UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

*Resolución: **RPC-SO-02-No.053-2021***

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del proyecto:
PROPUESTA DE UN MODELO DE GESTIÓN DE RIESGOS DE LA INFORMACIÓN EN SERVIENTREGA ECUADOR S.A
Línea de Investigación:
SEGURIDAD INFORMÁTICA
Campo amplio de conocimiento:
TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
Autor:
Cevallos Campaña Oswaldo Alejandro
Tutor:
Recalde Varela Pablo Marcel

Quito – Ecuador

2023

APROBACIÓN DEL TUTOR

Yo, Pablo M Recalde V con C.I: 1711685055 en mi calidad de Tutor del proyecto de investigación titulado**: PROPUESTA DE UN MODELO DE GESTIÓN DE RIESGOS DE LA INFORMACIÓN EN SERVIENTREGA ECUADOR S.A**

Elaborado por: Oswaldo Alejandro Cevallos C, de C.I:1718957267, estudiante de la Maestría: Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2023

_____

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Oswaldo Alejandro Cevallos C con C.I: 1718957267, autor del proyecto de titulación denominado **PROPUESTA DE UN MODELO DE GESTIÓN DE RIESGOS DE LA INFORMACIÓN EN SERVIENTREGA ECUADOR S.A**. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., marzo de 2023

_____

Firma

orcid: 0000-0003-2751-0695

Tabla de contenidos

Índice de tablas

Índice de Anexos

Índice de Gráficos

INFORMACIÓN GENERAL

Contextualización del tema

Desde el año 2020, en Servientrega Ecuador S.A. se ha venido trabajando en la gestión de seguridad de la información en conjunto con el departamento de procesos y tecnología se ha identificado que bajo su cargo se encuentra mucha información sensible y de uso exclusivo la cual debe ser tratada con mucho cuidado, los clientes posan su confianza en que dicha información va a tener un tratamiento seguro y que existen los lineamientos necesarios para hacerlo.

Acorde al modelo de Sistemas de Gestión de Seguridad de Servientrega. (12 de agosto de 2016), el tratamiento de esta información conlleva varios aspectos que deben tener un procedimiento estipulado dentro del sistema de gestión de seguridad de la información, que pueda garantizar la privacidad e integridad de los datos con cada uno de los actores internos y externos que interactúan en los procesos de la empresa.

Esta información en la actualidad es uno de los activos más valiosos de la empresa por la cantidad de clientes que nos confían su información personal, al igual que los equipos de computación, aplicativos web y servidores, el conjunto de todos estos elementos deben tener un tratamiento único y asegurar su funcionalidad en todo momento, para esto es necesario que la transmisión, recepción y funcionamiento tengan controles constantes y puedan ser auditados en cualquier momento.

Un sistema de gestión de seguridad de la información, puede garantizar que la empresa implemente este tipo de controles constantes y las herramientas necesarias para que se cumplan, claro que el costo de estas herramientas puede llegar a ser representativo para la organización, pero se debe evaluar qué tan importante es la seguridad de la información para con los clientes, para le empresa y para la sociedad.

Dentro de un SGSI uno de los primeros pasos a seguir es el levantamiento de una matriz de riesgos los mismos que deben ser analizados, evaluados y ponderados por categorías, esto permitirá un diagnóstico de las debilidades y fortalezas que en la actualidad existen en los procesos de la empresa, y facilitará que se puedan implementar una política adecuada y los controles necesarios para garantizar que la información está segura.

Problema de investigación

Servientrega Ecuador S.A. en la actualidad carece de un sistema de seguridad de la información que le permita gestionar las vulnerabilidades, riesgos y amenazas a las que se encuentra expuesta en cada uno de los procesos de la empresa, falta un proceso

para el tratamiento de dichos riesgos y se encuentra completamente a la deriva la integridad, disponibilidad y confidencialidad de la información de los clientes.

En la actualidad el proceso de tecnología es quien ha implementado ciertos mecanismos de seguridad que permiten mitigar y precautelar la información que se recibe día a día al momento que los clientes de los canales Retail y corporativo generan un envío por las herramientas digitales, no existe una política de seguridad de claves de acceso a los equipos de cómputo, no se tiene una directriz definida para el ingreso a los servidores, actualmente se lo maneja de manera empírica el proceso de creación, actualización y cambios en las bases de datos sin existir ningún documento que respalde dicho procedimiento.

Diariamente se reciben miles de envíos y cada uno de ellos contiene información sensible de remitentes y destinatarios los cuales realizan envíos de documentos y mercancías, el crecimiento de envíos de documentos sensibles también está creciendo en la actualidad con las negociaciones con entidades financieras que requieren la distribución de tarjetas de crédito y estados de cuenta físico, al igual que el manejo de información de los clientes de entidades públicas a nivel nacional, por este motivo se ve la necesidad de implementar un proceso de seguridad de la información con políticas, directrices y procedimientos que regulen el correcto manejo de la información en cada uno de los procesos y con cada uno de los empleados de la compañía.

Para lograrlo es indispensable realizar un análisis de riesgos de la seguridad de la información e incluir todos los actores directos e indirectos que tienen algún tipo de interacción con la información sensible de los clientes.

La alta dirección está totalmente comprometida con la implementación de un sistema de gestión de seguridad de la información y sabe que si no se siguen estos lineamientos en el futuro esta información puede correr más riesgo del que actualmente corre.

¿Si se implementa un SGSI se puede garantizar el correcto manejo de la información física y digital de los clientes?

Objetivo general

Proponer un modelo de gestión para el análisis de riesgos en seguridad de la información en Servientrega Ecuador S.A, mediante la comparativa de metodologías de gestión de riesgos.

Objetivos específicos

- Identificar los requerimientos necesarios que interactúan en el proceso de implementación de la gestión de riesgos mediante el diagrama organizacional.
- Seleccionar entre metodologías de análisis de riesgos mediante un cuadro comparativo la que más se ajuste a la realidad de la organización.
- Proponer un modelo de gestión de riesgos de seguridad de la información según la metodología seleccionada, que nos permita mitigar los riesgos encontrados.
- Realizar un informe donde se muestran los hallazgos y las recomendaciones que permitan la correcta implementación de un sistema de gestión de seguridad de la información acorde a las necesidades de Servientrega Ecuador S.A.

Vinculación con la sociedad y beneficiarios directos:

En la actualidad Servientrega Ecuador S.A. maneja una cantidad muy alta de envíos de empresas públicas, privadas y personas naturales y mantiene un control de sus procesos mediante un sistema de gestión de calidad ISO 9001-2015, esto permite que se tenga una base para el mantenimiento documental de la información y seguimiento constante de los procesos.

Este trabajo de investigación coopera con el Objetivo de Desarrollo Sostenible número nueve “Construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación”. (ODS, 2017)

Teniendo en cuanta lo antes expuesto se ve viable que se siga el mismo camino de implementación de un sistema de gestión de seguridad de la información basándose en la norma ISO 27000-2014 que permite que se implemente políticas, planes y controles de aseguramiento de la información y garantizar la continuidad del negocio en el proceso, en importante alinear los objetivos de calidad actuales que permitan asegurar la confidencialidad, disponibilidad e integridad de la información en cada uno de los procesos.

El primer paso a seguir dentro de una implementación de un SGSI es realizar un análisis de riesgos de seguridad de la información, acorde al modelo propuesto por la norma y basándonos en los procesos implementados en la actualidad y en la matriz de riesgos del sistema de gestión de calidad.

Al realizar un análisis de los riesgos de seguridad de la información podemos asegurar que la empresa maneja de manera eficiente la información de los clientes y que esto representa una fortaleza en las negociaciones con nuestros clientes corporativos de empresas privadas y públicas ya que en la actualidad por la ley de protección de datos personales es una obligación para todas estas empresas manejar un modelo de aseguramiento de la información para sus clientes y permiten que una certificación de un proveedor sea un buen punto de partida para aumentarla confianza en el servicio.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

Descripción de los métodos, necesidades y pasos a seguir antes de plantear un modelo de gestión de riesgos

1.1. Contextualización general del estado del arte

En las empresas Courier nacionales aún no se han implementado sistemas de seguridad de la información, gracias al caso exitoso que se evidencia en Servientrega Colombia, se toma como punto de partida dicha documentación que detalla una «ley de protección de datos personales» esta documentación se encuentra amparada en las disposiciones de la ley 1581 del año 2012 que en su artículo 1 detalla el Objeto de dicha ley: «La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.» Y el artículo 13 del decreto 1377 que en su Capítulo III dice «Artículo 13. Políticas de Tratamiento de la información.

