TESIS_PENAFIEL CON ANEXOS INCOMPLETOSPONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERÍA
ESCUELA DE SISTEMAS



DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS Y COMPUTACIÓN

Diseño de un modelo para establecer un sistema de gestión de la seguridad de la información dentro de un ambiente Cloud Computing, aplicando la Norma ISO 27001:2013.

Autor:

Cristhian Arecio Peñafiel Loayza

Director:

Msc. Oswaldo Espinosa

QUITO, 2019

DEDICATORIA

Dedico este trabajo de titulación a toda mi familia, ya que sin su apoyo incondicional no hubiera llegado a cumplir esta meta tan importante, en especial a mis padres ya que su esfuerzo y dedicación fue un pilar fundamental en esta etapa. A mis familiares cercanos y amigos que me han apoyado en momentos de necesidad y me han sabido motivar. A Alex y Karina ya que su cariño ha sido de vital importancia durante gran parte de la carrera.

Cristhian Peñafiel

AGRADECIMIENTO

Deseo agradecer a todos los que me han acompañado en este camino, a mi papá y a mi mamá por el eterno e ilimitado apoyo emocional y económico que me han sabido dar a lo largo de esta aventura. A mi familia que directa o indirectamente me han sabido motivar.

Un profundo agradecimiento a la Pontificia Universidad Católica del Ecuador y a los docentes que la conforman por los conocimientos, aprendizajes, oportunidades y buenos momentos vividos que sin duda serán de gran ayuda en mi vida profesional.

Cristhian Peñafiel

TABLA DE CONTENIDO

ÍNDICE DE TABLAS 9

ÍNDICE DE ILUSTRACIONES 10

RESUMEN 11

ABSTRACT 12

1. CAPÍTULO I: INTRODUCCIÓN 13

1.1. GENERALIDADES 13

1.2. JUSTIFICACIÓN 14

1.3. OBJETIVOS 15

1.3.1. OBJETIVO PRINCIPAL 15

1.3.2. OBJETIVOS ESPECÍFICOS 15

1.4. MARCO TEÓRICO 16

1.4.1. Conceptos de seguridad de la información 16

1.4.1.1. Sistema de Gestión de Seguridad de Información. 19

1.5. Historia norma ISO 27001:2013 20

1.6. Descripción general de la norma 21

1.7. Introducción a Cloud Computing 21

1.8. Modelos de Servicios 22

1.8.1. Infraestructura como un servicio (IaaS) 23

1.8.2. Plataforma como un servicio (PaaS) 25

1.8.3. Software como un servicio (SaaS) 26

1.9. Modelos de implementación Cloud Computing 27

1.9.1. Nube Pública 27

1.9.2. Nube Privada 29

1.9.3. Nube Hibrida 30
1.9.4. Otros tipos 31
1.10. Seguridad 31
1.10.1. Problemas y riesgos 31
1.10.2. Medidas de control de seguridad 33
1.10.3. Seguridad y Privacidad 34
1.11. Ciclo de vida de la Información 34
1.12. Ventajas y desventajas de un ambiente Cloud Computing 35
2. CAPÍTULO II: DISEÑO DEL MODELO DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN 37
2.1. Norma ISO 27001:2013 37
2.2. Fases de la norma ISO 27001:2013 38
2.3. Descripción de las fases de la Norma 27001:2013 39
2.3.1. Alcance 39
2.3.2. Referencias Normativas 40
2.3.3. Términos y definiciones 40
2.3.4. Contexto de la organización 40
2.3.5. Liderazgo 40
2.3.6. Planificación 40
2.3.7. Apoyo 41
2.3.8. Funcionamiento 41
2.3.9. Evaluación de desempeño 41
2.3.10. Mejora 41
2.4. Documentos y Registros 42

2.4.1. Documentos Obligatorios 42
2.4.2. Documentos no obligatorios 43
2.4.3. Requisitos 43
2.5. Adaptación de la norma ISO 27001:2013 a un ambiente Cloud Computing 44
2.6. Documentación para un ambiente Cloud Computing 47
3. CAPÍTULO III: ACTIVOS – RIESGOS – VULNERABILIDADES Y AMENEZAS EN UN AMBIENTE CLOUD COMPUTING 48
3.1. Activos 48
3.1.1. Identificación de Activos 48
3.1.2. Clasificación de Activos 49
3.1.3. Tasación de activos 50
3.2. Riesgos en un Ambiente Cloud Computing 51
3.2.1. Identificación de Riesgos 51
3.2.2. Evaluación del Riesgo 52
3.2.3. Agrupación de Riesgos 53
3.2.4. Tratamiento de riesgos 54
3.3. Amenazas 57
3.3.1. Identificación de amenazas 57
3.4. Vulnerabilidades 59
3.4.1. Identificación de Vulnerabilidades 59
4. CAPÍTULO IV: APLICACIÓN DEL MODELO DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN EN UN AMBIENTE CLOUD COMPUTING 62
4.1. Alcance 63
4.2. Referencias Normativas 63

4.3. Contexto de la Organización 64
4.3.1. Comprender la organización y su contexto 64
4.3.2. Comprender las necesidades y expectativas de las partes interesadas 64
4.3.3. Determinar el alcance del sistema de gestión de seguridad de la información. 64
4.3.4. Sistema de Gestión de Seguridad de la Información 65
4.4. Liderazgo 65
4.4.1. Liderazgo y compromiso 65
4.4.2. Política 66
4.4.3. Roles organizacionales 66
4.5. Planificación 67
4.5.1. Acciones para abordar riesgos y oportunidades 67
4.5.2. Objetivos de seguridad de la información y planes para alcanzarlos 71
4.6. Apoyo 71
4.6.1. Recursos 71
4.6.2. Competencia 72
4.6.3. Conciencia 72
4.6.4. Comunicación 72
4.7. Funcionamiento 72
4.7.1. Planificación y control operacional 72
4.7.2. Evaluación de riesgos de seguridad de la información 73
4.7.3. Tratamiento de riesgos de seguridad de la Información 74
5. CAPÍTULO IV: CONCLUSIONES Y RECOMENDACIONES 76
5.1. Conclusiones 76

5.2. Recomendaciones 77

BIBLIOGRAFIA 78

ANEXOS 81

ANEXOS 1: CATALOGO DE AMENAZAS EN UN AMBIENTE CLOUD COMPUTING 81

ANEXO 2. REGISTROS DESARROLLADOS 90

ANEXO 3: DOCUMENTOS APLICABLES EN UN AMBIENTE CLOUD COMPUTING 93

ANEXO 4: PROCESOS QUE SE REALIZAN EN LA EMPRESA TECNOLÓGICA 97

ÍNDICE DE TABLAS

Tabla 1: Adaptación de norma ISO 27001 a Cloud Computing (Peñafiel, 2019) 46

Tabla 2: Identificación de activos en Cloud Computing (Peñafiel, 2019) 49

Tabla 3: Matriz para la tasación de activos en Cloud Computing (Peñafiel, 2019) 50

Tabla 4: Levantamiento de Amenazas y Vulnerabilidades en Cloud Computing (Peñafiel, 2019) 61

Tabla 5: Mapa de procesos empresa Tecnológica (Peñafiel, 2019) 62

Tabla 6: Definición de roles (Peñafiel, 2019) 67

Tabla 7: Identificación de activos en la empresa tecnológica (Peñafiel, 2019) 67

Tabla 8: tasación de activos en la empresa tecnológica (Peñafiel, 2019) 68

Tabla 9: formato para la evaluación de riesgos (Peñafiel, 2019) 68

Tabla 10: Formato para el tratamiento de riesgos (Peñafiel, 2019) 70

Tabla 11: Evaluación de riesgos (Peñafiel, 2019) 73

Tabla 12: Tratamiento de riesgos (Peñafiel, 2019) 74

Tabla 13: Evaluación de amenazas (Peñafiel, 2019) 75

ÍNDICE DE ILUSTRACIONES

Ilustración 1: Consecuencias de las amenazas a la información (Peñafiel, 2019) 19

Ilustración 2: Historia de ISO 27001 e ISO 17799 (ISO 27000.ES, 2006). 20

Ilustración 3: Modelo de servicios (WordPress.com, 2019) 23

Ilustración 4: Fases elegidas en un modelo Cloud Computing (Peñafiel, 2019) 46

RESUMEN

El avance tecnológico se presenta día a día sea en hardware como en software, así también en la infraestructura que facilita a las organizaciones ofrecer sus servicios y productos; actualmente la mayoría de organizaciones ha decido migrar su información a un ambiente Cloud Computing por las ventajas que este ofrece, principalmente porque retira de las organizaciones una gran responsabilidad como es la actualización de software y muchas ocasiones de hardware para estar a la par con la tecnología.

El presente documento describe los requisitos que se requieren en el Diseño de un Modelo para establecer un Sistema de Gestión de la Seguridad de la Información dentro de un Ambiente Cloud Computing, con la aplicación de la Norma ISO 27001:2013, siendo necesario describir y conocer al ambiente Cloud Computing, las ventajas y desventajas que presenta.

La norma ISO27001se puede aplicar a cualquier tipo de empresa sin discriminar su naturaleza o tipo, por lo que se realiza un análisis que permita enfocar la norma al ambiente Cloud Computing, previamente conociendo los riesgos, amenazas y vulnerabilidades que se presentan en dicho ambiente.

ABSTRACT

Just as the infrastructure facilitates the organizations to offer their services and products, technological advances in hardware and software progress day by day; Currently, most companies have decided to migrate their information to a Cloud Computing environment because of the advantages it offers, mainly because it removes a great responsibility from companies such as software updates and many hardware occasions to keep up with technology.

