UNIVERSIDAD TÉCNICA DE MANABÍ
Fundada en 1952

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Análisis y evaluación de riesgos aplicado a la seguridad de la información bajo la norma ISO/IEC 27002: Caso de estudio Distribuidora Bravel

Analysis and risk assessment applied to information security under the ISO/IEC 27002 standard: Case study Bravel distributor

Autores

[1]* *María Angélica Velepucha Sánchez*

[2] *Jessica Morales Carrillo*

Marco Fernando Pazmiño Campuzano

[1,3] Instituto de Posgrado, Universidad Técnica de Manabí, Portoviejo, Ecuador.
[2] Grupo de Investigación SISCOM, Carrera de Computación, Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, Ecuador.

* Autor para correspondencia

Comó citar el artículo: Velepucha Sánchez, M. A., Morales Carrillo, J., & Pazmiño Campuzano, M. F. (2022). Análisis y evaluación de riesgos aplicado a la seguridad de la información bajo la norma ISO/IEC 27002: Caso de estudio Distribuidora Bravel. *Informática y Sistemas: Revista de Tecnologías de la Informática y las Comunicaciones, 6*(1), 60-70. DOI: https://doi.org/10.33936/isrtic.v6i1.4473

Enviado: 21/03/2022
Aceptado: 28/04/2022
Publicado: 02/06/2022

Resumen

El propósito del presente estudio fue diagnosticar el grado de los riesgos que sufren la información y activo que se encuentra en la distribuidora Bravel, ya que muchas empresas carecen de controles de seguridad por lo que no pueden garantizar la seguridad de la información. Esta investigación se encamino al análisis y evaluación para la gestión de activos de información mediante la secciones que tiene la norma ISO/IEC 27002. Se presenta los resultados aplicando la metodología del análisis y evaluación de riesgos con el diseño de diversos instrumentos como cuestionarios de los ítems que ha establecido la norma, en la cual nos permitirá conocer el riesgo que tiene la organización con respecto a la seguridad de la información como: clave de seguridad, datos del personal del área informática y usuarios de los sistemas, y realizar un testeo que permitieron establecer el diagnóstico de seguridad actual. Finalmente, y de acuerdo a los resultados del análisis y evaluación de los riesgos, se proponen los controles de seguridad para que sean integrados hacia el futuro dentro de un SGSI que responda a las necesidades de seguridad informática y de la información acorde a sus necesidades.

Palabras claves: Análisis; Información; Riesgo; Seguridad.

Abstract

The purpose of this study was to diagnose the degree of risks suffered by the information and assets found in the Bravel distributor, since many companies lack security controls, so they cannot guarantee the security of the information. This research was directed to the analysis and evaluation for the management of information assets through the sections that the ISO / IEC 27002 standard has. The results are presented applying the methodology of analysis and risk evaluation with the design of various instruments such as questionnaires of the items that the standard has established, in which it will allow us to know the risk that the organization has with respect to information security, such as: security key, data of the personnel of the computer area and users of the systems, and carry out a test that allowed to establish the current safety diagnosis. Finally, and according to the results of the analysis and evaluation of the risks, the security controls are proposed to be integrated into the future within an ISMS that responds to the needs of computer and information security according to their needs.

Keywords: Analysis; Information; Risk; Security.

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

1. Introducción

Esta investigación tuvo como objetivo específico diagnosticar el índice de riesgo que sufre la información procesada y activo que se encuentra dentro de la Distribuidora Bravel, ya que actualmente la información son los activos más valiosos que se presenta dentro de una organización. Por ende, este estudio tiene un aporte teórico al campo de conocimiento; debido a los resultados obtenidos de alguna forma aportarán significativamente a otras respectivas investigaciones.

El análisis y evaluación de riesgos, la verificación de la existencia de controles de seguridad existentes, las pruebas con software y el monitoreo de los sistemas de información permiten establecer el estado actual de la organización, identificar las causas de vulnerabilidades y proponer soluciones de control que permitan su mitigación (Solarte Solarte, 2015). Estas acciones deben estar enmarcadas en un proceso lógico, sistemático, documentado, que pueda ser difundido interno para garantizar la gestión correcta de la seguridad informática y de la información, siguiendo el ciclo de mejora continua (planear, hacer, verificar y actuar - PHVA) (Salazar Choez, 2018).

Inicialmente se trata de comprender la norma ISO/IEC27002 en cada uno de los dominios, para determinar el alcance de su aplicabilidad. Una vez definidos los dominios y determinados los activos existentes, se aplica la metodología para realizar análisis y evaluación de riesgos respecto a los tres criterios de información que son la confidencialidad, la integridad y la disponibilidad de la información.

La siguiente tarea consiste en la verificación de la existencia de controles de seguridad existentes en la empresa y su aplicación; ya que pueden estar incluidos dentro de los procesos de calidad organizacionales. Estos deben ser comparados los resultados con el software eMarisma e Isotools, definidos en la norma ISO/IEC 27002 como políticas y procedimientos; el resultado servirá de base para el diseño, la implementación e implantación futura de un SGSI como respuesta a los riesgos encontrados (Enríquez Collaguazo, 2018).

En el artículo se muestra un conjunto de instrumentos que posibilitan realizar el análisis y evaluación de riesgos, las técnicas utilizadas para conocer y comprender el estado actual de las organizaciones empresariales evaluadas y que pueden ser aplicados para realizar procesos de auditoría a la seguridad. Finalmente se explica la metodología para aplicar el proceso de análisis y evaluación de los riesgos desde la fase inicial de conocimiento del sistema, la fase de identificación de las vulnerabilidades, amenazas y riesgos de seguridad determinando el nivel de riesgo a que se ve expuesta la organización, por probabilidad e impacto en los criterios de confidencialidad, integridad y disponibilidad de la información, para luego aplicar el software que mejor resultado arroje.