Los responsables del tratamiento deberán desarrollar sus políticas para el tratamiento de los datos personales y velar porque los Encargados del Tratamiento den cabal cumplimiento a las mismas.

Las políticas de Tratamiento de la información deberán constar en medio físico o electrónico, en un lenguaje claro y sencillo y ser puestas en conocimiento de los Titulares. Dichas políticas deberán incluir, por lo menos, la siguiente información:

- Nombre o razón social, domicilio, dirección, correo electrónico y teléfono del Responsable.
- Tratamiento al cual serán sometidos los datos y finalidad del mismo cuando esta no se haya informado mediante el aviso de privacidad.
- Derechos que le asisten como Titular.
- Persona o área responsable de la atención de peticiones, consultas y reclamos ante la cual el titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.
- Procedimiento para que los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización.
- Fecha de entrada en vigencia de la política de tratamiento de la información y período de vigencia de la base de datos.

Cualquier cambio sustancial en las políticas de tratamiento, en los términos descritos en el artículo 5° del presente decreto, deberá ser comunicado oportunamente a los titulares de los datos personales de una manera eficiente, antes de implementar las nuevas políticas.» Servientrega. (12 de agosto de 2016).

Las empresas locales como “Urbano Express”, “Tramado Express”, “Laar Courier”, aún no ha empezado en el tratamiento de la protección de datos personales, según el acta levantada con los gerentes de cada una de las empresas Anexo-6 y los métodos de seguridad de la información están a cargo del departamento de tecnología de cada una de estas empresas, con protecciones perimetrales, anti spams, firewalls de última generación y antivirus. (ASEMEC, 2021)

Es necesario definir cuáles son los activos más importantes para la organización y determinar los lineamientos de seguridad que se debe seguir para precautelar dichos activos de información.

La seguridad debe ser planteada tanto desde la parte física como la lógica determinando cada uno de los planes, políticas y normativas a seguir, según los pilares de la gestión de seguridad de la información donde se aplican barreras con la finalidad de proteger los datos y permitir el acceso solo al personal autorizado.

Este proceso consiste en implementar un conjunto de técnicas que se encuentran destinadas a la protección de los datos preservando su confidencialidad, permitiendo que esta esté disponible cada vez que sea necesario y previniendo que sean alterados.

1.2. Proceso investigativo metodológico

A continuación, se explica el proceso de investigación a partir de los siguientes elementos.

Enfoque de la investigación

Según la interpretación de Hernández, R. F. (2014) el método cualitativo es inductivo ya que permite recolectar datos para responder las preguntas de la investigación o en su caso formular nuevas preguntas.

Tipo de investigación

La investigación realizada es de tipo aplicada y explicativa, según la Metodología de la Investigación de **Hernández** se va a realizar una exploración de los mecanismos o estrategias más adecuados para cumplir un objetivo, intentado determinar las causas o consecuencias de un fenómeno específico.

Con la investigación comparativa se realizó una comparación las características de las metodologías Octave y Magerit, con la finalidad de encontrar la más adecuada a la realidad de la empresa

Población y muestra

El presente trabajo determina como población el equipo de tecnología de la empresa Servientrega Ecuador S.A., ya que ellos son los encargados al momento de manejar las seguridades de los sistemas de información de la compañía.

$$n = \frac{N \cdot Z^2 \cdot p \cdot (1-p)}{(N-1) \cdot e^2 + Z^2 \cdot p \cdot (1-p)}$$

Para la muestra cualitativa se consultó con las personas encargadas de mantener el sistema de gestión de calidad de la empresa mediante encuestas en Microsoft forms.

Métodos

Método inductivo

Se utilizará este método de investigación, ya que partiremos de premisas particulares para generar conclusiones generales que se adapten al sistema de gestión de calidad actualmente implementado. (Quesada, 2020).

Método deductivo

Esta metodología va de lo particular a lo general permitiendo obtener conocimientos generalizados desde una premisa particular (Arellano, 2015)

Se emplea el método deductivo en la generación de una matriz de riesgos según los problemas puntuales que se encuentra en el proceso de tecnología, y enfocándose a resolver los problemas de los usuarios de la compañía.

1.3. Análisis de resultados

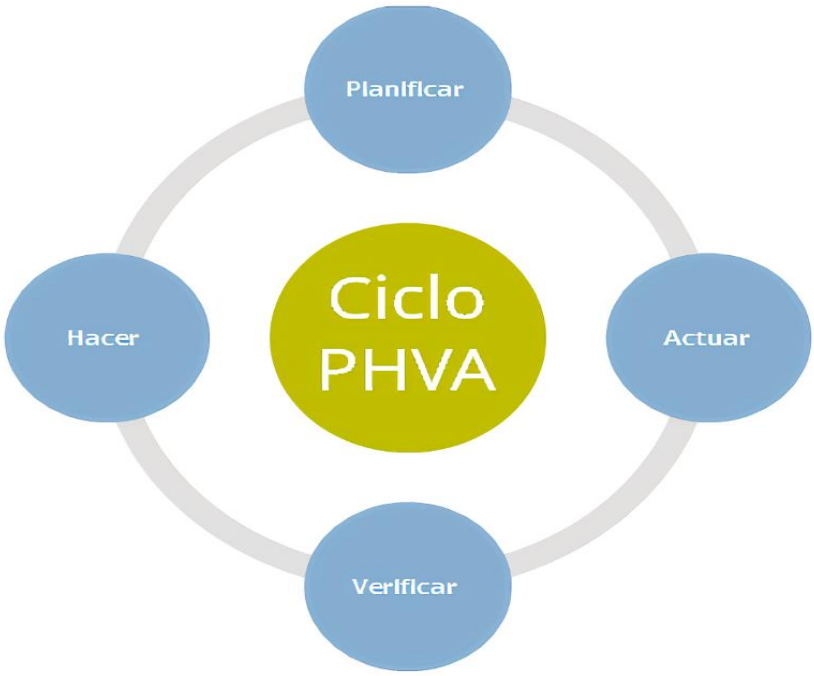
En el marco de la investigación aplicada, se plantean varias actividades que nos permitirán diseñar un proceso de análisis de riesgos y que se pueda concluir con una matriz acorde a los requerimientos de la alta dirección.

Según el modelo propuesto por ISO 27001 se pueden ejecutar las actividades en cuatro etapas que están distribuidas de la siguiente manera:

- Planificación.
- Análisis de riesgos
- Gestión de los riesgos
- Acciones a tomar.

Para ejecutar un análisis de riesgos se adoptará el ciclo de mejora continua PHVA según recomendación de la norma ISO/IEC 27001, el ciclo de Deming está enfocado en la mejora continua del proceso y se lo detalla según la Figura1.

Figura 1
Ciclo PHVA.



Nota: Excellence, I. (21 de mayo de 2015).

CAPÍTULO II: PROPUESTA

Se desarrollará la propuesta del tema de investigación que se planteó como: PROPUESTA DE UN MODELO DE GESTIÓN DE RIESGOS DE LA INFORMACIÓN EN SERVIENTREGA ECUADOR S.A

2.1. Fundamentos teóricos aplicados

Sistema de Gestión de Seguridad de la información (SGSI) es el encargado de proveer los mecanismos y herramientas necesarias con el único objetivo de conocer el interior de la una organización, con el afán de evidenciar a que puede estar expuesta su información, permitiendo definir el método adecuado para gestionar los riesgos según el marco legal de la empresa, y cumpliendo con el ciclo de Deming de mejora continua según la política establecida en la organización y tal como lo solicita la norma ISO 27001. (Excellence, I., 21 de mayo de 2015)

El proceso de seguridad de la información será el encargado de velar y proteger los activos informáticos con el fin de cumplir sus tres pilares fundaméntales, independientemente del tamaño, giro de negocio o razón social de la organización. Análisis de Gestión de Riesgos:

Según Leonardo Sena, S. M. (2004). en su libro «Introducción a Riesgo Informático»; se define como: «Riesgo se puede definir como aquella eventualidad que imposibilita el cumplimiento de un objetivo.