In this document, describe the requirements for the Design of a Model to establish an Information Security Management System within a Cloud Computing Environment, with the application of ISO 27001: 2013 standard, for this it is necessary to describe and get to know the Cloud Computing environment along with the advantages and disadvantages that it presents.

The ISO 27001 standard can apply any type of company without discriminating its nature or type, so an analysis is carried out that allows the standard to be focused on the Cloud Computing environment, knowing the risks, threats and vulnerabilities that arise in this environment.

1. CAPÍTULO I: INTRODUCCIÓN

1.1. GENERALIDADES

Cloud Computing, también conocido como computación en la nube es un paradigma y modelo de negocio, de servicios, que ha permitido en la actualidad brindar a los empleados en el contorno tecnológico de la información, ingeniería y en el mundo computacional una gran acogía porque ha impactado en su uso y los beneficios que conlleva, lo interesante es el alcance en que a simple vista "Cloud Computing" puede ofrecer.

Definiendo a "Cloud Computing" principalmente como un modelo de negocio basado en internet, en el que se comparten recursos de hardware, además de tres aspectos fundamentales de servicios: Infraestructura como un servicio (IAAS), que se refiere a que "los usuarios arriendan los recursos que van a ocupar para sus procesos, por cuanto y cuando sean necesarios". El segundo servicio es la Plataforma como un servicio (PAAS), que se orienta a los desarrolladores a crear aplicaciones y servicios que funcionen a través del internet, este servicio provee el entorno de programación que facilita a los desarrolladores su ejecución. El tercer servicio es Software como un servicio que se refiere a brindar aplicaciones a los consumidores finales, con el fin que puedan acceder a ellas ya que están alojadas en la nube, siendo operadas directamente por el proveedor del servicio y pueden ser utilizarse en una amplia variedad de tareas.

Seguridad, el aspecto de seguridad en el entorno de la nube está relacionado a las características de la información que contiene: Confidencialidad, Integridad y Disponibilidad, pero aun así recientes casos dentro de los servicios que ofrecen en la nube han sufrido violaciones es decir han sido vulnerables y la información de sus clientes ha sido expuesta.

El modelo "Cloud Computing" nos introduce nuevos enfoques en la protección de datos. Se necesita tomar en cuenta todos los riesgos y de esa manera proceder a desarrollar formas más complicadas, innovadores y robustas para la protección de la

información. Por estas circunstancias no solo los proveedores de servicios en la nube deben incurrir a nuevas formas de protección de información y recursos, sino que también las organizaciones que vean la alternativa de migrar e implementar el servicio de “Cloud Computing”, pero tomando como prioridad la seguridad de sus datos.

La norma ISO 27001 es un Estándar Internacional elaborado para proporcionar un modelo definido para Establecer, Implementar, Operar, Monitorear, Revisar, Mantener, Mejorar un SGSI.

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información.

1.2. JUSTIFICACIÓN

Siempre ha sido una preocupación la seguridad para la transición a la nube por ello se han implementado sistema de gestión de la seguridad de la información de esa manera brindar un apoyo a la seguridad de los datos.

Se propone un modelo de seguridad de la información que pueda otorgar mayor protección contra las vulnerabilidades que se pueden presentar en un ambiente de Cloud Computing y los riesgos.

Para abordar estos temas, se plantea un análisis y evaluación global y la aplicación de la norma ISO 27001:2013 relacionada con Seguridad de la Información.

1.3. OBJETIVOS

1.3.1. OBJETIVO PRINCIPAL

Diseñar un modelo de los procedimientos de Seguridad de Información, en miras de implementar un Sistema de Gestión de Seguridad de la Información de la Norma ISO 270001:2013 dentro de un ambiente "Cloud Computing". Observando los riesgos presentes en seguridad de la información a fin de demostrar que la adopción de una SGSI es una decisión estratégica que mejorará los procesos.

1.3.2. OBJETIVOS ESPECÍFICOS

- Evaluar la situación actual concerniente a la Seguridad de la Información para fijar los niveles de vulnerabilidad que presenta este tema.
- Analizar los procesos estratégicos para entender los requerimientos de seguridad mínimos para un funcionamiento óptimo dentro de un ambiente de la nube.
- Identificar parámetros o medidas que intervengan en el proceso de evaluación de seguridad de "Cloud Computing".
- Definir los procesos y dominios para determinar los criterios a evaluar en términos de disponibilidad de la información de acuerdo a la Norma ISO 270001:2013.
- Desarrollar una propuesta de un sistema de gestión de la seguridad de la información dentro de un ambiente Cloud Computing.

- Realizar un esquema de enfoque de los riesgos para las vulnerabilidades identificadas.

1.4. MARCO TEÓRICO

1.4.1. Conceptos de seguridad de la información

En la actualidad, la información es el factor más importante de cualquier empresa, se observa que, los gobiernos, entidades financieras, entre otras empresas públicas y privadas realizan inmensurables esfuerzos para la automatización de sus procesos, con el único fin de obtener una eficiencia y productividad mayor, esto lleva a tener una demanda y generar una gran cantidad de información, que puede ser confidencial, conteniendo información administrativa interna como datos de sus clientes, productos, situación financiera, rastreo de paquetes, etc (García & Alegre, 2011).

En general todas las entidades mantienen una gran cantidad de información, como por ejemplos en medio impresos, en un repositorio en la nube, disco de respaldo, debido a que dependiendo de la empresa debe realizar investigaciones y sustentarlas.

También se toma en cuenta como un conjunto de documentos de orden administrativo, siendo comúnmente las direcciones de Recursos Humanos, Administrativo y Financiero las que archivan una mayor cantidad de documentos en sus distintas zonas destinadas para su propósito.

La información se establece como el activo de mayor valor dentro de una empresa, y está en proporción al uso que se le pueda dar, sea esta por el responsable de la información, generalmente son los procesos relacionados con las Direcciones

Administrativas, así como el acceso o uso de la información. Uno de los inconvenientes más frecuentes al establecer políticas de seguridad inadecuadas es la apropiación de la

información clave del usuario para comercializarla dentro del país o fuera de el con fines ilícitos.

Es indispensable asegurar la información y protegerla contra las amenazas y eventos que pueden suceder o comprometerla. La información puede existir en sus diferentes medios de almacenamiento, pero independientemente de ello, es necesario que las entidades garanticen la protección de la información durante su recolección, tratamiento y uso.

La seguridad de la información como objetivo primordial tiene, salvaguardar la confidencialidad, integridad y disponibilidad de la información; mediante la incorporación de un conjunto oportuno de procesos, normas y herramientas para la gestión eficaz de acceso a la información en sus diferentes niveles, y la implementación de mecanismos y medidas de seguridad tanto lógicas como físicas, para la detección y prevención de amenazas sean internas o externas, que puedan atentar contra la seguridad de la organización o rentabilidad del negocio (Ramos & Ribagorda, 2004).

En una organización la seguridad de la información, es un proceso de mejora continua demandante de la participación activa de toda la organización.

Existen diversas áreas relacionadas con los sistemas de información en la cual la seguridad informática los abarca. Las áreas van desde la protección física correspondientes al hardware, de su ambiente, hasta la protección de la información en la nube.

Las cualidades de la seguridad de la información son:

Critica: Es imprescindible para el manejo de la empresa.

Valiosa: Es un activo único de la empresa.

Sensible: Deber ser conocida por las personas autorizadas.

Se debe tomar en cuenta dos palabras indispensables que son riesgo y seguridad:

Riesgo: Son vulnerabilidades, amenazas o impacto negativo de las operaciones del negocio.

Seguridad: Es protegerse contra los riesgos, según (Tendencias & Innovación, 2019) la integridad de los datos libres de sufrir modificaciones no autorizadas es uno de los factores primordiales de la seguridad de la información, conllevando a ser precisa, pertinente y confiable.

Es de vital importancia conservar la confidencialidad esto quiere decir, evitar que la información circule a personas o sistemas no acreditados. Por ejemplo, las transacciones realizadas con tarjetas de crédito, en las cuales se pretende que el sistema valide por medio del cifrado numérico los datos que tiene la banda magnética durante su transmisión hasta comprobar la legitimación del proceso, ya que si no existe una autorización de las partes se considerará como violación de la confidencialidad. Pero algo más sencillo es cuando alguien mira por encima de su hombro, mientras usted coloca su información confidencial, cuando se publica información privada o en el robo de información de un dispositivo electrónico; constituyendo los casos mencionados anteriormente como sustracción a la confidencialidad de la información.

Finalmente se debe hacer referencia a la disponibilidad de la información la misma que consiste en que las personas, aplicaciones o procesos puedan acceder de manera segura.

La disponibilidad en los sistemas cumple el objetivo de estar disponible en todo momento, evitando interrupciones del servicio, fallos o actualizaciones del sistema por tal razón deben estar protegidos y funcionando correctamente en todo momento (INCIBE Instituto Nacional de Cyberseguridad, 2019).

Algo que se debe recalcar en el proceso de seguridad de información es la variedad en el sentido de que existen un sin número de mecanismos o niveles de servicio que se requiera para protegerlos, tales como una infraestructura tecnológica,

servidores de correo, bases de datos, servidores espejo, redes de almacenamiento, etc. Estas posibilidades dependerán del nivel de servicio que se quiere suministrar.