2. Desarrollo

2.1. La seguridad

La seguridad, aún existe divergencia en los criterios de almacenamiento, acceso y transmisión de información de los pacientes porque los requerimientos físicos y lógicos varían para cada empresa, equipo desarrollador o intereses particulares. En general, las amenazas y ataques sobre una red de datos, obligan a establecer parámetros para prevenir o mitigar estas falencias, por medio de regulaciones y estándares (Enríquez Collaguazo, 2018).

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información (Armendáriz, 2017).

Actualmente las TICS (Tecnologías de la información y de la comunicación) es la base fundamental para el desarrollo y superación de un país, la información que en ellas se opera son consideradas como datos muy valiosos para todas organizaciones públicas como privadas con el fin de que tengan éxito, es por eso que debemos ofrecer seguridad a la información (Ladino, 2011).

Los modelos de evaluación de sistemas de seguridad permiten conocer, dentro de una organización, la madurez con la cual la organización lleva adelante sus políticas, actividades, usa sus herramientas y métodos, etc., en pos de su seguridad. Por lo tanto, para una organización preocupada en su seguridad informática, resulta necesario contar con estándares, así como herramientas apropiadas para evaluar el grado de adecuación con dichos estándares.

Los procesos de admisión y nivelación han operado normalmente sin que exista una evaluación o auditoria a las aplicaciones que los soportan situación que incrementa los riesgos a los que cada proceso y actividades están expuestas. La evaluación de dichos procesos con el objetivo de establecer recomendaciones que permitan mejorar los controles o deficiencias encontradas y comunicarlas formalmente a los directivos (Velasco, 2008).

En la actualidad todas las organizaciones dentro de nuestro medio se basan en la información para tomar decisiones que permitan la continuidad de los negocios, “innovar así los activos importantes para la empresa, siendo necesario protegerla ante cualquier evento que puede causar corrupción en los datos, dando la importancia de la información, organizaciones internacionales de estandarización han elaborado normas de buenas prácticas para seguridad y buen uso de la información y de los activos en general” (Figueroa Moran, 2017).

e-ISNN 2550-6730 | Vol. 6, Núm. 1 (60-70): Enero-Junio, 2022 | DOI: 10.33936/isrtic.v6i1.4473

La masiva incorporación de las tecnologías de las comunicaciones y la información al mundo de los negocios ha generado profundas transformaciones en las responsabilidades de la alta gerencia en las organizaciones. Es importante entender que hoy la inversión en TI no trata solamente de implementar soluciones tecnológicas, sino que se focalizan en implementar cambios y transformaciones en la organización posibilitados por TI. Esto genera mayor complejidad y mayores riesgos que en el pasado, y la aplicación de las prácticas tradicionales de gestión no son suficiente (Mora Palacios, 2017).

El amplio uso de las tecnologías de información en los negocios hace que cada vez sea más fácil la expansión de éstos. La comunicación con clientes que se encuentran en una ciudad o país diferente al de ubicación de la empresa, la posibilidad de realizar transacciones comerciales vía web y en general, la facilidad del uso de la tecnología y la globalización de la información para todas las personas ha contribuido a que las organizaciones crezcan cada vez más rápido (Pazmiño Flores, 2019).

La seguridad informática.

La seguridad informática se define como la protección de los recursos valiosos, que corresponden a un ente legítimo propietario, de los posibles riesgos y ataques efectuados por agentes no autorizados. De igual manera la seguridad informática tiene como finalidad en proteger los recursos de un sistema informático como la Información, Servicios y Arquitecturas. ISOTOOLS, (Bermudez Molina, 2015) Software de Gestión para la excelencia empresarial define que la seguridad informática es una rama de la ingeniería de sistemas que se encarga de coordinar acciones para proteger la integridad y la privacidad de la información que ha sido almacenada en un sistema informático.

Afirman que: "La seguridad informática se puede definir como un conjunto de procedimientos, dispositivos y herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información en un sistema informático e intentar reducir las amenazas que pueden afectar al mismo" (Bermudez Molina, 2015).

Al mismo tiempo la seguridad informática consiste en proteger la integridad de la información no sólo es una cuestión de ordenarlas, clasificarlas y almacenarlas porque no es suficiente. Las amenazas que velan a los datos tienen estrategias sofisticadas. Los virus informáticos, por ejemplo, son programas perjudiciales que se sitúan en la memoria RAM de los ordenadores del usuario, impidiendo el normal acceso a los datos que allí reposa.

Asimismo, existen los mencionados hackers o peritos del saqueo informático, que se encargan de bloquear los sistemas para acceder a bases de datos confidenciales y utilizar dicha información para fines desconocidos. Toda empresa u organización tienen información de carácter confidencial, de mayor o menor medida, con la finalidad de optimizar la seguridad requerida para la protección de la integridad de los recursos informáticos de las actividades de la misma (López Uriarte, 2017).

En la actualidad considera que la seguridad de los datos y la información comprenden 3 principios esenciales que son: Confidencialidad se trata de la cualidad que debe poseer un documento o archivo para que éste solo se entienda de manera comprensible o sea leído por la persona o sistema que esté autorizado; Integridad es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original; Disponibilidad se trata de la capacidad de un servicio, de unos datos o de un sistema a ser accesible y utilizable por los usuarios o procesos autorizados cuando lo requieran. También se refiere a la capacidad de que la información pueda ser recuperada en el momento que se necesite.

Como resultado la Seguridad Informática se preocupa de que la información operada por un ordenador no sea dañada o alterada, que esté disponible y en condiciones de ser procesada en cualquier momento y se mantenga confidencial.

El riesgo informático.

Los riesgos se pueden especificar como aquellas casualidades que impiden el cumplimiento de un objetivo ya que afectaría al total funcionamiento de la organización considerado un riesgo o amenaza para la entidad.