De manera cuantitativa el riesgo es una medida de las posibilidades de incumplimiento o exceso del objetivo planteado. Así definido, un riesgo conlleva dos tipos de consecuencias: ganancias o pérdidas»

- **Confidencialidad:** Está basada en que la información solo debe ser accesible para el personal necesario y autorizado, definiendo procedimientos de control y autorización, está diseñada para mantener en secreto la información y recursos que sean especificados por la compañía.
- **Disponibilidad:** Se enfoca en la necesidad que la información se encuentre constantemente disponible sin que la información sufra algún tipo de degradación en el acceso y ofrecer los recursos necesarios cuando los usuarios autorizados lo requieran.
- **Integridad:** Toda la información debe ser inalterable y se debe prevenir accidentes o intentos maliciosos de modificar la información.

Metodologías para el análisis de riesgos

- **Metodología de Análisis y Gestión de Riesgos de los sistemas de información (MAGERIT):** método cubre el Análisis y Gestión de Riesgos, siendo el núcleo de todo el proceso organizativo; «esta metodología tiene una visión estratégica global de la Seguridad de los Sistemas de Información ISO 27001, esta visión comienza en un modelo de análisis y gestión de riesgos que comprende tres modelos: entidades, eventos y procesos definidos.» (Gómez, J. C. 2012)
- **Operational Critical, Threat,Asset and Vulnerability Evaluation (OCTAVE):** en su traducción es una evaluación operativa crítica, de amenazas, de activos y vulnerabilidades; mediante esta metodología el sector corporativo, tecnología y logística puedan trabajar en conjunto con el único propósito de enfocarse en las necesidades que establezca la seguridad permitiendo que se equilibren los aspectos de riesgos operativos, tecnológicos y la práctica. (Excellence, I., 16 de marzo de 2015)

Metodología de verificación

Una de las etapas más importantes de la seguridad de los sistemas informáticos es la identificación, análisis y tratamiento de los riesgos de la organización, se utilizará OCTAVE como una metodología de gestión de riesgos más utilizada y MAGERIT al ser una metodología desarrollada por el Consejo de Administración electrónica.

Activos de Información

Son todos los recursos que la alta dirección ha propuesto para que la empresa funcione correctamente y cumpla con los objetivos.

Se considera a un activo de información a todos los datos que son utilizados y creados por alguno de los procesos de la empresa en un medio digital, papel u otro medio.

El software y hardware que la organización haya definido para la recepción, transporte y almacenamiento de la información, todos los servicios que se utilicen para la transmisión y control de la información.

Las herramientas tecnológicas que permiten el correcto desarrollo de las actividades y el soporte de los sistemas de información, las personas que utilizan dichos datos o que tengan un conocimiento importante para la empresa.

- **Infraestructura tecnológica**

Se puede definir con un conjunto de hardware y software sobre el cual funcionan los servicios de la organización permitiendo responder eficientemente a las necesidades de sus clientes internos y externos, en la actualidad se agrega una nueva prioridad a las redes o líneas de comunicación.

- **Accesos**

La gestión de accesos indica que se debe conceder el acceso a la información y a la red teniendo en cuenta los requisitos de la organización mediante una política de control de acceso que especifica los procedimientos de inicio seguro y restricciones.

- **Usuarios**

Están directamente relacionadas a la infraestructura tecnológica, comunicación y administración de la información, es importante que el SGSI establezca los controles necesarios para que se minimicen los riesgos relacionados a la información y su infraestructura trabajando sobre los pilares fundamentales de la seguridad y los modelos propuestos de análisis de riesgos.

2.2. Descripción de la propuesta

En el proceso de Gestión de Riesgos basados en la norma ISO 31000, donde se nos proporciona los principios y directivas eficaces para el tratamiento de riesgos, es la norma referente para la identificación, evaluación y tratamiento de riesgos de la organización.

En base a la norma ISO 31000 podemos aplicar la gestión de riesgos orientado a la ISO 27000 que se enfoca en “la información como el activo más importante de las personas y de la organización” (Excellence, I., 16 de marzo de 2015)

La correcta gestión y buenas prácticas de seguridad pueden lograr que la información esté protegida ante eventos naturales, deliberados o fortuitos.

La seguridad no solo debe estar apoyada por herramientas tecnológicas también se debe respaldar en procedimientos que permitan una gestión adecuada de la seguridad de la información.

El riesgo está definido como «La estimación del grado de exposición en el que una amenaza se materializa» (Rodríguez, 7 de mayo de 2020)y esto puede ser sobre uno o más activos de la organización causando daños y pérdida para la misma.

La identificación del riesgo nos permite saber qué es lo que podría pasar si los activos no se encuentran protegidos de manera correcta para esto es importante saber las características de cada activo y el peligro que pueden correr.

El análisis de los riesgos es un proceso sistemático que permite realizar una estimación de la magnitud de un riesgo, realizando una ponderación de los riesgos sobre los activos permitiéndonos saber qué tan protegidos se encuentran los activos.

Los activos de la empresa están relacionados directamente a la política, misión y visión de la organización y las actividades que nacen de la gestión de riesgos permitirán que se elabore un plan de seguridad acorde a las necesidades y objetivos de la organización, de los empleados y de la alta dirección.

En Servientrega Ecuador S.A. al momento se trabaja con un sistema de gestión de calidad basado en una norma internacional ISO 90001 en su versión 2015, la misma que ya cuenta con una matriz de riesgos según el SGC, nos basaremos en dicha matriz en su estructura con la finalidad de mantener el mismo formato que los procesos ya conocen.

Para realizar una evaluación de los riesgos en seguridad de la información se pueden utilizar varias metodologías que son aceptadas por la norma internacional, en nuestro caso realizaremos la evaluación mediante una comparativa de dos metodologías que permitirán que se pueda seleccionar la más adecuada según el modelo de gestión y la estructura organizacional.

Comparativa entre Octave y Magerit

Antes de comparar estas dos metodologías es importante saber a qué se refiere cada una de ellas:

- Magerit: Esta metodología está enfocada en la administración pública y fue elaborada por el «Consejo Superior de Administración Electrónica.»
- Octave Esta metodología se basa en un conjunto de herramientas, técnicas y métodos enfocado en la planificación y evaluación de los riesgos.

Se realiza una tabla comparativa entre las dos metodologías con la finalidad de conocer a qué se refieren cada una de ella, como difieren y cuáles son los pasos a seguir en cada una de ellas, como se muestra en la Tabla 1.

Tabla 1
Comparación de metodologías

Criterio de comparación	Magerit	Octave
Versiones	Existen tres versiones	Dependiendo de la organización se puede implementar las siguientes versiones: ● Octave ● Octave – s ● Octave Allegro
Objetivos	Implantar conciencia en los usuarios responsables del tratamiento de la información que existen riesgos y que es necesario detenerlos a su debido tiempo. Brindar un método que permita analizar los riesgos de forma sistemática. Descubrir y planificar los pasos a seguir para implantar las medidas necesarias para mantener un control sobre los riesgos encontrados. Realizar el proceso de auditoría y certificación y mantener a la organización preparada para los mismos.	Octave tiene como objetivo que la organización desarrolle una perspectiva en cada uno de los procesos y sus niveles con la finalidad de que la implementación sea sencilla.
Fases o tareas	Se detallan dos etapas específicas en el proceso. ● Análisis de riesgos ● Gestión de riesgos	Se desarrollan fases de las cuales se desprenden procesos adicionales. ● Fase 1 ● Fase 2 ● Fase 3
Inicio del método	El proceso metodológico inicia con el análisis de riesgos, la detección de los activos, su importancia y amenazas sobre cada uno de ellos	Se identifican cuatro procesos, sobre los cuales se dan distintos puntos de vista con respecto a: ● Los activos y su criticidad ● Áreas importantes ● Requerimientos ● Estrategias de protección actuales ● Vulnerabilidades Identificación de la información a nivel de la alta dirección.
Detección de amenazas	● Estimación de riesgos Impacto ● Tiempo de ocurrencia ● Probabilidad de la amenaza	Organización de los perfiles de las amenazas según los activos que se designaron críticos.
Evaluación de riesgos	Se considera la probabilidad, el impacto, el tipo de riesgo y que se debe hacer sobre cada riesgo	Se determina los sistemas importantes sobre activos críticos, sus vulnerabilidades, sus componentes clave

Criterio de comparación	Magerit	Octave
		y finalmente se evalúa componente sobre dos procesos identificados.
Salvaguardas	Se planifica cómo detener el impacto y el riesgo	Se determina acciones, planes y estrategias sobre los activos críticos
Presentación de resultados	Para finalizar la matriz de riesgos se analiza las pérdidas y ganancias según la alta dirección según las responsabilidades de las insuficiencias halladas. Se formalizan las acciones a tomar según el marco que dicta la norma.	Se realiza un proceso de análisis de cada uno de los riesgos y se presenta una estrategia de protección la misma que entra a evaluación y aceptación.