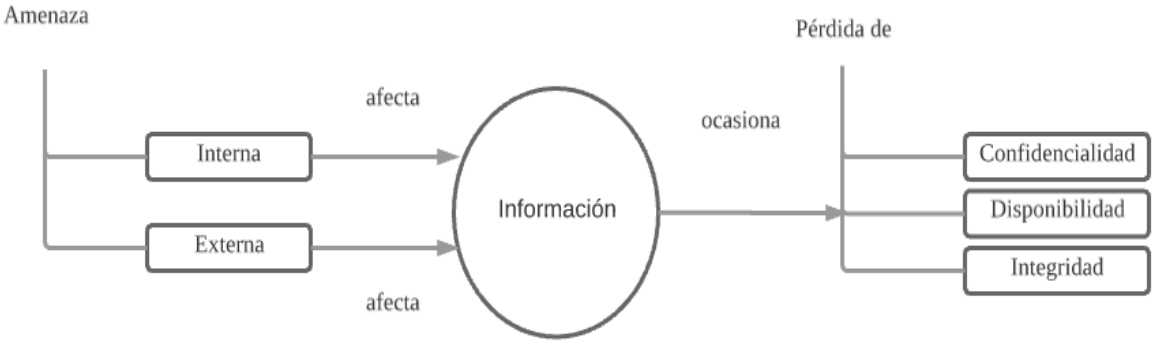


Ilustración 1: Consecuencias de las amenazas a la información (Peñafiel, 2019)

Cualquier debilidad en alguna de estas tres dimensiones supondrá una amenaza para la organización. Una garantía del buen uso y protección de la información reducirá los riesgos, permitirá cumplir con la legislación y los reglamentos vigentes y causará también impacto positivo en la imagen corporativa de la organización.

1.4.1.1. Sistema de Gestión de Seguridad de Información.

El (SGSI) es la abreviatura utilizada para referirse al Sistema de Gestión de Seguridad de la Información; ISMS son las siglas en inglés lo cual significa Information Security Management System; ayuda a instituir directrices, políticas, procedimientos, recursos y actividades, necesarias para la organización; así como para proteger la información sobre sus activos (García & Albarran, 2015).

Las ((ISO/IEC 27000: 2014 - 3.2.1, 2014) consideran al SGSI como un enfoque consecuente para instaurar, implementar, manejar, monitorear, inspeccionar, conservar y mejorar la seguridad de información de las organizaciones, permitiéndoles cumplir los objetivos propuestos del negocio, para lo cual se realiza la evaluación del riesgo, los niveles de aceptación del mismo dentro de las empresas, la manera de gestionarlos

de forma segura. Para la implementación eficiente de un SGSI es necesario que se proteja los activos que contienen información aplicando controles óptimos que garanticen su protección.

1.5. Historia norma ISO 27001:2013

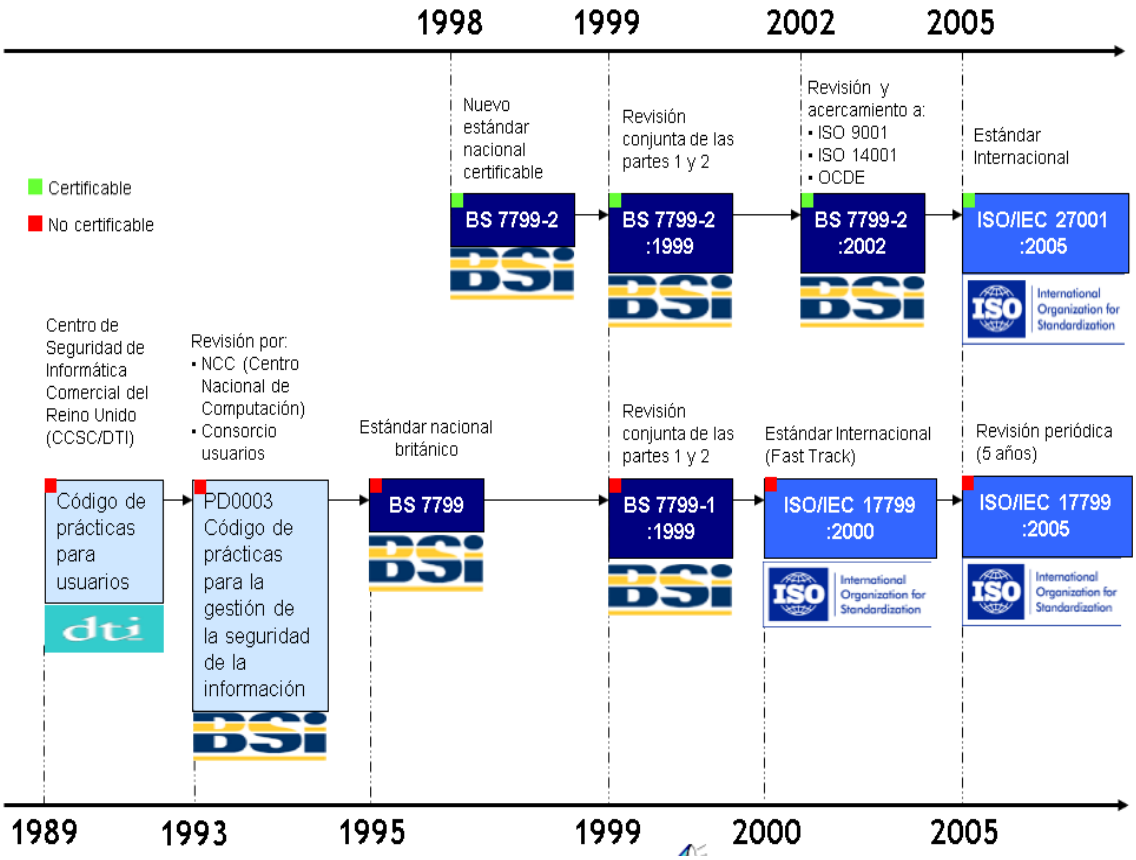


Ilustración 2: Historia de ISO 27001 e ISO 17799 (ISO 27000.ES, 2006).

A principios de 1995, apareció la norma BS 7799 de BSI (British Standards Institution) con la intención de proporcionar a las instituciones británicas prácticas seguras y adecuadas de manejo y gestión de la información.

El enfoque de la primera parte de la norma (BS 7799-1) fue una guía de buenas prácticas, en cambio la segunda parte (BS 7799-2), publicada en 1998, estableció los

requisitos de un sistema de seguridad de la información cuya base fue el ciclo PDCA (planificar, hacer, verificar y actuar).

ISO adoptó posteriormente a los dos complementos de la norma BS 7799 sin ningún tipo esencial de modificación denominándose como ISO/IEC 17799 en el año 2000; esta última contenía un conjunto de normas sobre buenas prácticas, las mismas que se podían aplicar en cualquier tipo de organización sin tener en cuenta el tamaño de la misma, flexible e independiente ante cualquier procedimiento de seguridad.

Cuya norma seria adecuada a la filosofía de normas ISO de sistemas de gestión.

En 2005, con una mayor acogida y con empresas ya certificadas en BS 7799-2, se publicó el estándar ISO 27001 quien se convirtió en la norma principal de la serie, conteniendo los requisitos del sistema de gestión de seguridad de la información. Al tiempo se revisó y actualizó ISO 17799, cuya norma se renombro como ISO 27002:2005.

Por último, la norma actual ISO/IEC 27001:2013, ISO/IEC 27002:2013 ambas aprobadas el 25 de septiembre del 2013 (ISO 27000.ES, 2006).

1.6. Descripción general de la norma

La norma ISO 27001 se encarga de la seguridad de la información la cual debe regularse bajo controles, basada en normas estratégicas y enfocadas en la aplicación de un sistema de gestión de seguridad de la información, permitiendo que haya confidencialidad, integridad y acceso a la misma. Dentro de ella incluye la información interna y externa. ((ISO/IEC 27000: 2014 - 3.2.1, 2014).

1.7. Introducción a Cloud Computing

Cloud Computing, también conocido como computación en la nube es un paradigma y modelo de negocio, de servicios, que ha permitido en la actualidad brindar a los empleados en el contorno tecnológico de la información, ingeniería y en el mundo

computacional una gran acogía porque ha impactado en su uso y los beneficios que conlleva, lo interesante es el alcance en que a simple vista “Cloud Computing” puede ofrecer.

Definiendo a “Cloud Computing” principalmente como un modelo de negocio basado en internet, en el que se comparten recursos de hardware, además de tres aspectos fundamentales de servicios: Infraestructura como un servicio (IAAS), que se refiere a que “los usuarios arriendan los recursos que van a ocupar para sus procesos, por cuanto y cuando sean necesarios”.

El segundo servicio es la Plataforma como un servicio (PAAS), que se orienta a los desarrolladores a crear aplicaciones y servicios que funcionen a través del internet, este servicio provee el entorno de programación que facilita a los desarrolladores su ejecución.

El tercer servicio es Software como un servicio que se refiere a brindar aplicaciones a los consumidores finales, con el fin que puedan acceder a ellas ya que están alojadas en la nube, siendo operadas directamente por el proveedor del servicio y pueden ser utilizarse en una amplia variedad de tareas (RedHat, 2019)

1.8. Modelos de Servicios

Las organizaciones nuevas cuentan con más opciones en cuanto a cómo hacer uso de sus infraestructuras, delegación de responsabilidades a los proveedores de servicio y ahorro de costos. Convirtiéndose los modelos de servicios en parte fundamentales de la tecnología en la actualidad y de los modelos de negocio, forzando a nuevos dilemas y competencias para adaptarse a las nuevas estrategias que rigen sobre la tecnología.

Los modelos de servicios se refieren a la forma en que están disponibles al cliente, estos son interdependientes y con una sinergia entre ellos, por ejemplo,

Infraestructura como un servicio (IaaS), Plataforma como un servicio (PaaS) y Software como una asistencia (Saas).

