información para la gestión del riesgo aplicable a MPYMES," *El Escorial*, 2016.

[7] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "OCTAVE{®}-S Implementation Guide," *Software Engineering Institute*, vol. 1, no. V 1.0, pp. 1–63, 2005.

[8] Z. Yazar, "A qualitative risk analysis and management tool–CRAMM," *SANS InfoSec Reading Room White Paper*, pp. 1–13, 2002.

[9] Microsoft, "The Security Risk Management Guide," *Microsoft Solutions for Security and Compliance and Microsoft Security Center of Excellence*, 2006.

[10] ISO, "ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements." [Online]. Disponible en https://www.iso.org/standard/54534.html.

[11] ISO, "ISO 31000 - Risk management, ISO 31000: 2009." [Online]. Disponible en https://www.iso.org/iso-31000-risk-management.html, 2009.

[12] ISO, "ISO/IEC 27005:2011." [Online]. Disponible en https://www.iso.org/obp/ui/{#}iso:std:iso-iec:27005:ed-2:v1:en, 2011.

[13] ISO, "ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls." [Online]. Disponible en https://www.iso.org/standard/54533.html, 2013.

[14] M. Ivanka and B. Gerard, *ITIL Foundation Complete Certification Kit - Fourth Edition: Study Guide Book and Online Course*. 2011.

[15] ISO, "ISO/Guide." [Online]. Disponible en https://www.iso.org/obp/ui/{%}7B{#}{%}7Diso:std:iso:guide:73:ed-1:v1:en, 2009.

[16] A. Calder and S. Watkins, *A Manager's Guide to Data Security and ISO 27001/ISO 27002*. Kogan Page, 4 ed., 2008.

[17] G. Disterer, "ISO/IEC 27000, 27001 and 27002 for Information Security Management," *Journal of Information Security*, vol. 4, no. April, pp. 92–100, 2013.

[18] M. AMUTIO, J. Candau, and J. Mañas, *MAGERIT – Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro I*. Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012.

[19] J. Burgos Salazar and P. Campos, *Modelo Para Seguridad de la Información en TIC*. Concepción, Chile: Universidad del Bío-Bío, 2008.

[20] P. Castaño, "Metodología de Análisis de Riesgos: MAGERIT." [Online]. Disponible en http://blacksecurity.net/Gr2Dest/metodologia-de-analisis-de-riesgos-magerit/, 2014.

[21] T. Gorschek, P. Garre, S. Larsson, and C. Wohlin, "A model for technology transfer in practice," *IEEE Software*, 2006.

[22] M. Gallego Ruiz, "Relación con los Stakeholders." [Online]. Disponible en http://slideplayer.es/slide/1064742/, 2012.

[23] Object Management Group, "BPMN: Business Process Model and Notation." [Online] . Disponible en http://www.bpmn.org/.

[24] ISO, "ISO/IEC 27000:2016. Information technology - Security techniques - Information security management systems - Overview and vocabulary." [Online]. Disponible en http://www.iso.org/iso/home/store/catalogue{_}tc/catalogue{_}detail.htm?csnumber=66435, 2016.

***Recibido**: 01 de agosto de 2017*

***Aceptado**: 31 de agosto de 2017*

Franklin Mauricio Arévalo Moscoso: *Egresado del programa de Maestría en Gestión Estratégica de TICs de la Universidad de Cuenca, Analista de Sistemas e Ingeniero de Sistemas graduado en la Universidad Católica de Cuenca. Actualmente trabaja como Jefe del departamento de TI en la empresa Italimentos Cía. Ltda. desde el año 2007.*

Irene Priscila Cedillo Orellana: *PhD en Informática graduada en la Universidad Politécnica de Valencia, Ingeniera de Sistemas graduada en la Universidad de Cuenca, Master en Telemática en la Universidad de Cuenca; Master en Ingeniería del Software y Métodos Formales graduada en la Universidad Politécnica de Valencia. Profesora titular en la Universidad de Cuenca desde el año 2009. Correo electrónico: priscila.cedillo@ucuenca.edu.ec*

Santiago Arturo Moscoso Bernal: *Tecnólogo Electrónico, Ingeniero Eléctrico y Especialista en Docencia Universitaria en la Universidad Católica de Cuenca, Magister en Aprendizaje de la Física en la Universidad Nacional de Chimborazo, Master en Energías Renovables en la Universidad Europea del Atlántico (España), actualmente es Director del Dep. de Gestión de Calidad y docente de Ingeniería Eléctrica en la Universidad Católica de Cuenca. Correo electrónico: smoscoso@ucacue.edu.ec*