Nota: Desarrollo de autoría propia

Una vez realizado el proceso comparativo entre las metodologías y basándose en el levantamiento de los riesgos del SGC, se decide realizar el análisis gestión de riesgos de seguridad de la información mediante la metodología MAGERIT.

La metodología seleccionada permite que se siga con el mismo estándar de trabajo que ya es conocido por parte de los procesos.

2.3. Validación de la propuesta

Levantamiento de activos.

Se procederá a realizar un levantamiento del inventario de los activos tecnológicos de la organización mediante el aplicativo «INGSIGTH», el mismo que está implementado en todos los equipos de la organización y permite saber el estado de seguridad de antivirus y de funcionalidad de cada uno de estos equipos. ANEXO-1

En el levantamiento de activos documentales, en la actualidad el SGC determina un procedimiento según la directriz de cada uno de los procesos, los cuales se encuentran en un repositorio seguro en una aplicación llamada «KAWAK». ANEXO-2

Análisis de riesgos

Para el análisis de riesgos se determina que se realizara un anal FODA con el cual se determinara las Fortalezas, Oportunidades, Debilidades y Amenazas de los activos importante y de los sistemas de información de la organización, es un método de análisis que nos permite conocer el estado en el que se encuentra el proceso de seguridad, este debe ser levantado en conjunto con los encargados de cada uno de los procesos que interactúan con la información que se desea asegurar tal como se puede evidenciar en la Tabla 2.

Tabla 2
Matriz FODA

MATRIZ FODA	
FORTALEZAS	**DEBILIDADES**
● Control y administración de la infraestructura tecnológica ● Monitorios y alertas con proveedores externos ● Alta disponibilidad de Servicios logísticos. ● Retail con respaldos de contingencia. ● Implementaciones e integración entre sistemas ● Contrato con proveedores certificados en servicios que cuenta la compañía ● Buen nivel organizacional ● Marca posicionada y certificada en el mercado ● Mercadeo y fidelidad de los clientes ● Se cuenta con licencia para respaldos de información crítica de la empresa en la nube	● Tiempo de solución tardío en el CAT de Ecuador ● Afectación en los sistemas Core del negocio (Servicli, Serviretail, Servicore) ● Afectación imprevista de herramientas tecnológicas (Hardware)
OPORTUNIDADES	**AMENAZAS**
● Soluciones tecnológicas en la Nube para garantizar alta disponibilidad sobre los sistemas y optimización de recursos. ● Líderes de proceso predispuestos para implementar nuevas soluciones ● Confianza de la alta dirección de nuevas implementaciones tecnológicas ● Oportunidades de negocio con alianzas estratégicas ● Planes de capacitación desarrollados por Calidad y vida ● Mantenernos a la vanguardia en servicios logísticos integrales	● Ataques de seguridad en servicios publicados ● Vulnerabilidad de los sistemas de información ● Caída de enlaces de comunicaciones ● Fuga de información sensible de la empresa ● Restricciones de movilidad por catástrofes ● Sistema del Core del negocio centralizado

Nota: Elaboración propia

Una vez que se realiza el levantamiento de esta información es necesario saber hacia dónde aplican los riesgos encontrados según la debilidad y la amenaza relacionadas entre sí como se evidencia en la Tabla 3, ANEXO-4

Tabla 3
Análisis FODA

APLICADO	RIESGO (CONSIDERAR LAS DEBILIDADES Y AMENAZAS)
Cliente interno y externo	Equipos de cómputo sin antivirus o con antivirus desactualizado
Cliente interno	Vulnerabilidad de los sistemas de información
Cliente interno	Afectación imprevista de herramientas tecnológicas (Hardware)
Cliente interno y externo	Caída de enlaces de comunicaciones
Cliente interno y externo	Afectación en los sistemas Core del negocio (Servicli, Serviretail, Servicore)

Nota: Elaboración propia

Matriz de riesgos

Una vez levantado el análisis FODA se procede a crear una matriz de riesgos mediante la cual se registran los riesgos encontrados, la causa de cada uno de los riesgos, la probabilidad, la consecuencia, la valoración inicial, la coloración actual, hacia donde está dirigida la acción de cada riesgo y finalmente las acciones a tomar por cada uno de los riesgos encontrados.

Probabilidad.

El siguiente paso es evaluar cada uno de los riesgos según su probabilidad, sabiendo que existe un concepto de la ocurrencia que se puede dividir en

- **Muy Alto:** ocurre varias veces en un mismo mes.
- **Alto:** Ocurre 6 o más veces al año.
- **Bajo**: No se ha presentado hasta el momento, pero puede ocurrir 1 vez al año.

Cada uno de estos conceptos tendrá una calificación:

- **Muy Alto:** 4.
- **Alto:** 3.
- **Bajo**: 1.

Consecuencia.

La consecuencia se evalúa según el impacto que puede tener un riesgo en la organización teniendo en cuenta si la afectación puede causar pérdidas económicas, también tiene ciertos criterios de evaluación que están definidos de la siguiente manera:

- **Muy Alto:** Impacto que puede generar pérdidas financieras y afecta a toda la organización y/o incumplimiento de regulaciones.
- **Alto:** Afectación significativa a uno o más procesos de la organización con afectación financiera.
- **Medio:** Afectación significativa a uno o más procesos de la organización sin afectación financiera.
- **Bajo:** Afectación insignificante al proceso.

Cada una de estas consecuencias detalladas también deben tener su calificación con la finalidad de poder realizar una valoración de los riesgos.

- **Muy Alto:** 4.
- **Alto:** 3.
- **Medio**: 2.
- **Bajo:** 1.

Riesgo Aceptable.

Un riesgo no se puede eliminar por completo porque por algún motivo puede suceder y si se lo trata de eliminar el costo puede ser muy elevado, por este motivo existen los riesgos aceptables que su ocurrencia se puede reducir y minimizar su consecuencia con la finalidad que la organización no tenga un perjuicio grave.

Riesgo Residual.

Un riesgo puede permanecer y subsistir después de haber implementado todos los controles necesarios, puede existir la posibilidad de ocurrencia pese a todas las medidas tomadas, evaluadas y corregidas.

La matriz de riesgos es clave en el proceso de gestión de riesgos y es importante que se diligencie de manera correcta según el análisis previo y teniendo en cuenta cada uno de los campos que conlleva esta matriz, como se puede evidenciar en la Tabla 4.