En lo relacionado con la tecnología, señala que totalmente el riesgo se traza directamente como amenaza, estableciendo el nivel de muestra a la ocurrencia de una pérdida, como, por ejemplo, el riesgo de datos debido a rotura de disco, virus informáticos, etc. (Silva Coelho, 2018).

Resalta que la Organización Internacional por la Normalización (ISO) define el riesgo como "La probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándole pérdidas o daños". Por otra parte, los riesgos informáticos se mencionan a la inseguridad existente por la posible realización de un suceso concerniente con la amenaza de daño relacionado a los bienes o servicios informáticos (Periféricos, instalaciones, proyectos, programas de cómputo, archivos, información, datos confidenciales, entre otros) (Silva Coelho, 2018).

Elemento de riesgo.

Existen algunos tipos de riesgos que corren los sistemas informáticos y para los cuales los responsables del manejo de la información deben tomar acciones para corregirlos, los riesgos se pueden clasificar de la siguiente manera: "Respecto a los equipos, respecto a los programas, respecto a las personas, y respecto a los trabajos"

Activos.

Es cualquier elemento que posee valor para la organización, sus operaciones comerciales o su continuidad, incluidos los recursos de información que apoyan la misión de la organización. Se pueden distinguir dos clases de activos: los activos primarios que incluyen a los procesos del negocio, actividades e información; y los activos de apoyo, que incluyen hardware (equipos de procesamiento de datos, periféricos y medios de comunicación), software (sistema operativo, servicio, software de aplicación), redes, personal (directores, usuarios, personal de operación y desarrolladores), lugar y estructura de la organización (proveedores y fabricantes) (Bermudez Molina, 2015).

e-ISNN 2550-6730 | **Vol. 6, Núm. 1 (60-70): Enero-Junio, 2022** | **DOI: 10.33936/isrtic.v6i1.4473**

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

Los activos forman uno de los 14 dominios que trata el estándar ISO/IEC 27002, el cual contiene 3 objetivos de control y 10 controles, siendo la finalidad de este dominio que la organización tenga un conocimiento preciso sobre los activos que posee, su responsabilidad y su clasificación como parte importante de la gestión de riesgos. Según el estándar ISO/IEC 27002, los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objetivo de indicar cómo ha de ser tratada y protegida dicha información (ISO/IEC 27002, 2013) (Disterer, 2013).

La información es un activo que, como otros activos comerciales importantes, tiene valor para la organización y en consecuencia necesita ser protegido adecuadamente. La seguridad informática protege la información de un amplio rango de amenazas con la finalidad de asegurar la continuidad de los negocios, minimizar el daño comercial y maximizar el reembolso de las inversiones y oportunidades comerciales. La información puede existir en muchas formas; puede ser de forma escrita, impresa, electrónica, transmitida por correo o usando medios electrónicos o hablado en una conversación (Bermudez Molina, 2015).

Amenazas

Las amenazas siempre estarán presentes en los sistemas informáticos debido a la fragilidad que muchos de éstos presentan y se lo puede definir de la siguiente manera:

En sistemas de información se entiende por amenaza la presencia de uno o más factores de diversa índole (personas, máquinas o sucesos) de tener la oportunidad afectarían al sistema produciéndole daños aprovechándose de su nivel de vulnerabilidad. Hay diferentes tipos de amenazas de las que hay que proteger al sistema, desde las físicas como cortes eléctricos, fallos del hardware o riesgos ambientales hasta los errores intencionados o no de los usuarios, la entrada de software malicioso (virus, troyanos, gusanos) o el robo, destrucción o modificación de la información (Chamorro, 2015).

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 (Silva Coelho, 2018). “Las vulnerabilidades deben ser clasificadas de acuerdo a la clase de activos, es decir: hardware (susceptibilidad a la humedad, polvo, suciedad, almacenamiento sin protección), software (falta de pruebas del software, falta de seguimiento de auditoría), red (líneas inadecuadas, falta de seguridad), sitio (ubicación en un área susceptible a inundaciones, red de energía inestable), y organización (falta de auditorías periódicas, falta de planes de continuidad del negocio)”. (López Uriarte, 2017)

Impacto.

Al respecto de lo que son los impactos y las consecuencias que puede ocasionar, se puede mencionar que: “Son la consecuencia de la materialización de una o más amenazas sobre uno o varios activos aprovechando la vulnerabilidad del sistema o, dicho de otra manera, el daño causado. Los impactos pueden ser cuantitativos, si los perjuicios pueden cuantificarse económicamente, o cualitativos, si suponen daños no cuantificables, como los causados contra los derechos fundamentales de las personas” (Ladino, 2011). Todos los riesgos mencionados pueden suceder dentro de los sistemas informáticos, por lo que se deben tomar las respectivas precauciones para proteger la información.

Análisis de riesgo.

El modelo PDCA

Algunos autores como (Disterer, 2013) y (Bermudez Molina, 2015) coinciden en que, para ejecutar el análisis y posterior gestión del riesgo, se tiene que continuar un ciclo con cuatro etapas conocido por sus siglas en inglés como PDCA (Plan-Do-Check-Act) o Planificar-Ejecutar-Verificar-Actuar, que se ilustra en la Figura 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 la necesidad de la orientación al proceso, así como la integración del planeamiento de las operaciones y la verificación constante de la implementación conforme a la planificación.” (Disterer, 2013). “Los sistemas de gestión de la seguridad de la información formalizan cuatro etapas cíclicas donde el análisis de riesgos es parte de las actividades de planificación, se toman decisiones de tratamiento y estas decisiones se materializan en la etapa de implantación, en la cual se despliegan elementos que acceden la monitorización de las medidas tomadas para poder evaluar la efectividad de las mismas y actuar dependiendo de éstas, dentro de un círculo de excelencia o mejora continua” (Figueroa Moran, 2017).