Hoy en día, como regla general, las empresas estiman que los servicios de plataforma y de software se adaptan más a sus necesidades que los de infraestructura. Por lo tanto, perderá mercado con respecto a sus otros dos servicios antes mencionados. (RedHat, 2019)

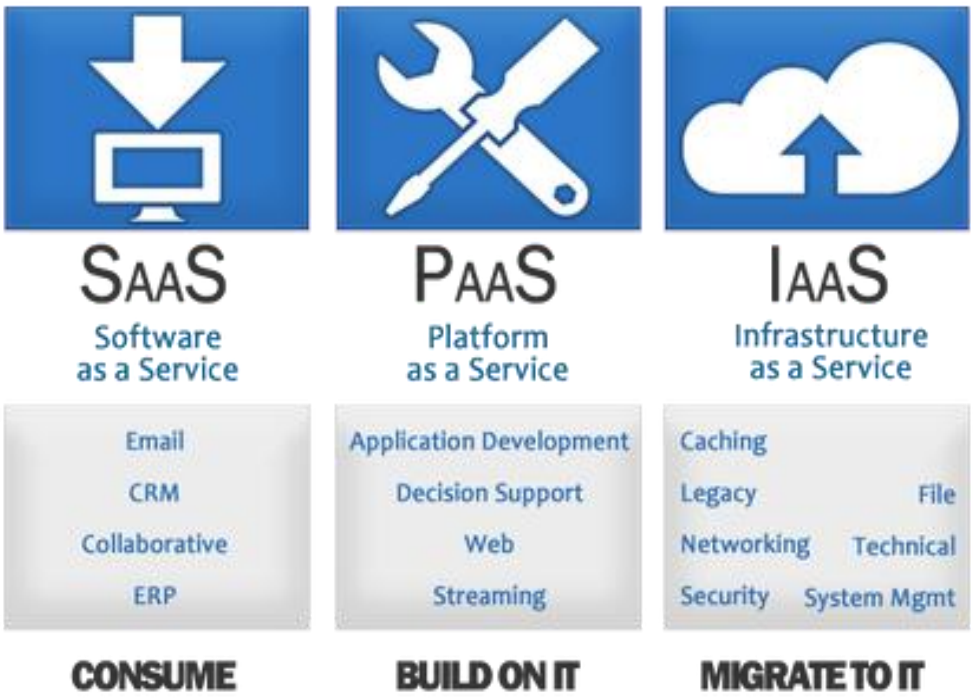


Ilustración 3: Modelo de servicios (WordPress.com, 2019)

1.8.1. Infraestructura como un servicio (IaaS)

Lo primordial de IaaS es que la empresa externaliza sus componentes de infraestructura, de forma que el proveedor brinde acceso, alojamiento, funcionamiento

y mantenimiento del mismo. Los componentes pueden incluir máquinas virtuales, firewalls, conexiones de redes y procesamiento entre recursos.

Algunos de los beneficios de IaaS son:

- Acceso rápido y facilidad para cumplir con las capacidades que la empresa lo requiera en su despliegue.
- Escalabilidad: recursos disponibles como y cuando el cliente los necesita, no retrasos en expandir la capacidad, y disminución del recurso malgastado.
- Simplicidad: asume gestión el proveedor de la infraestructura (hardware, software), y cualquier otro detalle vinculado a la misma.
- Reducción del costo de inversión en hardware: IaaS asume y soporta la configuración y mantenimiento por su proveedor.
- Seguridad física de los lugares de los centros de datos.
- Independencia de la ubicación: acceso al servicio desde cualquier sitio, contando con una conexión a Internet y protocolos de seguridad.

La mayor desventaja de IaaS es el riesgo del negocio es decir la confianza al proveedor, disponibilidad y seguridad de sus datos (IONOS España, 2019).

El principal proveedor de IaaS es Amazon asignado a Amazon Web Services[1]; en forma general el proveedor brinda al cliente la capacidad de ocupar o emplear los recursos necesarios para que funcione el software (sistemas operativos o aplicaciones) que requiere y construir sus propias plataformas.

[1] (Amazon Web Services, Inc,2016)

Con ello el cliente realizara todo sin tener que controlar, administrar, monitorear, ni configurar la infraestructura, pero tiene control sobre los sistemas operativos, aplicaciones desplegadas y almacenamiento.

Simplificando todo, IaaS es un modelo en el que el proveedor cumplirá con albergar el hardware (almacenamiento, redes, servidores), y demás componentes que conforman la infraestructura tecnológica permitiendo al usuario o cliente realizar todo sin la necesidad de administrarlo por sí mismo.

1.8.2. Plataforma como un servicio (PaaS)

Este modelo otorga un entorno o plataformas ya previamente construidas orientadas al desarrollo, despliegue, almacenamiento, mantenimiento y aplicaciones propias del cliente, lo cual es distribuida a través del internet.

Facilita que las aplicaciones del cliente no estén asociados a las complejidades y preocupaciones de su gestión, con ello todos los recursos que necesite serán configurados por el proveedor.

Entre las características que incluye PaaS son:

- Entorno de programación
- Sistemas Operativos
- Soporte al cliente
- Almacenamiento
- Hosting
- Sistemas de administración de BD (bases de datos)

Los entornos platforms as a service representan una oportunidad excelente en el momento de utilizar aplicaciones que estén conectadas a la nube, sin embargo, hay

muchas personas que aún no han usado este servicio debido a que tienen muchas inquietudes o porque desconocen como iniciar su uso, a continuación, se describen los beneficios de PaaS.

- Desarrollo de Software: permite utilizar entornos individuales para los diferentes procesos de desarrollo (desarrollar, probar, alojar) de sus aplicaciones.
- Ser ubicuo para la colaboración de proyectos y capacidad de albergarlos para su progreso.
- Flexibilidad: control de las herramientas y adaptación a las necesidades específicas de las mismas.
- Maximizar el tiempo: evitando un tiempo inactivo del uso de las herramientas es decir interrupciones no planificadas.
- Escalabilidad: modificar las características si las circunstancias lo requieran.

Y su desventaja es que, dependiendo del proveedor de PaaS, el usuario podrá verse limitado en su interfaz, lenguaje o entorno de software adquirido.

El PaaS está enfocado a proveer API´s en las áreas que el usuario requiera por ejemplo esta Google App Engine, Akamai Edge Platform, Microsoft Azure Services Platform y Google Cloud Platform. (IONOS España, 2019).

1.8.3. Software como un servicio (SaaS)

Es un modelo de entrega de aplicaciones como servicio, mediante el cual el proveedor ofrece el uso bajo demanda y simplemente elimina la instalación de dicha petición (aplicación) en todos los ordenadores.

El cliente puede acceder a estos servicios utilizando un navegador de internet, con dicha facilidad no tiene por qué gastar más recursos en la ejecución, brindado una optimización de su uso.

Es importante señalar que el cliente no gestiona la infraestructura subyacente, únicamente la aprovecha para cumplir con sus necesidades.

Entre sus beneficios consta:

- Es flexible: servicio bajo demanda.
- Estable: proveedores con reputación y protegidos.
- Despliegue rápido.
- Accesible: simplemente una conexión a internet.
- Versiones (Actualizadas).

Una de sus desventajas es la velocidad de las aplicaciones SaaS, pero poco a poco se irá mejorando con las nuevas tecnologías.

Ejemplos de SaaS, tenemos servicios de email, CRM´s y aplicaciones Web (COMUNICACION ONLINE, 2016)

1.9. Modelos de implementación Cloud Computing

Con respecto a los modelos de implementación existen 3 fundamentales y 1 no tan frecuente.

1.9.1. Nube Pública

La nube publica es aquel modelo el cual la tecnología es propia de una organización y a su vez se encarga de vender los servicios de Cloud Computing al público. Por lo general, los proveedores como Microsoft, Amazon AWS y Google

poseen y operan dicha infraestructura para ofrecerla mediante acceso a internet para el público en general (Cierco, 2011).

Con ayuda de este modelo los clientes no tienen control sobre la infraestructura, pero comparten la misma con una configuración limitada, protección y variaciones de disponibilidad por parte del proveedor.

Ejemplos simples, tales como los servicios en línea de almacenamiento (fotografías, documentos, videos, etc.), servicios de correo electrónico, o redes sociales.

La adopción de Cloud Computing en las empresas según el estudio realizado por Deloite en el año 2010, apuestan a que con una implementación de modelos tecnológicas basado en Cloud Computing tendrá un valor agregado y ventajas operacionales inmediatas para su negocio: una de ellas la eficiencia en costos, ajuste de la inversión y agilidad en los procesos.

Con ello se puede afirmar que gracias a que los recursos se ofrecen como un servicio, se pueden obtener una escala en su uso en función de su demanda y no tener grandes gastos en hardware para utilizar el servicio. Los proveedores de nubes públicas solo podrán gestionar la infraestructura y los recursos según la capacidad requerida por el mercado de sus usuarios.

Uno de los beneficios es la economía de escala, minimizando el coste de infraestructura distribuidas entre todos los usuarios, permitiendo a cada cliente operar según el modelo que se apegue a sus acuerdos de uso.

La nube pública es la opción acertada cuando se trata:

- Alta disponibilidad: el modelo es muy adaptable a las capacidades de sus distintos clientes y usos.
- Instalación fácil y bajo costo: consumo de los recursos prestados del proveedor en un costo reducido debido a no existir cantidades de

instalaciones sino solo un cómputo centralizado de forma general para todos.

- Adecuado uso de los recursos: ocupar el 100% de la infraestructura sin desperdiciarlo para no tener ninguna pérdida de la inversión realizada.

En el caso de una nube publica por la existencia de grandes cantidades de clientes accediendo al recurso, este aspecto se minimiza y se usa con mayor eficiencia la tecnológica disponible (Torres, 2011).

1.9.2. Nube Privada

En la nube privada, la infraestructura se centra como propiedad exclusiva de un único cliente u organización. Además, nace este concepto debido a que muchas organizaciones se mantuvieron alejadas de emplear la nube pública, principalmente por el tema de "seguridad de su información" y que en este modelo supone una mejoría sustancial.