Tabla 4
Formato de matriz de riesgos

MATRIZ DE RIESGOS													
Macro proceso	Proceso	Riesgo	Causa del riesgo	Probabilidad		Consecuencia		Riesgo inherente		Riesgo residual		La acción está dirigida a:	Acciones	Control
				Concepto de ocurrencia	Calificación	Concepto de afectación	Calificación	Fecha	Factor de riesgo	Fecha	Factor de riesgo			

Nota: Elaboración propia

Tabla 5

Descripción de los campos de la matriz

Nombre del campo de la matriz		Descripción
	Macroproceso	Detalla el macroproceso donde se identificó el riesgo
	Proceso	Detalla el proceso existente dentro del macroproceso donde se identificó el riesgo
	Riesgo	Nombre del riesgo
Probabilidad	Concepto de ocurrencia	Muestra el concepto de probabilidad de ocurrencia que ha tenido el riesgo
	Calificación	Se detalla la escala de calificación según la evaluación de la probabilidad del 1 al 4
Consecuencia [si un riesgo ocurre]	Concepto de afectación	Muestra los conceptos determinados de consecuencia que tiene el riesgo en el caso que ocurra (1 al 4)
	Calificación	Se detalla la escala de calificación según la evaluación de la probabilidad del 1 al 4
Riesgo residual	Fecha	Muestra la fecha en la que se detectó el riesgo
	Factor riesgo	El factor del riesgo que tiene en la valoración actual (resultado después de evaluar la eficacia de las acciones) de la probabilidad y consecuencia que se muestra en la matriz.
Riesgo inherente	Fecha	Muestra la fecha en la que se detectó el riesgo
	Factor de riesgo	El factor del riesgo que se obtuvo en la valoración inicial (cuando se identifica el riesgo) de la probabilidad y consecuencia que en su momento de levantó en la matriz.
	La acción está dirigida a	Muestra el concepto del enfoque a la cual están dirigidas las acciones que tiene ya implementada el proceso de forma preventiva.
	Acciones	Muestra las acciones que ya tiene implementada el proceso de forma preventiva en relación al riesgo.
	Control	Muestra la herramienta que posee el proceso para monitorear el comportamiento del riesgo.

Nota: Elaboración propia

Matriz de articulación de la propuesta

Tabla 6

Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Inventario de parque tecnológico	Identificación de activos	Método descriptivo	Informe de equipos activos de la organización	ANEXO 1	Insight
Inventario de activo documental	Identificación de documentos importantes para la organización	Método descriptivo	Detalle de documentos importante y su manejo por cada proceso	ANEXO 2	KAWAK
Antivirus instalado	Confirmación de antivirus instalado en los activos	Método descriptivo	Informe de equipos con antivirus instalado	ANEXO 3	Invgate
Matriz DOFA	Identificación de riesgos	Método analítico	Identificación de los riesgos mediante una matriz DOFA	TABLA 2	Análisis propio
Formato de matriz de riesgos	Formato para elaboración de una matriz de riesgos	Método analítico	Creación de un formato para el manejo de la matriz de riesgos	TABLA 4	Elaboración propia.

CONCLUSIONES

En el análisis de metodologías para la gestión de riesgos de seguridad de la información se pudo identificar que el método que se adapta de mejor manera a las necesidades de la organización en MAGERIT, ya que se vienen trabajando con otras normas ISO que permiten que la matriz de riesgos tenga un formato establecido y adecuado a las necesidades de cada uno de los procesos.

Los principales riesgos según su ponderación y que son parte del primer levantamiento de riesgos de seguridad son:

- Equipos de cómputo sin antivirus o con antivirus desactualizado.
- Vulnerabilidad de los sistemas de información
- Afectación imprevista de herramientas tecnológicas (Hardware).
- No contar con servidores de pruebas y produccion.

Aún hay que analizar muchos más riesgos que afecta a los procesos involucrados en el manejo del principal activo de la compañía.

La información está al alcance de todos dentro de la organización, pero aún se deben implementar políticas, objetivos, controles y seguimientos constante, con la única finalidad de que se pueda agregar una certificación más que permita que la gestión documental, la seguridad en el trabajo y la seguridad de la información trabajen bajo un mismo esquema normativo y que el control sea transversal para toda la organización.

Para concluir con el primer y más importante paso de la gestión de riesgos se presenta una primera matriz de riesgos de seguridad de la información orientada hacia el activo físico de la organización según se muestra en el ANEXO 5.

RECOMENDACIONES

Se recomienda que el seguimiento y análisis de los riesgos se lo realice de manera periódico y con la participación de cada uno de los líderes de los procesos involucrados en el manejo de la información, la matriz de riesgo es el primer paso y el más importante para aceptar que aún se está comenzando con un proceso que es necesario para el cliente interno y externo.

La matriz DOFA será la mejor aliada para la identificación de riesgos, el acompañamiento de un experto en el proceso de implementación de ISO 27000 e ISO 27001 es necesario para que estas normas se puedan enlazar con las normas ya implementadas.

Es necesario identificar los riesgos que se presenten en cada uno de los procesos de la compañía y realizar un análisis y evaluación de cada uno de ellos, para tomar las acciones necesarias.

Todo el personal de la compañía debe conocer el correcto manejo de la informacion, saber cuáles son sus obligaciones sobre la informacion y cuáles son los derechos que los clientes tienen sobre su informacion personal.

Se debe definir una política de seguridad de la informacion con el apoyo de la alta dirección y los líderes de proceso nacionales y regionales.

BIBLIOGRAFÍA

Alina Karla Quesada Somano, A. M. (2020). *MÉTODOS TEÓRICOS DE INVESTIGACIÓN.* Matanzas: Universidad de Matanzas.

Arellano, F. (2015). *Método Inductivo*. Obtenido de https://www.significados.com/metodo-inductivo/

Calidad. (2019). *Conocimiento EAC*. Obtenido de https://www.eac.es/web/guest/centro-conocimiento/seguridad-de-la-informacion

CEUPE. (s.f.). Política de seguridad de la información y SGSI. *Política de seguridad de la información y SGSI*, págs. https://www.ceupe.com/blog/ejemplo-politica-seguridad-informacion-y-sgsi.html.

ESCUELA EUROPEA DE EXCELENCIA. (5 de septiembre de 2019). *Cómo gestionar los controles de acceso según ISO 27001*. Obtenido de https://www.escuelaeuropeaexcelencia.com/2019/09/como-gestionar-los-controles-de-acceso-segun-iso-27001/

Excellence, I. (21 de mayo de 2015). *ISO 27001: ¿Qué significa la Seguridad de la Información?* Obtenido de https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

Excellence, I. (16 de marzo de 2015). *ISO 27001: El método MAGERIT*. Obtenido de https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/

Excellence, I. (28 de enero de 2015). *ISO 27001: La implementación de un Sistema de Gestión de Seguridad de la Información.* Obtenido de https://www.pmg-ssi.com/2015/01/iso-27001-la-implementacion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/

Excellence, I. (23 de febrero de 2017). *¿Cómo realizar un inventario de activos de información?* Obtenido de https://www.pmg-ssi.com/2017/02/realizar-inventario-activos-de-informacion/

Excellence, I. (1 de febrero de 2018). *Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad.* Obtenido de https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

Helena Alemán Novoa, C. R. (16 de mayo de 2014). *Metodologías Para el análisis de riesgos en los SGSI.* Obtenido de

https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1754

Hernández, R. F. (2014). Metodología de la investigación. En R. F. Hernández, *Metodología de la investigación.* McGrwall Hill.

ISO.27000.ES. (2005). *Información fundamental sobre el significado y sentido de implantación y mantenimiento de los Sistemas de Gestión de la Seguridad de la Información*. Obtenido de https://www.iso27000.es/sgsi.html

Leonardo Sena, S. M. (2004). Introducción a Riesgo Informático. 10.

México, P. I. (10 de julio de 2020). *La importancia de la Seguridad de la Información.* Obtenido de https://blog.posgrados.ibero.mx/seguridad-de-la-informacion/

Miguel Ángel Amutio Gómez, J. C. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Ministerio de Hacienda y Administraciones Públicas.

R, B. (2014). Implementación efectiva de un SGSI. En B. R, *ACADEMIA* (pág. 30).