Figura 1. Etapas del ciclo PDCA según ISO.
Fuente: (Disterer, 2013)

e-ISNN 2550-6730 | Vol. 6, Núm. 1 (60-70): Enero-Junio, 2022 | DOI: 10.33936/isrtic.v6i1.4473

Según (Disterer, 2013), en un Sistema de Gestión de Seguridad de la Información (SGSI), en la etapa de planificación es donde se definirán los requisitos para la protección de la información, se identificarán y evaluarán los riesgos y se desarrollarán los procedimientos y medidas adecuados para reducir los riesgos. Estos procedimientos y medidas se implementan durante la etapa de implementación y operación (o etapa de ejecución). Los informes generados a través del monitoreo continuo de las operaciones (etapa de verificación) se utilizarán en la última etapa (Actuar) para obtener las mejoras y el desarrollo posterior y continuo del SGSI. Estas etapas se resumen en la Figura 1. La mayoría de las metodologías de gestión de riesgos utilizan como base el modelo PDCA (Disterer, 2013), y lo realizan con la propósito de establecer un proceso de gestión que se enfoque en la mejora continua, siguiendo teniendo las siguientes actividades en cada una de sus etapas:

- Planificar: "Se establecen los objetivos, procesos y procedimientos para la gestión de riesgos tecnológicos. El objetivo de esta etapa es la entrega de resultados acordes con las políticas y objetivos globales de la organización. Además, se forma el plan de comunicaciones y el análisis del contexto organizacional actual para limitar el alcance de la gestión de riesgos tecnológicos". (Disterer, 2013)

- 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" (Disterer, 2013).

- Verificar: "En esta etapa se evalúa y se mide la ocupación de los procesos contra la política y los objetivos de seguridad. Además, se debe informar los resultados obtenidos" (Silva Coelho, 2018).

- Actuar: "En esta etapa se establece la política para la gestión de riesgos tecnológicos y se realizan los cambios solicitados 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 los cumplimientos de indicadores establecidos en la etapa de planificación" (Guamán, 2019).

Gestión de riesgo.

La gestión de riesgos radica en el proceso de analizar, evaluar, tratar, monitorizar y comunicar los riesgos encontrados. "La gestión de los riesgos es un desafío estratégico para las organizaciones, las cuales enfrentan amenazas cada vez más complejas y diversas. Caldera y Watkins indican que todas las organizaciones se enfrentan diariamente a riesgos de un tipo u otro" (Silva Coelho, 2018). Se definen a la Gestión de Riesgos como una disciplina no especulativa, que son aquellos riesgos de los cuales sólo puede ocurrir una pérdida; en cambio, los riesgos especulativos son aquellos a partir de los cuales se puede producir una ganancia o una pérdida, que a menudo son estrategias de negocio de la organización (Enríquez Collaguazo, 2018).

La gestión de riesgos, suelen tener cuatro objetivos vinculados (Silva Coelho, 2018), los cuales son:

- Eliminar los riesgos

- Reducir a niveles "aceptables" aquellos riesgos que no pueden eliminarse; y entonces

- Convivir con ellos, ejerciendo cuidadosamente los controles que los mantienen en niveles "aceptables"; o

- Transferirlos, por medio de aseguradoras, por ejemplo, a otra instancia u organización.

Según (Bermudez Molina, 2015), la gestión del riesgo en general consiste en seis procesos: establecimiento del contexto, evaluación del riesgo, tratamiento del riesgo, aceptación de riesgos, comunicación y consulta de riesgos, revisión y seguimiento del riesgo (Bermudez Molina, 2015). Estos procesos y su interrelación se los puede apreciar en la Figura 2.

Figura 2. Proceso de la gestión de riesgo.
Fuente: (Bermudez Molina, 2015).

2.2. Metodología de gestión de riesgo.

Magerit.

Es una de las metodologías más utilizadas en la gestión de riesgos de los Sistemas de Información; fue creada por el Consejo Superior de Administración Electrónica del Ministerio de Hacienda y Administraciones Públicas de España (Ministerio de Hacienda y Administraciones Públicas de España, 2012) para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información siguiendo la terminología de la norma ISO 31000 y, en el año 2012 se actualizó a la versión 3 (Genova Garcia, 2017). La entidad que creo esta metodología, la define como: "Una metodología que ha sido elaborada como respuesta a la percepción de la administración pública (y en general toda la sociedad), depende de forma creciente de los sistemas de información para alcanzar sus objetivos (De la Torre, 2018). Así, menciona que el uso de tecnologías de la información y comunicaciones (TIC) supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben gestionarse prudentemente con medidas de seguridad que sustenten la confianza de los usuarios de los servicios" (Velasco, 2008). Según (Bermudez Molina, 2015), "los objetivos que busca alcanzar esta metodología son los siguientes:

- Innovar que los responsables de los sistemas de información sean conscientes de la existencia de riesgos y de la

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

necesidad de conocer a tiempo.

- Dar un método sistemático para el análisis de riesgos.
- Ayudar en la diseño y planificación de las medidas adecuadas para mantener los riesgos bajo control.
- De forma indirecta, preparar la organización de los procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso".

La metodología se resume en el modelo de la Figura 3.

Figura 3. Modelo Magerit.