Por lo tanto, alojar datos y aplicaciones con esta nube implicara un entorno más seguro y controlado respecto a las nubes públicas. A través de líneas privadas (VPN) o conexiones cifradas, seguras para clientes autorizados y especializados en operar, reduciendo los problemas de seguridad y limitando el acceso no autorizados conllevando a una administración de forma adecuada.

La realización de una nube privada requiere un nivel y compromiso significativo para virtualizar el entorno empresarial ofreciendo un nivel mayor de seguridad y control.

En resumen, una nube privada es la mejor opción cuando se requiere:

Seguridad de datos y privacidad, mayor nivel.

Nivel de control elevado.

Eficiencia en la nube y control de los datos. (Red Hat , 2019).

1.9.3. Nube Hibrida

La nube hibrida es una combinación de la nube publica con la nube privada, como punto de intersección el hecho de contar con la facilidad de dos infraestructuras para optimizar el uso de los recursos y minimizar costos sin olvidar de crear una solución personalizada en base a los requerimientos de la organización.

Un aspecto de dicha nube es su eficiencia por ser más escalables y rentables por reducir la demanda de una nube privada al no contener datos no sensibles o aplicaciones y transferirlas a una nube pública (Mayevsky, 2013).

Se centra este tipo para empresas con alto valor dinámico en el manejo de datos y procesamiento de información con una alta carga de trabajo.

Por ejemplo, entidades financieras (transaccionales) en donde el manejo y sobrecargas, pueden causar un colapso si no se usara este tipo de nubes que permiten una redistribución de procesamiento para optimizar los recursos y que el sistema este funcional.

El mayor reto en las nubes hibridas es darle un seguimiento de las múltiples plataformas de seguridad y asegurar que todos los aspectos del negocio puedan comunicarse entre sí.

Una nube hibrida es accesible cuando:

- Para pruebas y desarrollo en la nube pública y en la nube privada un alojamiento para el despliegue en producción.
- Para aplicaciones internas y externas correspondientes al uso de cada nube.

- Interacción con clientes (nube pública) y confidencialidad (nube privada) (Red Hat , 2019).

1.9.4. Otros tipos

El modelo que es más empleado y se distingue es el de Nube Comunitaria o Nube en Comunidad.

Una nube de comunidad es un modelo de servicio que se caracteriza por compartir entre varias organizaciones y tener intereses comunes o necesidades para apoyarse mutuamente y lograr sus objetivos de negocio.

Se sitúan en un punto intermedio respecto a la economía y seguridad frentes a las nubes públicas y privadas contando que las organizaciones participantes tengan beneficios, pero con mayor nivel de privacidad, seguridad y cumplimientos de políticas dentro de sus alianzas estratégicas que contemplan. (Red Hat , 2019).

1.10. Seguridad

Para proteger la información de una empresa se deben tomar varias medidas, pero la principal es la prevención ya que este el origen de casi todos los problemas informáticos, y son causados por el desconocimiento. Toda empresa debe proteger su información.

1.10.1. Problemas y riesgos

Proteger la información requiere de una inversión económica que en muchas ocasiones las empresas no están dispuesta a realizar, sin embargo, comparando al valor que mantiene la información de una empresa al ser considerado como un activo, la inversión es baja. La información en general tiene varias amenazas, por eso se debe

contar con un sistema de información confiable y seguro, por lo que han establecido protocolos, reglas y técnicas para prevenirlas.

Una amenaza se puede categorizar en dos, de acuerdo al efecto que causan y de acuerdo a su origen, en la primera se encuentra: intercepción, modificación, interrupción y generación: mientras que en el segundo grupo pueden ser: naturales, físicas, involuntarias, intencionadas.

Las amenazas pueden ser causadas por: usuarios, programas maliciosos, errores de programación, siniestros (Digimarketing Copyrigth©, 2016).

Entre los principales riesgos que se pueden presentar la información en una empresa se encuentra:

Ordenadores sin antivirus: los antivirus pueden bloquear o eliminar gran parte de virus informáticos, hay que tomar en cuenta que un ordenador conectado o no al internet puede correr un peligro grande ya que el virus no solo se puede colar por una descarga sino también por medio de un USB que se use, por lo que trabajar en un ordenador sin antivirus es un riesgo que debe ser tomado en cuenta.

Copias de Seguridad: realizar copias de seguridad es importante en el caso de restauración de un ordenador, si no se cuenta con las copias de seguridad se puede perder gran información como catálogos de clientes, productos; sin embargo, estas copias de seguridad deben ser almacenados en un dispositivo seguro, y nunca realizar la copia de seguridad en el propio ordenador, pues si el ordenador resulta infectado pueda que también se vea afectada la copia de seguridad.

Correos electrónicos sospechosos: la ciber-delincuencia aprovecha la mínima oportunidad para poder acceder a la información que le interesa por lo que realiza el envío masivo de correos electrónicos con temas novedosos, y al no tener un criterio para tratar con el correo electrónico el usuario termina haciendo lo que los ciber-delincuentes desean. Por lo que lo más recomendable es no descargar archivos adjuntos de correos que provienen de personas o entidades sospechosas.

Mensajes en las redes sociales: la navegación permanente en las redes sociales también es aprovechada por la ciber-delincuencia, pues a través de un enlace se puede direccionar a una web infectada lo que termina infectando los dispositivos utilizados en ese momento, así también recabar datos personales (GADAE NETWEB, 2019).

1.10.2. Medidas de control de seguridad

Para el control de la seguridad de la información existen varios protocolo y medidas que son muy útiles, dichos controles se agrupan en: control físico, control técnico y control administrativo.

Controles físicos: comprende la implementación de medidas de seguridad con una estructura definida de acuerdo a las necesidades, con el fin de prevenir el acceso no autorizado

Los controles físicos pueden ser: cámaras de circuito cerrado, puerta de acero con seguros especiales, acceso biométrico.

Controles Técnicos: se basa en la tecnología y se utiliza para controlar el acceso a información confidencial mediante una estructura física implementada dentro de la red, los controles técnicos incluyen tecnología como: encriptación, tarjetas inteligentes, autentificación a nivel de la red, software de auditoría de integridad de archivos, listas de control de acceso.

Controles administrativos: dentro de estos controles se encuentran factores humanos e incluye todos los niveles de la organización, determina el rol de cada usuario y los accesos permitidos, los controles administrativos son: preparación para desastres, entrenamiento y difusión del conocimiento, selección del personal (Red Hat Enterprise, 2019).

1.10.3. Seguridad y Privacidad

La privacidad es el derecho a mantener la información de manera reservada y datos confidenciales, la privacidad de la información se ve violentada por: cookies, spywares, virus, piratas informáticos.

Existen herramientas que garantizan la privacidad de la información como son: contraseñas, configuración del firewall, criptografía.

Contraseñas: para controlar el acceso hacia algún recurso que se encuentra en la red se puede usar contraseñas las mismas que deben ser entregadas solo a personas que requiera utilizar de manera frecuente y segura dicho recurso, para mayor seguridad esta contraseña debe mantenerse de forma secreta.

Firewall: generalmente los ataques a la privacidad se ven realizados por un spyware que esta categorizado dentro de un malware, este programa se instala en un ordenador para recabar información, la información más recopilada es la información del usuario con el fin de distribuirlo a empresas publicitarias, la vía de instalación es la conexión a internet por lo que también se puede ver afectado el ancho de banda y la velocidad de transferencia de datos.

Criptografía: utiliza técnicas especiales para el cifrado y descifrado de la información y permite el intercambio de mensajes que solo pueden ser leídos por las personas a las que se encuentras dirigidas y que pueden descifrarlos (Albert de la Cruz, 2010).

1.11. Ciclo de vida de la Información

En la seguridad de la información de un ambiente Cloud Computing, la protección de datos es una parte fundamental es por ello que debe ser fortalecido.

Para esto se debe diferenciar entre ciclo de vida de la información y ciclo de vida de los datos, la primera hace referencia a la creación, almacenamiento, utilización, archivo

y destrucción, mientras que la segunda corresponde a la seguridad, geo-localización, permanencia y backups. (Gonzáles Hernández, 2016)

1.12. Ventajas y desventajas de un ambiente Cloud Computing

Entre las principales ventajas se puede mencionar

- El acceso a la información y a las aplicaciones se la puede realizar desde cualquier lugar y en cualquier momento ya que Cloud Computing se encuentra diseñado para poder utilizarse a la distancia.
- Los servicios alojados en Cloud Computing permiten a las organizaciones dejar la preocupación por adquirir software y hardware para las operaciones propias de cada empresa.
- La actualización de las aplicaciones es constante por lo que las organizaciones siempre contaran software actualizado.
- La infraestructura que el cliente adquiere es realmente la que necesaria y con un bajo costo en relación a tener una infraestructura propia en un ambiente tradicional.

Las desventajas que presenta el ambiente Cloud Computing se detallan a continuación.

- Se genera una interdependencia hacia los proveedores por la centralización de almacenamiento y de aplicaciones.
- Para acceder a las aplicaciones y a los datos se debe tener una conexión a internet.
- Se exponen datos sensibles y confidenciales de la empresa lo que puede ocasionar el robo de información.
- Los servicios tecnológicos dependen exclusivamente de los proveedores de servicios.

- La información recorre por varios canales, por lo que es sensible a la inseguridad (Gonzáles Hernández, 2016)

2. CAPÍTULO II: DISEÑO DEL MODELO DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

2.1. Norma ISO 27001:2013

Para diseñar el modelo del sistema de seguridad de la información dentro de un ambiente Cloud Computing, se toma como base la ISO27001:2013 ya que esta ISO especifica los requisitos necesarios para: establecer, implementar, mantener y mejorar el sistema de seguridad de la información dentro de una organización. Incluye requerimientos para evaluar y tratar los riesgos. Los requisitos definidos en la ISO27001:2013 son genéricos y se pueden aplicar en todas las organizaciones sin importar la naturaleza, tipo o tamaño de la misma.