RCG. (21 de junio de 2017). *Cómo aumentar el rendimiento de tu infraestructura informática*. Obtenido de https://rcg-comunicaciones.es/rendimiento-infraestructura-informatica/

Rodríguez, P. (7 de mayo de 2020). *Análisis de riesgos informáticos y ciberseguridad*. Obtenido de https://www.ambit-bst.com/blog/an%C3%A1lisis-de-riesgos-inform%C3%A1ticos-y-ciberseguridad

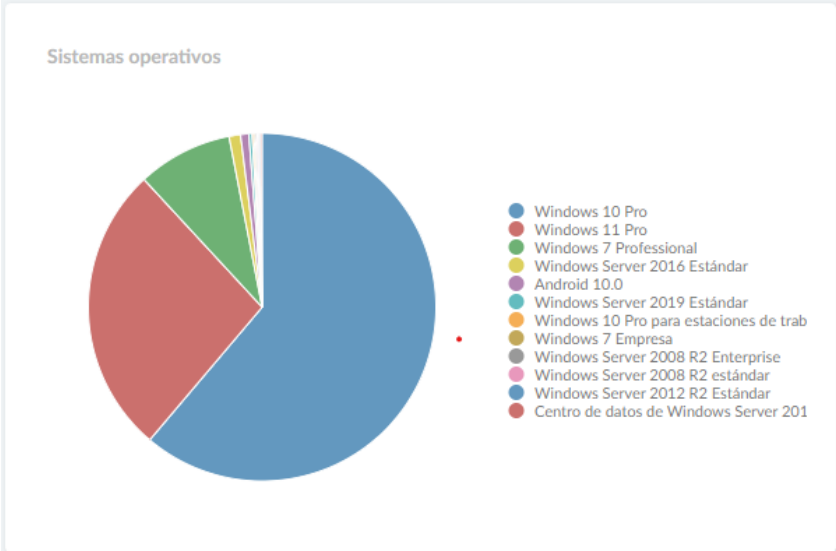
Servientrega. (12 de Agosto de 2016). *Disposiciones generales para la protección de datos personales*. Obtenido de https://www.servientrega.com

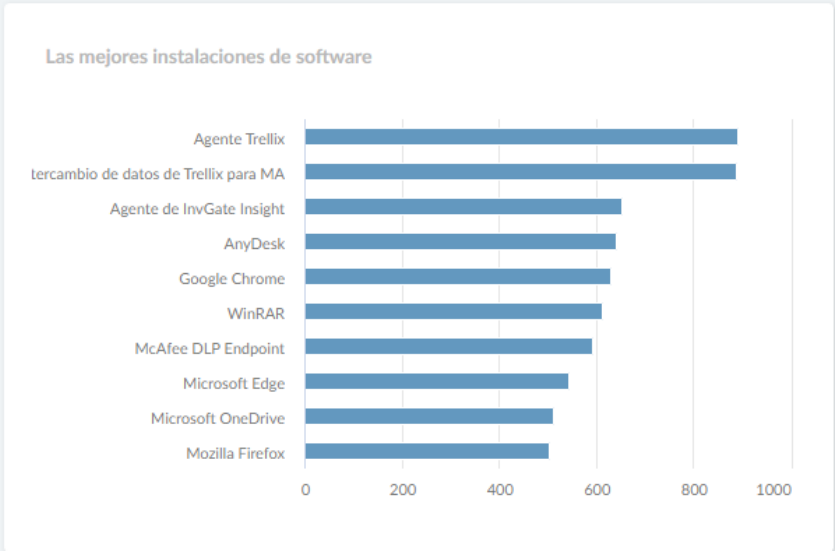
Unidas, N. (2023). Los Objetivos de Desarrollo Sostenible (ODS). págs. https://www.undp.org/es/sustainable-development-goals.