El desarrollo de esta esta metodología contempla las siguientes fases:

- Fase 1: definir el alcance. "El primer paso a la hora de llevar a cabo el análisis de riesgos es establecer el alcance del estudio. Vamos a considerar que este análisis de riesgos forma parte del Plan Director de Seguridad. Por lo tanto, recomendamos que el análisis de riesgos cubra la totalidad del alcance del PDS, dónde se han seleccionado las áreas estratégicas sobre las que mejorar la seguridad.
- Fase 2: Identificar los activos. Una vez definido el alcance, debemos identificar los activos más importantes que guardan relación con el departamento, proceso, o sistema objeto del estudio.
- Fase 3: Identificar amenazas. Habiendo identificado los principales activos, el siguiente paso consiste en identificar las amenazas a las que estos están expuestos. Tal y como imaginamos, el conjunto de amenazas es amplio y diverso por lo que debemos hacer un esfuerzo en mantener un enfoque práctico y aplicado.
- Fase 4: Identificar vulnerabilidades y salvaguardas. La siguiente fase consiste en estudiar las características de nuestros activos para identificar puntos débiles o vulnerabilidades.
- Fase 5: Evaluar el riesgo. Disponemos de los siguientes elementos (inventarios de activos, conjunto de amenazas a las que están expuestas los activos, conjunto de vulnerabilidades asociadas a cada activo, conjunto de medidas de seguridad implantadas)" (Chamorro, 2015).

Elementos de Magerit

Los elementos considerados significativos por Magerit para el estudio de los sistemas de información:

- ACTIVOS: "Recursos del sistema de información o relacionados con este, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por la dirección". (López Uriarte, 2017)
- AMENAZAS: "Eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o perdidas inmateriales en sus activos". (Bermudez Molina, 2015)
- VULNERABILIDAD DE UN ACTIVO: "Potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo". (Bermudez Molina, 2015)
- IMPACTO DE UN ACTIVO: "Consecuencia sobre este de la materialización de un activo.
- RIESGO: Posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización.
- SERVICIO DE SALVAGUARDIA: Acción que reduce el riesgo.
- MECANISMO DE SALVAGUARDA: Procedimiento, dispositivo, físico o lógico, que reduce el riesgo". (Silva Coelho, 2018)

La Figura 4 muestra los elementos y sus interrelaciones:

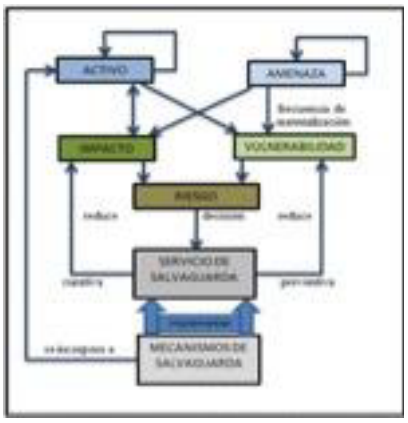

Figura 4. Elementos del Magerit.

e-ISNN 2550-6730 | Vol. 6, Núm. 1 (60-70): Enero-Junio, 2022 | DOI: 10.33936/isrtic.v6i1.4473

Norma ISO/IEC 27002

"La norma internacional ISO/IEC 27002, que se centra en las buenas prácticas para gestión de la seguridad de la información (Armendáriz, 2017). Esta norma se basa en el código de las buenas prácticas para la gestión de la seguridad. Se puede dar recomendaciones sobre qué medidas tomar para asegurar los sistemas de información de una organización. Esta norma también describe los objetivos de control (aspectos para garantizar la seguridad de la información) y especifica los controles recomendables a implantar (medidas tomar)" (Sanchez, 2017).

Principales ítems que componen la ISO 27002:

"La parte principal de la norma se encuentra distribuida en las siguientes secciones, que corresponden a controles de seguridad de la información. Es importante recordar que la organización puede utilizar esas directrices como base para el desarrollo del SGSI" (Silva Coelho, 2018).

Sección 5 – Política de Seguridad de la Información

"Se debe crear un documento sobre la política de seguridad de la información de la empresa, que debe contener los conceptos de seguridad de la información, una estructura para establecer los objetivos y las formas de control, el compromiso de la dirección con la política, entre tantos otros factores" (Genova Garcia, 2017).

Sección 6 – Organización de la Seguridad de la Información

"Para implementar la Seguridad de la Información en una empresa, es necesario establecer una estructura para gestionarla de una manera adecuada. Para ello, las actividades de seguridad de la información deben ser coordinadas por representantes de la organización, que deben tener responsabilidades bien definidas y proteger las informaciones de carácter confidencial" (De la Torre, 2018).

Sección 7 – Gestión de activos

"Activo, según la norma, es cualquier cosa que tenga valor para la organización y que necesita ser protegido. Pero para ello los activos deben ser identificados y clasificados, de modo que un inventario pueda ser estructurado y posteriormente mantenido. Además, deben seguir reglas documentadas, que definen qué tipo de uso se permite hacer con dichos activos" (López Uriarte, 2017).

Sección 8 – Seguridad en recursos humanos

"Antes de la contratación de un empleado – o incluso de proveedores – es importante que sea debidamente analizado, principalmente si se trata de información de carácter confidencial. La intención de esta sección es mitigar el riesgo de robo, fraude o mal uso de los recursos. Y cuando el empleado esté trabajando en la empresa, debe ser consciente de las amenazas relativas a la seguridad de la información, así como de sus responsabilidades y obligaciones" (Romo Villafuerte, 2012).

Sección 9 – Seguridad física y del medio ambiente

"Los equipos e instalaciones de procesamiento de información crítica o sensible deben mantenerse en áreas seguras, con niveles y controles de acceso apropiados, incluyendo protección contra amenazas físicas y ambientales" (Chamorro, 2015).

Sección 10 – Seguridad de las operaciones y comunicaciones

"Es importante que estén definidos los procedimientos y responsabilidades por la gestión y operación de todos los recursos de procesamiento de la información. Esto incluye la gestión de servicios tercerizados, la planificación de recursos de los sistemas para minimizar el riesgo de fallas, la creación de procedimientos para la generación de copias de seguridad y su recuperación, así como la administración segura de las redes de comunicaciones" (Montoya, 2017).