La norma ISO 27001 establece controles apropiados para mitigar el peligro mediante la permisividad de establecer mejoras continúas evaluando cualquier tipo de riesgo o amenaza que afecte o ponga en riesgo la información de cualquier organización.

La norma ISO 27001 consiste en un ciclo de planificar, hacer, verificar y actuar

Planificar: en esta parte del ciclo se establece el alcance, análisis, controles, competencias, se mapean procesos y se definen responsables.

Hacer: corresponde a la implantación del plan de gestión, controles.

Controlar: con la realización de auditorías internas, revisión permanente por la dirección, y la ejecución de controles, indicadores y métricas.

Actuar: se aplican las acciones preventivas y correctivas que permitan la mejora en los procesos.

2.2. Fases de la norma ISO 27001:2013

1. Alcance
2. Referencias Normativas
3. Términos y definiciones
4. Contexto de la organización
    - Comprender la organización y su contexto
    - Comprender las necesidades y expectativas de las partes interesadas
    - Determinar el alcance del sistema de gestión de seguridad de la información
    - Sistema de gestión de seguridad de la información.
5. Liderazgo
    - Liderazgo y compromiso
    - Política
    - Roles organizacionales, responsabilidades y autoridades
6. Planificación
    - Acciones para abordar riesgos y oportunidades
        - General
        - Evaluación de riesgos de seguridad de la información
        - Tratamiento de riesgos de seguridad de la información
    - Objetivos de seguridad de la información y planes para alcanzarlos
7. Apoyo
    - Recursos
    - Competencia
    - Conciencia

- Comunicación
- Información Documentada
    - General
    - Creando y actualizando
    - Control de información documentada

8. Funcionamiento
    - Planificación y control operacional
    - Evaluación de riesgos de seguridad de la información
    - Tratamiento de riesgos de seguridad de la información
9. Evaluación de desempeño
    - Monitoreo, medición, análisis y evaluación
    - Auditoría interna
    - Revisión de gestión
10. Mejora
    - No conformidad y acción correctiva
    - Mejora continua (©ISO/IEC 2012- All rights reserved, 2013)

2.3. Descripción de las fases de la Norma 27001:2013

2.3.1. Alcance

La norma ISO 27001:2013 se puede aplicar en cualquier tipo de organización, por lo que indica los requisitos necesarios para: establecer, implementar, mantener y mejorar continuamente el sistema de gestión de seguridad de la información. Incluye también los requisitos necesarios para realizar la evaluación y tratamiento de la seguridad de la información. (Advisera, 2019)

2.3.2. Referencias Normativas

Toma como referencia obligatoria a la norma ISO27000, ya que aquí se describen definiciones nuevas y términos (ISOTools, 2017).

2.3.3. Términos y definiciones

Con el fin de mantener una guía de términos y definiciones, también se realiza una referencia a la norma ISO 27000 (ISOTools, 2017).

2.3.4. Contexto de la organización

Se enfoca en comprender los problemas internos y externos de una organización, mediante la identificación de la organización y sus necesidades (ISOTools, 2017).

2.3.5. Liderazgo

Define responsabilidades de alta dirección y demuestra el compromiso para garantizar que los objetivos definidos se cumplan, así también poner a disponibilidad los recursos necesarios, asignar roles y responsabilidades (Advisera, 2019)

2.3.6. Planificación

Define los objetivos para la seguridad de la información y requerimientos para evaluar y tratar los riesgos (Advisera, 2019)

2.3.7. Apoyo

Establece los recursos, competencias que permitan gestionar de manera óptima el Sistema de Gestión de Seguridad de la información (ISOTools, 2017).

2.3.8. Funcionamiento

En esta fase se describe los requerimientos que permitan medir el funcionamiento del Sistema de Gestión de Seguridad de la Información, por lo que es necesario que las organizaciones planifiquen y controlen las operaciones así también los requisitos necesarios para la seguridad (Advisera, 2019).

2.3.9. Evaluación de desempeño

Mediante las auditorías internas y revisiones, se identifica y mide la eficiencia de un sistema de Gestión de Seguridad de la Información (Advisera, 2019)

2.3.10. Mejora

Se realiza la contabilización y comparación de los registros no conformes identificados, con las acciones correctivas establecidas. Con el fin que las no conformidades no sean repetitivas y las acciones tomadas sean efectivas (ISOTools, 2017)

2.4. Documentos y Registros

La norma ISO27001:2013 se requieren varios documentos y requisitos, sin embargo, no todos los documentos son obligatorios.

Los documentos requeridos son los siguientes

2.4.1. Documentos Obligatorios

- Alcance del SGSI
- Políticas y objetivos de seguridad de la información
- Metodología de evaluación y tratamiento de riesgos
- Declaración de la aplicabilidad
- Plan de tratamiento del riesgo
- Informe sobre evaluación y tratamiento de riesgos
- Definición de funciones y responsabilidades de seguridad
- Inventario de activos
- Uso aceptable de los activos
- Políticas de control de acceso
- Procedimientos operativos para gestión de TI
- Principios de ingeniería para sistema seguro
- Política de seguridad para proveedores
- Procedimiento para la gestión de incidentes
- Procedimientos de la continuidad del negocio
- Requisitos legales, normativos y contractuales (Advisera, 2019)

2.4.2. Documentos no obligatorios

- Procedimiento para el control de documentos
- Controles para gestión de registros
- Procedimiento para auditoría interna
- Procedimiento para medidas correctivas
- Política trae tu propio dispositivo (BY OD)
- Política de clasificación de la información
- Política de claves
- Política de eliminación y destrucción
- Procedimiento para trabajo en áreas seguras
- Política de pantalla y escritorio limpio
- Política de gestión de cambio
- Política de creación de copias de seguridad
- Política de transferencia de la información
- Análisis de impacto en el negocio
- Plan de prueba y verificación
- Plan de mantenimiento y revisión

2.4.3. Requisitos

- Registro de capacitación, habilidades, experiencia y calificaciones
- Monitoreo y resultados de medición
- Programa de Auditoria interna
- Resultados de auditorías internas
- Resultados de la revisión por parte de la dirección
- Resultado de medidas correctivas
- Registro sobre actividades de usuarios, excepciones y eventos de seguridad (Advisera, 2019)

2.5. Adaptación de la norma ISO 27001:2013 a un ambiente Cloud Computing

A pesar que la norma ISO 27001:2013 indica que se adapta a cualquier tipo de organización sin importar el entorno del negocio, en el presente proyecto se realizara un análisis de las fases que se adaptan exclusivamente a un ambiente Cloud Computing.

Fase	Análisis
1. Alcance	Esta fase es un requisito para que una organización obtenga la certificación, por lo tanto, debe formar parte de la adaptación a un ambiente Cloud Computing.
2. Referencias Normativas	Proporciona definiciones y términos nuevos, al ser Cloud Computing un ambiente nuevo en el que se va a aplicar la norma se considera necesario.
3. Términos y definiciones	Hace relación a la fase dos por lo no será considerada para el ambiente Cloud Computing.
4. Contexto de la organización	Se enfoca en el análisis de los problemas internos y externos de cada organización, Pero en un ambiente Cloud Computing debe ponerse especial enfoque a los proveedores que brindan este ambiente.

5. Liderazgo	Se definen roles y responsabilidades que deben considerarse para el manejo de la información en un ambiente Cloud Computing
6. Planificación	Define los requerimientos para evaluar y tratar los riesgos por lo que se debe considerar en el ambiente Cloud Computing
7. Apoyo	Define recursos, comunicación y competencia por lo que esta fase si se considera para el ambiente Cloud Computing exceptuando el control de documentos y registros.
8. Funcionamiento	Al enfocarse en la implementación para evaluar y tratar riesgos, es una fase que se debe incluirse en el ambiente Cloud Computing
9. Evaluación de Desempeño	Esta fase debe se orienta a la realización de auditorías internas por lo que no se considera para el modelo en el ambiente Cloud Computing.
10. Mejora	Esta fase se enfoca en el tratamiento para la corrección de inconformidades, sin embargo, estas generalmente se presentan por parte de los clientes, por lo que esta fase

	no se considera para el ambiente Cloud Computing

Tabla 1: Adaptación de norma ISO 27001 a Cloud Computing (Peñafiel, 2019)

Una vez analizada la norma ISO 27001:2013, se establecen las siguientes fases en el Diseño de un modelo para establecer un sistema de gestión de la seguridad de la información dentro de un ambiente Cloud Computing



Ilustración 4: Fases elegidas en un modelo Cloud Computing (Peñafiel, 2019)

2.6. Documentación para un ambiente Cloud Computing

la norma ISO27001:2013 agrupa a los documentos en obligatorios y no obligatorios, en un ambiente Cloud Computing algunos de los documentos agrupados en no obligatorios deben considerarse como obligatorio por lo que a continuación, se enumera los documentos necesarios en un ambiente Cloud Computing.

En el Anexo 3 se realiza una descripción del contenido de cada uno de los documentos definidos como obligatorios para un ambiente Cloud Computing.