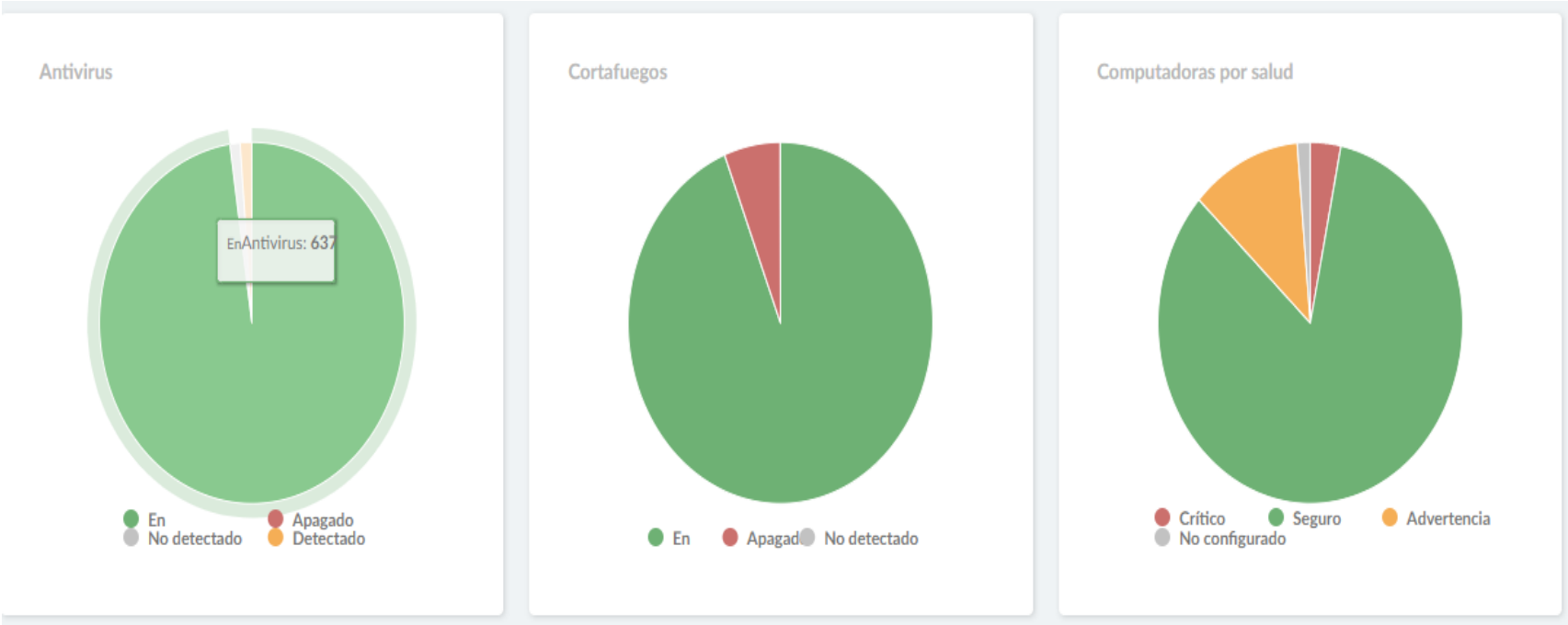
ANEXOS

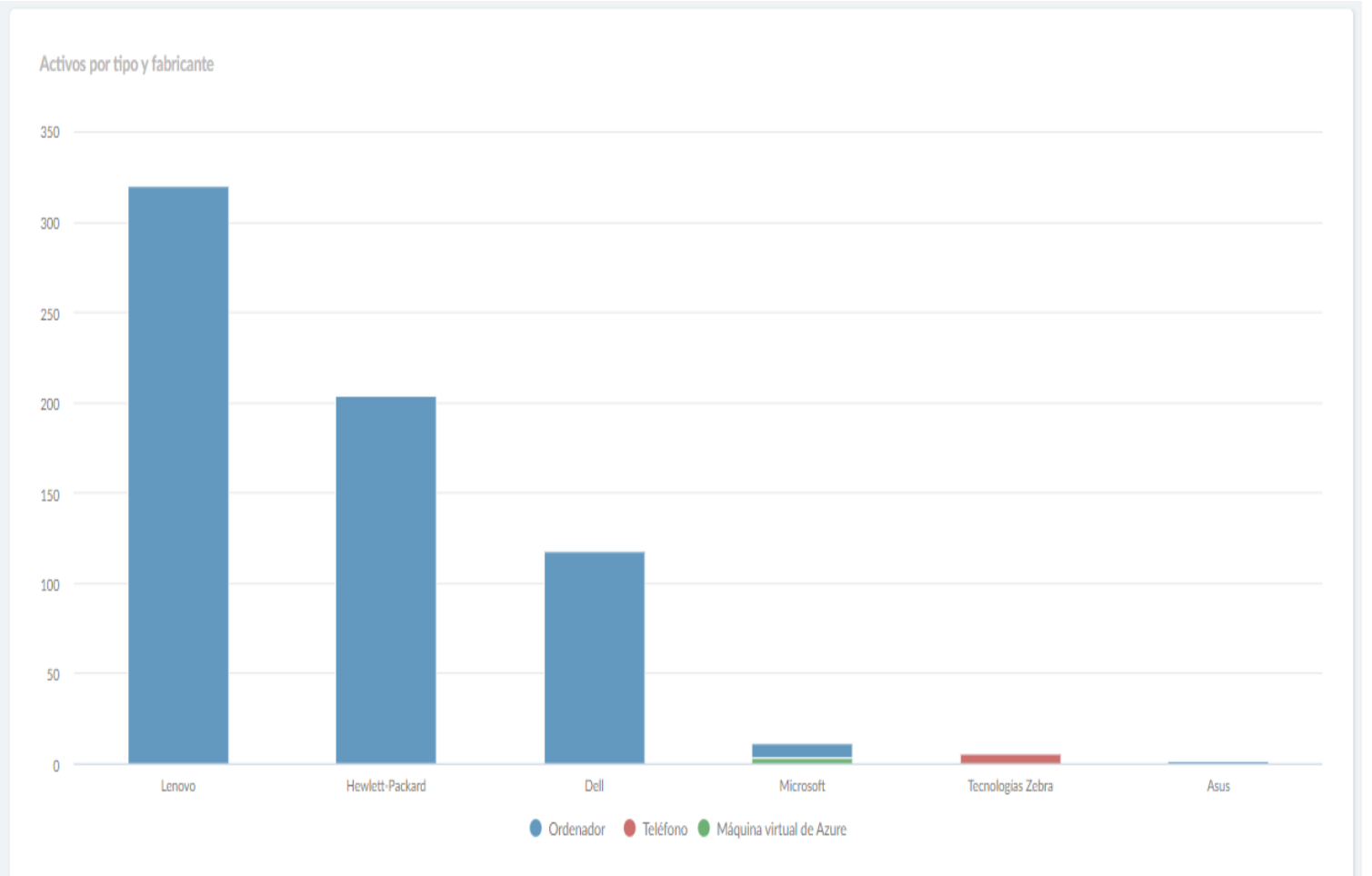
Anexo 1

Informe de IngSigth de inventario de parque tecnológico.



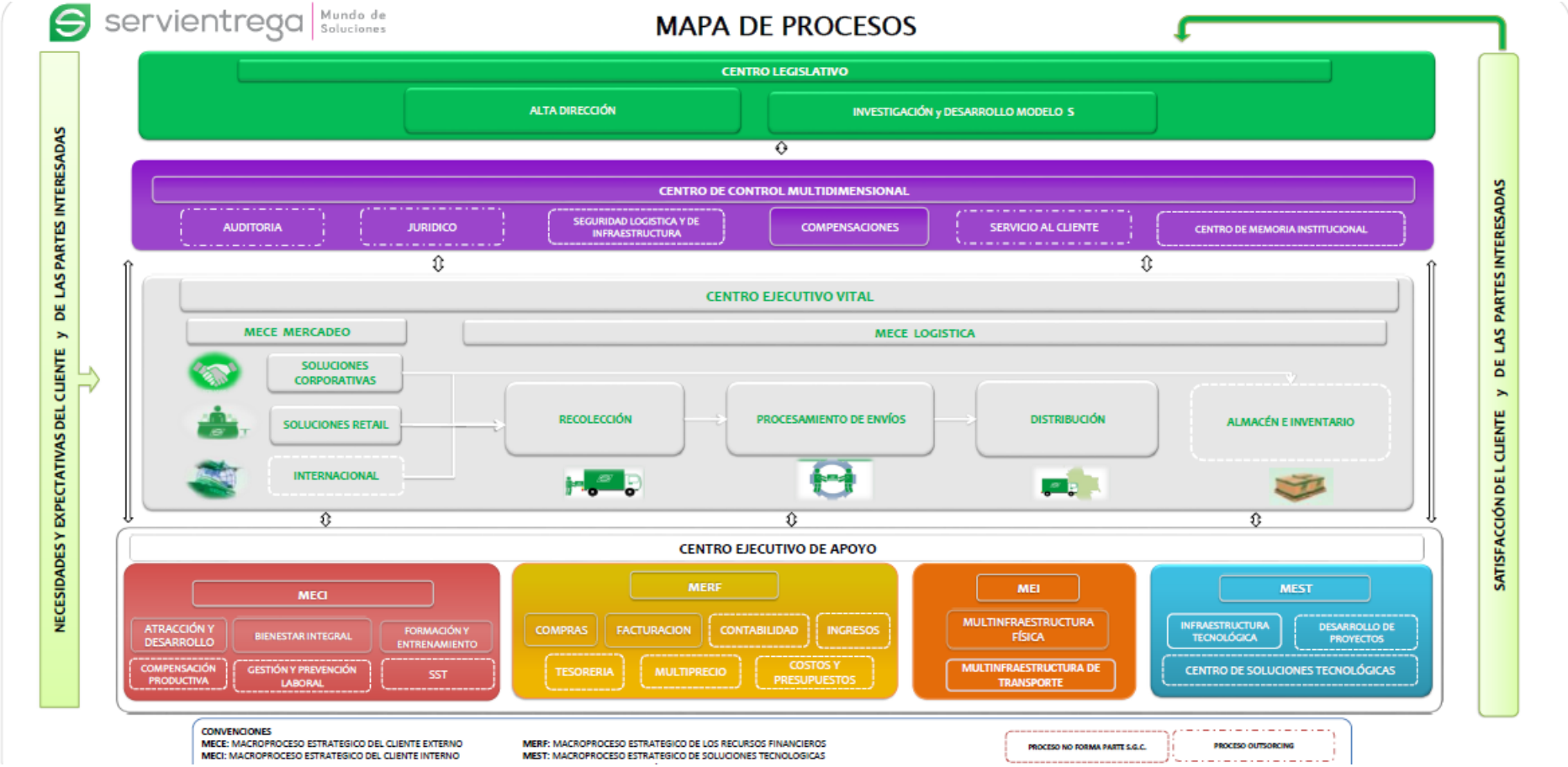



Antivirus
EnAntivirus: 637
En
Apagado
No detectado
Detectado
Cortafuegos
En
Apagad
No detectado
Computadoras por salud
Crítico
Seguro
Advertencia
No configurado


Activos por tipo y fabricante
350
300
250
200
150
100
50
0
Lenovo
Hewlett-Packard
Dell
Microsoft
Tecnologías Zebra
Asus
Ordenador
Teléfono
Máquina virtual de Azure