Sección 11 – Control de acceso

"El acceso a la información, así como a los recursos de procesamiento de la información y los procesos de negocios, debe ser controlado con base en los requisitos de negocio y en la seguridad de la información. Debe garantizarse el acceso de usuario autorizado y prevenido el acceso no autorizado a los sistemas de información, a fin de evitar daños a documentos y recursos de procesamiento de la información que estén al alcance de cualquiera" (López Uriarte, 2017).

Sección 12 – Adquisición, desarrollo y mantenimiento de sistemas

"Los requisitos de seguridad de los sistemas de información deben ser identificados y acordados antes de su desarrollo y/o de su implementación, para que así puedan ser protegidos para el mantenimiento de su confidencialidad, autenticidad o integridad por medios criptográficos" (Pacheco Villamar, 2018).

Sección 13 – Gestión de incidentes de seguridad de la información

"Los procedimientos formales de registro y escalonamiento deben ser establecidos y los empleados, proveedores y terceros deben ser conscientes de los procedimientos para notificar los eventos de seguridad de la información para asegurar que se comuniquen lo más rápido posible y corregidos en tiempo hábil" (Disterer, 2013).

Sección 14 – Gestión de continuidad del negocio

"Los planes de continuidad del negocio deben ser desarrollados e implementados, con el fin de impedir la interrupción de las actividades del negocio y asegurar que las operaciones esenciales sean rápidamente recuperadas" (Genova Garcia, 2017).

Sección 15 – Conformidad

"Es importante evitar la violación de cualquier ley criminal o civil, garantizando estatutos, regulaciones u obligaciones contractuales y de cualesquiera requisitos de seguridad de la información. En caso necesario, la empresa puede contratar una consultoría especializada, para que se verifique su conformidad y adherencia a los requisitos legales y reglamentarios" (Guamán, 2019).

2. Materiales y Métodos

La metodología propuesta consistió en la detección, análisis a las

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

vulnerabilidades a las que se ven expuesto la distribuidora, ya que nos permite conocer cada factor que pueda estar poniendo en riesgo a la organización que se está elaborando el estudio.

Una de la parte importante es la información de la empresa, donde se evaluará los puntos críticos en la hora de manejar el riego que tiene cada activo dentro del departamento de TI, de esta manera nos permitirá conocer los niveles de riego de cada uno de los activos.

Las fases que se van a realizar son las siguientes:

● Definir el alcance: Se implementa el ciclo PDCA (Planifica, Hacer, Verificar, Actuar), dentro de este ciclo se logra obtener la información que se necesita para la evaluación del riesgo de los activos, Y poder llevar acabo las acciones correctivas y verificar las planificaciones que se tiene la empresa con el respecto del cuidado de la información.

● Identificar los activos: Una vez ya teniendo hasta donde se puede llegar, con la evaluación dentro de la empresa, podemos identificar los activos que están en riesgo como se evidencia en la Tabla 1.

Tabla 1. Identificación de activo de la distribuidora Bravel.
Fuente: Los autores.

ITEM	TIPO DE ACTIVO	ACTIVO
1	Información	Datos de los clientes
2	Equipo informático (hardware)	Servidor de base de dato, Pc's, impresora, Servidor de Intranet, Firewall, Router.
3	Red de comunicación	Red inalámbrica
4	software	Herramienta a utilizar para el desarrollo de las actividades (sistema).
5	Equipamiento Auxiliar	Fibra Óptica, Aire Acondicionado
6	Personal	Responsables del área de ti

Amenazas: Acorde a la metodología Magerit catálogos de elementos, hace referencia a:

D=disponibilidad, C=confidencialidad, A=autenticidad y

T=trazabilidad para dar significado al activo de la empresa. En donde cada nivel de riesgo toma un valor de una escala de 1-5. Las amenazas se presentan en la Tabla 2.

Tabla 2. Identificación de valoración de las amenazas de la distribuidora Bravel.
Fuente: (Armendáriz, 2017).

Ítem	Activos críticos	Dimensiones de valoración				
		C	I	D	A	T
1	Servidor de base de datos	5	5	5	5	5
2	Redes de datos	5	5	5	5	5
3	Servidor proxy	5	5	5	5	5

Identificar vulnerabilidad y salvaguardas: La información suministrada por el personal encargado del área de TI, se pudieron identificas las siguientes salvaguardas: Backup Se tiene como procedimiento establecido las copias de seguridad como factor fundamental para salvaguardar la información como se presenta en la Tabla 3.

Mantenimiento de hardware: se tiene como prioridad los días o fechas que se tiene para el óptimo Funcionamiento.

En el estudio que se realizó en la empresa, se pudieron identificar las amenazas y vulnerabilidades con respecto, a los activos críticos identificados.

Tabla 3. Identificación de Vulnerabilidades de la distribuidora Bravel.
Fuente: Los autores.