- Alcance del SGSI
- Políticas y objetivos de seguridad de la información
- Metodología de evaluación y tratamiento de riesgos
- Declaración de la aplicabilidad
- Plan de tratamiento del riesgo
- funciones y responsabilidades de seguridad
- Inventario de activos
- Políticas de control de acceso
- Procedimientos operativos para gestión de TI
- Principios de ingeniería para sistema seguro
- Política de seguridad para proveedores
- Procedimiento para la gestión de incidentes
- Política de claves
- Política de eliminación y destrucción
- Política de creación de copias de seguridad

3. CAPÍTULO III: ACTIVOS – RIESGOS – VULNERABILIDADES Y AMENEZAS EN UN AMBIENTE CLOUD COMPUTING

El objetivo principal de la gestión de riesgos de la información es la identificación de riesgos, vulnerabilidades y amenazas de la información con el fin de tomar medidas que ayuden a prevenir o corregir dichas amenazas.

3.1. Activos

3.1.1. Identificación de Activos

Se considera un activo a cualquier cosa que posea valor para la entidad, sean bienes materiales o información propia de la empresa que permite establecer reglas de negocio con los clientes.

Una organización dispone de varios activos que ayudan a ejecutar los procesos propios de la empresa, sin embargo, en muchas ocasiones estos activos son desconocidos por el personal interno de la organización lo que impide que algunos procesos no se puedan ejecutar de manera inmediata o continua, por lo tanto, es muy importante identificarlos y difundirlos de acuerdo al área y necesidades del personal.

Al momento de migrar los datos al ambiente Cloud Computing sea de forma parcial o total, los activos deben ser identificados de acuerdo a su valor en función de la confidencialidad, integridad y disponibilidad, y asociarlo a un riesgo, también se debe considerar el aumento de tráfico en la red, las operaciones y datos.

Confidencialidad: es la propiedad de la información de cada organización, y debe ser accedida solo por personas autorizadas, la confidencialidad se considera como una

garantía de acceso a la información solo por usuarios autorizados para de esta manera evitar la divulgación de la misma.

Integridad: se refiere a que la información no debe ser alterada accidental o maliciosamente, la información solo se debe modificar con una autorización.

Disponibilidad: en un ambiente Cloud Computing tanto la información como los recursos debe estar disponibles en todo momento, para que los usuarios que la requieran puedan acceder sin ningún inconveniente.

Para identificar los activos se la puede hacer con la siguiente matriz.

ACTIVO				PROCESO
Item	**Descripción**	**Tipo**	**Propietario**	

Tabla 2: Identificación de activos en Cloud Computing (Peñafiel, 2019)

3.1.2. Clasificación de Activos

De acuerdo al entorno de negocio de una organización, estos disponen de varios recursos que permiten ejecutar distintos procesos propios de la organización, por lo que es muy importante que sean clasificados de acuerdo a su función y puedan ser utilizados

eficientemente, esta clasificación permite optimizar recursos así también el aumento en la productividad.

Los activos se pueden clasificar de acuerdo a: servicios, datos, software, hardware, redes de comunicación, soportes de información, equipamientos auxiliares, instalaciones, personal.

3.1.3. Tasación de activos

Una vez que se han identificado y clasificado los activos estos deben tasarse de acuerdo a la disponibilidad, confidencialidad e integridad, se verifica de qué manera afecta a estas tres condiciones la falla o pérdida de cierto activo y con el fin de ubicar los activos que pueden detener la ejecución algún proceso o procesos.

Para la tasación de los activos se puede aplicar la escala de Likert con un rango de valoración de 1 a 5 iniciando de muy bajo a muy alto.

ACTIVOS	CRITERIOS DE EVALUACIÓN			TOTAL
	Confidencialidad	Integridad	Disponibilidad	

Tabla 3: Matriz para la tasación de activos en Cloud Computing (Peñafiel, 2019)

3.2. Riesgos en un Ambiente Cloud Computing

3.2.1. Identificación de Riesgos

Cuando una empresa o negocio migra de un ambiente tradicional a un ambiente Cloud Computing la seguridad de la información de la misma se puede ver afectada por muchos riesgos, por lo tanto, dichas empresas deben buscar la manera de mitigarlos aplicando acciones correctivas o preventivas. (EVALUANDO CLOUD.COM, 2015).

Se considera un riesgo a la posibilidad de que alguna amenaza explote una vulnerabilidad causando daño o perdida a un activo de la información.

Los riesgos que presenta el ambiente Cloud Computing son iguales a los ambientes tradicionales como es la infraestructura no externalizada, sin embargo, los riegos más latentes en el ambiente Cloud Computing en términos de seguridad son:

Pérdida de Gobernanza: al momento que un cliente u organización migra a un ambiente Cloud Computing permite que el proveedor mantenga la seguridad de los datos, por lo que el cliente ya no tiene control sobre ellos

Riegos del cumplimiento normativo: si una empresa u organización obtuvo alguna certificación antes de migrar al ambiente Cloud Computing, es posible que alguno de sus procesos ya no cumpla con alguna norma.

Protección de datos: para un cliente es muy difícil comprobar que el proveedor utilice y aplique las técnicas necesarias para la gestión de datos y sobre todo que estas se encuentren en conformidad con la ley.

Vinculación: para que la migración de un proveedor a otro no sea un proceso complejo se deben aplicar procedimientos que se encuentren estandarizados.

Supresión de datos incompleta: se presenta cuando en los procesos de eliminación existen errores o los respaldos no se encuentran clasificados debidamente. De tal forma

que al igual que en un ambiente tradicional la eliminación de datos puede ser complicada en el ambiente Cloud Computing.

Fallo de aislamiento: al momento de querer separar los recursos de memoria, almacenamiento o enrutamientos, los mecanismos aplicados pueden presentar fallas de tal manera que la separación puede ser complicada.

Miembro malicioso: en toda organización existen perfiles de alto riesgo tales como la administración de sistemas o administración de la seguridad de la información, por lo que estos cargos deben asignarse a personas en las que se pueda confiar.

Comprometimiento de la interfaz: una interfaz es la conexión entre el usuario y los recursos de la organización por lo tanto es un punto con muchas vulnerabilidades al momento de conectarse al internet o realizar un acceso remoto.

3.2.2. Evaluación del Riesgo

Es el proceso que compara el riesgo con un criterio dado, con el fin de establecer la importancia del riesgo.

Se lo realiza en base a una estimación de nivel, probabilidad que suceda un incidente y el impacto que puede presentar.

Para cada riesgo se debe analizar varios parámetros como son.

- Nivel de probabilidad
- Grado de impacto
- Activos Afectados
- Nivel de riesgo

3.2.3. Agrupación de Riesgos

- Riesgos legales
- Riesgos técnicos
- Riesgos no específicos en un ambiente Cloud Computing
- Riesgos políticos.

Riesgos Legales

Entre los riesgos legales se puede considerar: riesgos de la licencia, la protección de datos, un cambio jurídico así también las órdenes judiciales. La probabilidad que sucedan estos riesgos se considera de alta a muy alta, ocasionando un impacto a las organizaciones de medio a alto.

Riesgos Técnicos

Los riesgos técnicos que se encuentran en un ambiente Cloud Computing son: finalización de recursos, abuso de funciones de usuarios con privilegios, fallo de aislamiento, intercepción de datos, perdida de datos en la subida o bajada de datos, pérdida de claves, escaneados maliciosos. La probabilidad que estos riesgos sucedan es de baja a media, pero en el caso que estos riesgos sucedan pueden ocasionar un impacto alto a las operaciones de las organizaciones.

Riegos no específicos en un ambiente Cloud Computing

Los riesgos que se pueden agrupar aquí son: administración de la red, cambios en a la configuración de la red, pérdida de copias de seguridad, suplantación de identidad, accesos no autorizados, catástrofes naturales. La probabilidad que estos

riesgos se presenten se encuentra en un rango de muy baja a baja, sin embargo, el impacto ocasionado puede ser de medio a alto.

Riesgos políticos.

La probabilidad que estos riesgos ocurran es de baja a muy alta ocasionando un impacto alto a muy alto; los riesgos que se agrupan aquí son: Fallo en la cadena de suministros, pérdida de la gobernanza, cancelación de los servicios en el ambiente Cloud Computing, adquisiciones realizadas por el proveedor del ambiente Cloud Computing, vinculación, cumplimiento.

3.2.4. Tratamiento de riesgos

Cuando el riesgo ya se encuentra evaluado, se deben definir las acciones que se deben ejecutar en cada uno, considerando tanto el impacto económico como operacional que puede sufrir la organización en el caso que un riesgo llegue a materializarse.

En base a la norma ISO27001-2013 el riesgo puede ser mitigado, aceptado, transferido o evitado, considerando que un riego no puede ser eliminado completamente.

Frecuentemente los riesgos deben ser analizados y controlados ya que nuevas vulnerabilidades o amenazas pueden afectarlos.

Los riesgos detectados en el ambiente Cloud Computing se pueden reducir o mitigar con el siguiente tratamiento.

Abuso y mal uso del Cloud Computing

- Implementación de procesos para validar y registrar los accesos.
- Verificar las credenciales de los usuarios con información más personalizada.
- Validaciones constantes de listas negras de las direcciones IP.
- No permitir pagos con tarjetas de crédito de terceros.

Interfaces Inseguras

- Crear interfaces de monitoreo más seguras.
- Aplicando el cifrado de datos validar la autenticación para los accesos.

Amenaza Interna

- Crear cláusulas de confidencialidad para los contratos del personal, incluso que apliquen un tiempo después de la separación definitiva de la empresa.

- Como cliente se puede solicitar al proveedor del servicio Cloud Computing una cláusula de transparencia para los procesos usados en el manejo de la información y la seguridad.

Inconvenientes con tecnologías compartidas

- Ya que al migrar la información al ambiente Cloud Computing también implica que tanto recursos y aplicaciones se deben compartir con otras organizaciones especialmente en el servicio IaaS, es por eso que se propone la implementación de buenas prácticas con respecto a la seguridad enfocándose especialmente en la instalación y la configuración de los servicios IaaS.