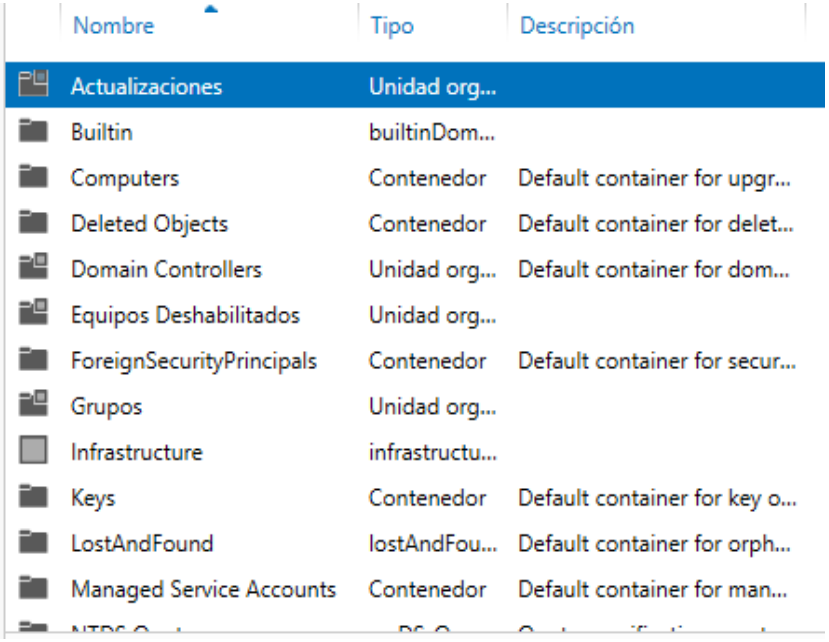
Anexo 2

Mapa de procesos

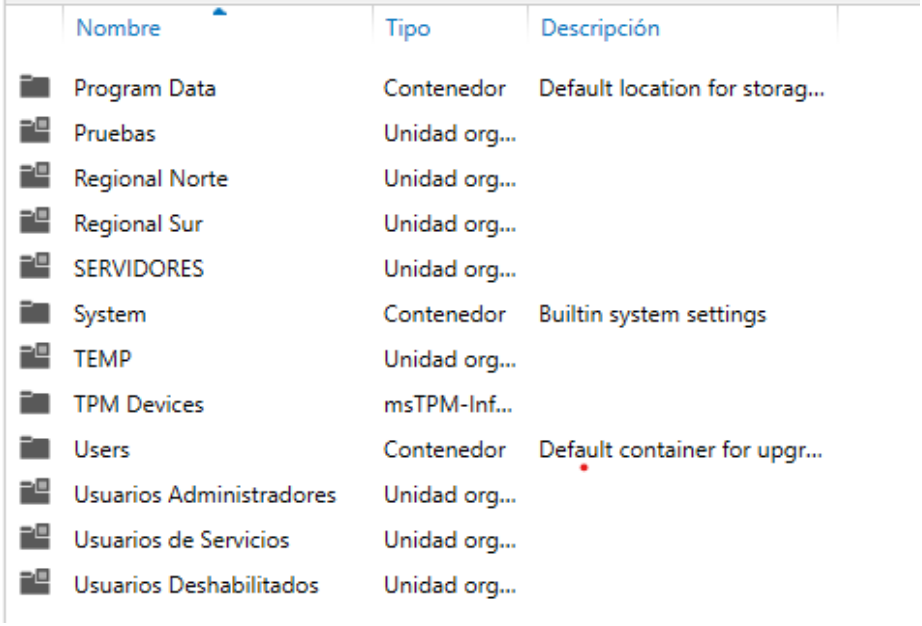


Anexo 3

Información del directorio activo



Nombre	Tipo	Descripción
Actualizaciones	Unidad org...	
Builtin	builtinDom...	
Computers	Contenedor	Default container for upgr...
Deleted Objects	Contenedor	Default container for delet...
Domain Controllers	Unidad org...	Default container for dom...
Equipos Deshabilitados	Unidad org...	
ForeignSecurityPrincipals	Contenedor	Default container for secur...
Grupos	Unidad org...	
Infrastructure	infrastructu...	
Keys	Contenedor	Default container for key o...
LostAndFound	lostAndFou...	Default container for orph...
Managed Service Accounts	Contenedor	Default container for man...



Nombre	Tipo	Descripción
Program Data	Contenedor	Default location for storag...
Pruebas	Unidad org...	
Regional Norte	Unidad org...	
Regional Sur	Unidad org...	
SERVIDORES	Unidad org...	
System	Contenedor	Builtin system settings
TEMP	Unidad org...	
TPM Devices	msTPM-Inf...	
Users	Contenedor	Default container for upgr...
Usuarios Administradores	Unidad org...	
Usuarios de Servicios	Unidad org...	
Usuarios Deshabilitados	Unidad org...	

Anexo 4

ESCALA DE CONSECUENCIAS		
Calificación	**Valor**	**Consecuencias**
Bajo	1	Afectación insignificante al proceso
Medio	2	Afectación significativa al proceso y/o a otros procesos de la organización (Sin afectación financiera)
Alto	3	Afectación significativa al proceso y/o a otros procesos de la organización (Con afectación financiera)
Muy alto	4	Impacto que puede generar pérdidas financieras y afecta a toda la organización y/o incumplimiento a regulaciones

ESCALA DE PROBABILIDADES		
Calificación	**Valor**	**Probabilidades**
Bajo	1	No se ha presentado hasta el momento, pero podría ocurrir y ocurre 1 vez al año
Medio	2	Ocurre hasta 5 veces al año
Alto	3	Ocurre 6 o más veces al año
Muy alto	4	Ocurre varias veces en un mismo mes

ESCALA DE EVALUACIÓN DE RIESGO	
De 1 a 2	**BAJO**
De 3 a 6	**MEDIO**
De 8 a 9	**ALTO**
De 12 a 16	**MUY ALTO**

MAPA DE CALOR				
Consecuencia/Probabilidad	1	2	3	4
1	1	2	3	4
2	2	4	6	8
3	3	6	9	12
4	4	8	12	16

Anexo 5

MATRIZ DE RIESGOS													
Macro proceso	Proceso	Riesgo	Causa del riesgo	Probabilidad		Consecuencia		Riesgo inherente		Riesgo residual		La acción está dirigida a:	Acciones
				Ocurrencia	Calificación	Concepto de afectación	Calificación	Fecha	Factor de riesgo	Fecha	Factor de riesgo		
MEST	Infraestructura tecnológica	Equipos de cómputo sin antivirus o con antivirus desactualizado	Afectación de equipos de cómputo por falta de antivirus instalado o actualizado en los CL principales y regionales.	Alto	3	Medio	2				6 [MEDIO]	Cambia la Probabilidad	Realizar un informe de los equipos con antivirus instalado o actualizado desde la herramienta insigth, confirmar con el inventario del parque tecnológico
MEST	Infraestructura tecnológica	Afectación imprevista de herramientas tecnológicas (Hardware)	Falta de mantenimientos de los equipos por no contar dentro del cronograma (inventario) No contar con equipos de backup Mala manipulación por parte del usuario Equipos obsoletos en tiempo y características tecnológicas	Muy alto	4	Alto	3				12 [MUY ALTO]	Cambia la Probabilidad	Realizar una mesa de trabajo con el proceso MEI, con la finalidad de asignar equipos de backup y seleccionar el proveedor de mantenimientos correctivos y preventivos de equipos de computo
MEST	Infraestructura tecnológica	No contar con servidores de pruebas y produccion	Falta de control en el proceso de actualización y desarrollo de nuevos aplicativos	Alto	4	Alto	3				12 [MUY ALTO]	Cambia la Probabilidad	Generar un requerimiento de actualización al Tenant de Azure con la finalidad de separar los ambientes de pruebas y produccion.

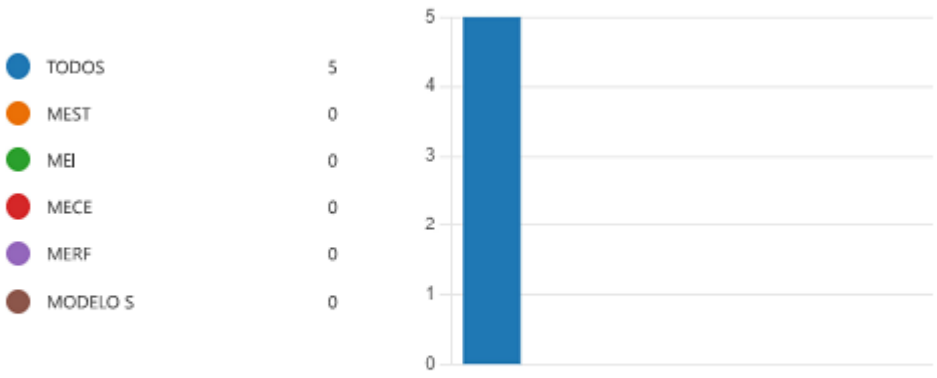
Anexo 6

Gestión de riesgos de la información en Servientrega Ecuador S.A:

5	03:09	Activo
Respuestas	Tiempo medio para finalizar	Estado

1. Cuál cree usted que es el principal riesgo de la información en Servientrega Ecuador S.A.

2. Cuáles son los procesos que se involucran en la seguridad de la información



3. La seguridad de la información está enfocada solo a la información digital

VERDADERO	2
FALSO	3

4. Nuestros proveedor de desarrollo, cloud e internet son RESPOSABLES de nuestra información

VERDADERO	1
FALSO	4

5. Servientrega Ecuador S.A. es la ENCARGADA de precautelar información

SI	1
NO	4