Item	Activos	Vulnerabilidades	Amenazas
1	Servidor de base de datos	Fallos del sistema eléctrico	Perdida de la información
			Incendio
2	Red de datos	Manipulación de la red	Interrupción en las actividades
			Perdida de la información
4	Servidor proxy	Ataques internos	Manipulación de la información

Evaluar el riesgo: Dentro de la evaluación que se realizó dentro de la empresa, se estable los valores del riesgo, que se presenta en los activos de la organización que se realizó el estudio, como se observa en la Figura 5 y Tabla 4 a continuación.

e-ISNN 2550-6730 | Vol. 6, Núm. 1 (60-70): Enero-Junio, 2022 | DOI: 10.33936/isrtic.v6i1.4473

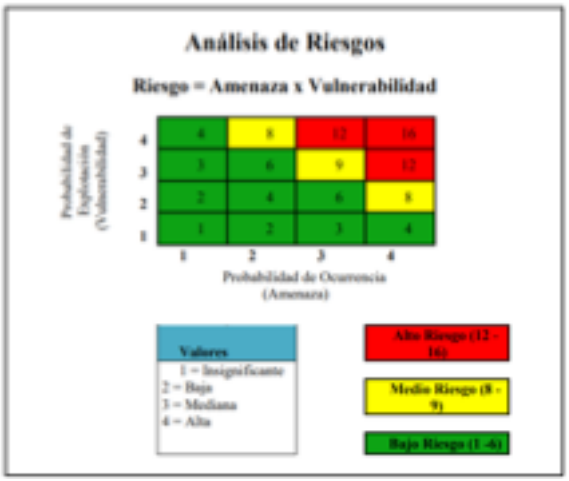

Figura 5. Análisis de riesgo.
Fuente: (Genova Garcia, 2017)

Tabla 4. Identificación de Riesgo de la distribuidora Bravel.
Fuente: Los autores.

Item	Activos	Vulnera-bilidades	Amenazas	Probabili-dad	Item
1	Servi-dor de base de datos	Fallos del sistema eléctrico	Deterior o del gabi-nete cortocir-cuito	3	3
2	Red de datos	Manipu-lación de la red	Interrup-ción en las actividades Perdida de la infor-mación	3	4
3	Ser-vidor proxy	Ataques internos	Manipu-lación de la infor-mación	3	4

3. Resultados y Discusión

Después de la evaluación de las 3 formas para poder evaluar la distribuidora, nos permite llegar a una nueva metodología. Que consta en los siguientes:

Fase 1: Revisión manual: En esta fase se realizará el proceso de análisis y evaluación de riesgos de acuerdo al estándar MAGERIT que permite valorar los riesgos en cada uno de los criterios de información evaluados, identificando las posibles causas que los originan y que posteriormente permitan definir un sistema de control de seguridad de acuerdo a los hallazgos confirmados, lo que permitirá disminuir el impacto en la organización y probabilidad de ocurrencia de los mismos. El proceso de análisis y evaluación de los riesgos se lleva a cabo teniendo en cuenta el estándar MAGERIT versión 3.0, que permite hacer la clasificación de amenazas y riesgos, los activos informáticos, muestra las escalas de valoración y los criterios de información que será evaluados.

Posteriormente se aplican las listas de chequeo que son utilizadas para verificar y determinar la existencia de controles de seguridad informática y de la información, diseñadas de acuerdo a la norma ISO/IEC 27002, la cual observaremos los riesgos que está presentando a organización y también si cumple con cada uno de los objetivos de control que tiene la norma como se observa en la Figura 6.

Figura 6. ISO/IEC 27002, dominio, objetivo de control y controles.
Fuente: www.iso27000.es/assets/files/ControlesISO27002-2013.pdf.

Fase 2: Elección del software a aplicar: En esta fase se va tener en cuenta 2 software para la respectiva comparación, que son eMarisma e ISOtolls, la cual nos permite conocer el riesgo de la organización de cada uno de los activos y el manejo de la información que se encuentra en el departamento de TI, y conocer el riesgo que tiene la distribuidora.

Fase 3: implementación del software eMarisma: en esta fase se implementa el software la cual se debe realizar unos pasos antes de la realización de la evaluación, debemos realizar primeramente el proyecto de estudio que se va a realizar, una vez ya realizado se debe realizar una nueva auditoría para proceder a crear cada uno de los activos que tiene la organización para después realizar un agrupamiento para poder tenerlo relacionado con cada uno del proceso a examinar.

Por último, se debe realizar el SOA (arquitectura orientada a servicios), es el nexo que une las metas de negocio con el sistema de software. Su papel es el de aportar flexibilidad, desde la automatización de las infraestructura y herramientas necesarias consiguiendo, al mismo tiempo, reducir los costes de integración. SOA se ocupa del diseño y desarrollo de sistemas distribuidos y es un potente aliado a la hora de llevar a cabo la gestión de grandes volúmenes de datos, datos en la nube y jerarquías de datos. Ver Figuras 7, 8 y 9 a continuación.

e-ISNN 2550-6730 | **Vol. 6, Núm. 1 (60-70): Enero-Junio, 2022** | **DOI: 10.33936/isrtic.v6i1.4473**

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

Figura 7. Ingreso de los activos que tiene la distribuidora.

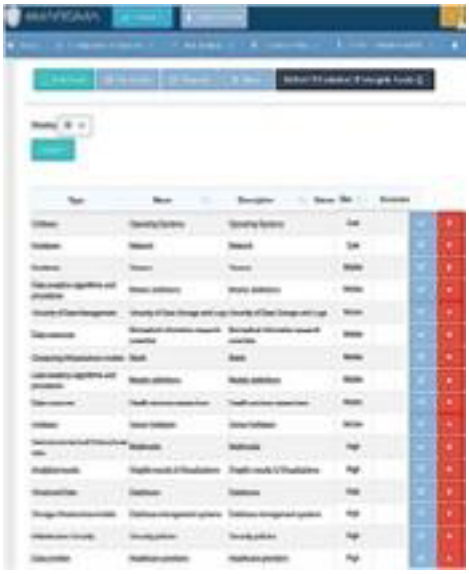

Figura 7. Activos para el uso del caso agregados en la herramienta eMARISMA.

4. Conclusiones

La investigación realizada demuestra que no existe una cultura de seguridad dentro de la distribuidora; por esta razón tampoco existe sistemas de control de seguridad informática y de información, y mucho menos, procesos y procedimientos documentados para protección de la información.

Por tanto, es fundamental que las organizaciones cuenten con un marco normativo de seguridad, que permita aplicar la auditoría basada en la norma ISO/IEC 27002.

La seguridad de la información se concluye que este proceso

Figura 9. Cuadro de mando generado por la herramienta eMARISMA para nuestro caso de estudio.

debe ser continuo y que debe ser realizado por los entes de control interno de la organización, y periódico, implementación de un SGSI adecuado a sus necesidades.

Es necesario realizar una constante actualización y búsqueda de las mejores herramientas disponibles para la detección de amenazas a las que se exponen los activos.

Contribución de los autores

María Angélica Velepucha Sánchez: Conceptualización, Metodología, Análisis formal. **Jéssica Morales Carrillo:** Metodología, Análisis formal, Revisión y edición del artículo. **Marco Fernando Pazmiño Campuzano:** Metodología, Revisión y edición del artículo.

Conflictos de interés

Los autores declaran no tener ningún conflicto de interés.

Referencias bibliográficas

Armendáriz, D. N. L. (2017). Modelo de gestión de los servicios de tecnología de información basado en COBIT, ITIL e ISO/IEC 27000. *Revista Tecnológica-ESPOL, 30*(1).

Bermúdez Molina, K. G. (2015). Análisis en seguridad informática y seguridad de la información basado en la norma ISO/IEC 27001-sistemas de gestión de seguridad de la información dirigido a una empresa de servicios financieros. https://dspace.ups.edu.ec/handle/123456789/10372

Aguayo Chamorro, C. R. (2015). Propuesta para un adecuado

e-ISNN 2550-6730 | Vol. 6, Núm. 1 (60-70): Enero-Junio, 2022 | DOI: 10.33936/isrtic.v6i1.4473

manejo de la seguridad de la información en base a la norma ISO 27002 para la Dirección de Gestión Tecnológica del Ministerio del Deporte, Quito. http://bibdigital.epn.edu.ec/handle/15000/12650

De la Torre, C. (2018). *SCP progreso.* Obtenido de https://www.scprogress.com/NOTICIAS/CyberNoticia47-20170824.pdf

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information. *Scientific Research An Academic publisher,* 92-100. http://dx.doi.org/10.4236/jis.2013.42011

Enríquez Collaguazo, A. A. (2018). *Repositorio Digital Unversidad Técnica del Norte.* Obtenido de http://repositorio.utn.edu.ec/handle/123456789/8572

Figueroa Moran, G. L. (2017). *Repositorio digital UNESUM.* Obtenido de http://repositorio.unesum.edu.ec/handle/53000/980

Silva Coelho, F. E. (2018). *Gestión de la Seguridad de la informacion.* Colombia: ebook. Obtenido de https://www.cedia.edu.ec/assets/docs/publicaciones/libros/GTI8.pdf

Genova Garcia, L. Z. (2017). Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información. *UNE-EN normalizacion español,* 13-22. https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0058429

Guamán, V. L. (2019). *Evaluación de seguridad de la información aplicado al sistema de evaluación de docentes de la Universidad Técnica del Norte basado en la ISO 27002:2017 con la metodología Magerit V3.* Ibarra: Universidad Tecnica del Norte. http://repositorio.utn.edu.ec/handle/123456789/9535

Mora Palacios, J. P. (2017). Desarrollo y Adaptación de COBIT 5 como metodología de gestión de riesgos a la norma ISO/IEC 27001, utilizando el proceso APO12. *GIS Gestión, Ingenio y Sociedad*, 18-37. http://gis.unicafam.edu.co/index.php/gis/article/view/22/70

López Uriarte, E. D. (2017). *Evaluación de la Red Inalámbrica en el Hospital Escuela Cesar Amador Molina, basado en la norma IEEE 802.11 y controles de seguridad del estándar ISO 27002-2013 Matagalpa, I semestre 2015.* Managua: Universidad Nacional Autónoma de Nicaragua. http://repositorio.unan.edu.ni/id/eprint/3198

Ladino, M. I., Villa, P. A., & López, A. M. (2011). Fundamentos de ISO 27001 y su aplicación en las empresas. *Scientia et technica, 17*(47), 334-339.

https://www.redalyc.org/pdf/849/84921327061.pdf

Montoya, Y. A. (2017). *Repositorio Escuela Superior Politécnica del Litoral.* Obtenido de http://www.dspace.espol.edu.ec/xmlui/handle/123456789/38692

Pacheco Villamar, R. A. (2018). *Repositorio Digital de la Universidad Espiritu Santo.* Obtenido de http://repositorio.uees.edu.ec/handle/123456789/3059

Pazmiño Flores, C. D. (2019). *Repositorio de la Universidad Internacional SEK ecuador.* Obtenido de https://repositorio.uisek.edu.ec/handle/123456789/3345

Romo Villafuerte, D. &. (2012). *Repositorio Institucional de la Universidad Politécnica Salesiana* . Obtenido de https://dspace.ups.edu.ec/handle/123456789/3163

Sanchez, J. D. (2017). *Secretaria general de industria y de la pequeña y mediana empresa.* Obtenido de https://static.eoi.es/inline/une-en_iso-iec_27002_norma_mincotur.pdf

Solarte, F. N. S., Rosero, E. R. E., & del Carmen Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica-ESPOL, 28*(5).

Salazar Choez, T. K. (2018). *REPOSITORIO UNESUM.* Obtenido de http://repositorio.unesum.edu.ec/bitstream/53000/1469/1/UNESUM-ECU-REDES-2017-01.pdf

Velasco, M. A. (2008). El derecho informático y la gestión de la seguridad de la información una perspectiva con base en la Norma ISO 27 001. *Revista de derecho,* 320. https://www.redalyc.org/articulo.oa?id=85102913

e-ISNN 2550-6730 | **Vol. 6, Núm. 1 (60-70): Enero-Junio, 2022** | **DOI: 10.33936/isrtic.v6i1.4473**