- Un constante monitoreo de estos servicios con el fin de detectar cambios y corregirlos inmediatamente de ser el caso.

Pérdida de la Información

- Generar e implementar interfaces robustas que permitan un control de acceso más seguro.
- Proteger los datos en todo momento que se ejecuten.
- Generación de claves basados en parámetros propios del cargo.
- Solicitar políticas de respaldo y eliminación de datos.

Secuestro de sesión

- Establecer políticas para compartir las credenciales entre usuarios.
- De la misma forma que se plantea generar claves con parámetros propios del cargo también se deben generar para validar la identidad de los usuarios.
- Detectar actividades no permitidas mediante un monitoreo permanente.

Riesgos por desconocimiento

- Divulgación a todo el personal de la infraestructura técnica de acuerdo a las necesidades propias del usuario.

  Emitir alarmas a usuarios con privilegios sobre actividades críticas que realicen los demás usuarios

3.3. Amenazas

3.3.1. Identificación de amenazas

Las amenazas que pueden tener los activos en un ambiente Cloud Computing es una preocupación latente, es por ello que varias organizaciones de la seguridad de la información han realizado investigaciones para que sean utilizados tanto por clientes, proveedores y auditores de servicios.

Se considera una amenaza a la causa de un incidente no deseado, y como consecuencia puede dañar un sistema u organización.

Las principales amenazas detectadas se enfocan en la confidencialidad, integridad, privacidad, autentificación, disponibilidad y localización de los datos.

Uso inadecuado del ambiente Cloud Computing: Aunque para que un usuario o una organización puedan acceder a las plataformas que se encuentran en un ambiente Cloud Computing hay que seguir un proceso riguroso para la identificación, al final el único requisito es contar con una tarjeta de crédito activa, de tal forma que la contratación generalmente se la realiza de forma anónima por lo que el uso de la Infraestructura y Plataforma como servicio (IaaS y PaaS) permite que hackers o criminales utilicen las infraestructuras de otros clientes para su beneficio.

Interfaces inseguras: muchos proveedores ofrecen a sus clientes interfaces que permiten interactuar y controlar recursos, por lo que muchas organizaciones utilizan estas interfaces para monitorizar sus recursos en el ambiente Cloud Computing, sin embargo, estas interfaces pueden ser un riesgo para la seguridad, disponibilidad, confidencialidad e integridad de los datos por ser un medio para causar daños intencionados o accidentales, estas interfaces deben ser diseñadas para proteger la seguridad de los datos.

Amenazas internas: tal como sucede en un ambiente tradicional, los usuarios de una organización pueden acceder tanto a datos como a las aplicaciones propias de la empresa, sin embargo, al tener un acceso libre puede causar incidentes provocados en la seguridad de la información, sea por error o descontento. Por lo que las organizaciones deberían optar por procesos más rigurosos para la contratación del personal y de esta manera evitar que personas malintencionadas se adentren a sus empresas y obtengan información confidencial.

Inconvenientes con tecnologías compartidas: afecta principalmente a la Infraestructura como servicio (IaaS), ya que los componentes físicos no son diseñados para una arquitectura compartida, por lo que los hipervisores de virtualización pueden acceder a los recursos físicos, provocando incidentes en la seguridad de la información.

Este inconveniente se puede evitar mediante un sistema que pueda garantizar a cada usuario las operaciones, sin causar inconvenientes al resto de usuarios que se encuentren alojados en el mismo ambiente de tal forma que ningún usuario pueda ingresar a los activos que no le corresponda.

Perdida de datos: para los clientes que ofertan los servicios en un ambiente Cloud Computing la perdida de datos o la fuga de información puede traer consecuencias graves para su negocio.

Los datos se pueden perder por eliminación o modificación de la información sin que exista un respaldo de dicha información. Por las interacciones que existe en un ambiente Cloud Computing este riesgo es alto.

La realización de backups debe ser un proceso primordial por parte del proveedor Cloud Computing para de esta manera garantizar la integridad de los datos.

Secuestros de sesiones: en un ambiente tradicional y en el ambiente Cloud Computing, las fallas en las seguridades o el phishing permiten que usuarios indebidos

tengan acceso a datos confidenciales, mediante el robo de credenciales a usuarios propios de la empresa.

Cuando un usuario indebido accede a las credenciales de otro, puede realizar actividades como la manipulación de datos, transacciones, emisión de información falsa, así también realizar un redireccionamiento a un sitio malicioso o ilegitimo.

En el ambiente Cloud Computing se debe prestar mucha atención a este riesgo para que los usuarios maliciosos no tengan acceso a las credenciales de otros usuarios y evitar que la reputación del proveedor se vea comprometida.

Riesgos por causa del desconocimiento: la razón más importante por la que un cliente puede migrar de un ambiente tradicional a un ambiente Cloud Computing es que este puede concentrarse en las actividades de su negocio, dejando de lado la preocupación por la adquisición de software y hardware necesario para el funcionamiento, sin embargo el cliente debe tener pleno conocimiento de la infraestructura adquirida, así también, conocer con quien o quienes comparte dicha infraestructura con el fin de tomar medidas de seguridad para proteger la información.

3.4. Vulnerabilidades

3.4.1. Identificación de Vulnerabilidades

Las vulnerabilidades que se presentan en un ambiente Cloud Computing son las mismas de un ambiente tradicional, sin embargo, existen otras vulnerabilidades que pueden causar mayor daño en un ambiente Cloud Computing

Se considera una vulnerabilidad a la debilidad que presenta un activo el mismo, puede ser explotado por una amenaza.

Existen vulnerabilidades de seguridad específicas y no especificas en un ambiente Cloud Computing, Las principales vulnerabilidades detectadas son:

- Vulnerabilidades específicas en un ambiente Cloud Computing
    - Sistemas pobres de Autentificación, Autorización y Auditoria.
    - Poco o nada de control en los procesos de registros de usuarios.
    - La infraestructura en un ambiente Cloud Computing se ve comprometida por el acceso que se realiza remotamente a la interfaz de gestión.
    - Autenticación baja en la codificación de la comunicación.
    - Gestión de claves sin los procesos necesarios.
    - Ausencias de acuerdos de soporte a proveedores PaaS o SaaS.
- Vulnerabilidades no específicas en un ambiente Cloud Computing
    - Ausencia de conciencia en la seguridad de la información en un ambiente Cloud Computing.
    - Ausencia de procesos investigativos al perfil de usuarios privilegiados.
    - La infraestructura en un ambiente Cloud Computing se ve comprometida por el acceso que se realiza remotamente a la interfaz de gestión.
    - Responsabilidades y funciones no definidas claramente entre clientes y proveedores.
    - Procesos inadecuados en la Seguridad Física.

- Inventario ausente o inadecuado de los activos de las empresas.

Para la identificación de las amenazas y vulnerabilidades se puede ayudar con la siguiente matriz.

Activo	Amenaza	Vulnerabilidades

Tabla 4: Levantamiento de Amenazas y Vulnerabilidades en Cloud Computing (Peñafiel, 2019)

4. CAPÍTULO IV: APLICACIÓN DEL MODELO DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN EN UN AMBIENTE CLOUD COMPUTING

La aplicación del modelo diseñado para un ambiente Cloud Computing, se realizará en una empresa tecnológica que ha realizado la migración parcial de la información a un ambiente Cloud Computing, empezando por el área técnica, la razón de iniciar por esta área es porque la empresa brinda el soporte a nivel nacional y el personal técnico necesita ingresar y descargar información en línea.

El proceso migrado se denomina Gestión de Informes Técnicos (GIT)

Gestión de Informes Técnicos (GIT): las actividades que se ejecutan en este proceso son: Ingreso, modificación, eliminación de Informes Técnicos, estos informes se ingresan a partir de la realización del mantenimiento preventivo o correctivo.

Nivel 1	**Nivel 2**	**Nivel 3**
Gestión de Informes Técnicos	*Mantenimiento Preventivo con Contrato*	*Realización del Mantenimiento*
	Mantenimiento Preventivo sin Contrato	
	Mantenimiento Correctivo con Contrato	
	Mantenimiento Correctivo sin Contrato	

Tabla 5: Mapa de procesos empresa Tecnológica (Peñafiel, 2019)

En el anexo 4 se detallan los procesos que se realizan en los mantenimientos preventivo con contrato, preventivo sin contrato, mantenimiento correctivo con contrato, correctivo sin contrato.

4.1. Alcance

Este manual reglamenta los procesos necesarios para establecer, implementar, mantener y mejorar continuamente el sistema de gestión de seguridad, Incluye también los requisitos necesarios para realizar la evaluación y tratamiento de la seguridad de la información.

4.2. Referencias Normativas

Cloud Computing: proporciona una infraestructura informática en la nube, y se encuentra disponible cuando el usuario lo requiera, para acceder a esta infraestructura es necesario contar con el servicio de internet.

Usuarios: persona que tiene acceso limitado a la información que se encuentra en Cloud Computing.

VPN: hace referencia a una conexión de red segura sobre una red pública no controlada.

Logs. Registro de eventos realizados en un tiempo particular.

GIT: Gestión de Informes Técnicos

Inventario Físico: Lista de repuestos y equipos que se pueden utilizar al momento de realizar un mantenimiento preventivo o correctivo.

Mantenimiento Preventivo: mantenimiento periódico que se realiza cada 3 meses con el fin que los equipos funcionen correctamente.

Mantenimiento Correctivo: mantenimiento que se realiza a un equipo cuando este presenta algún daño.

4.3. Contexto de la Organización

4.3.1. Comprender la organización y su contexto

El principal problema que enfrenta la empresa de tecnología es en la Gestión de Informes técnicos pues ahí, el personal ingresa información que debe estar disponible en todo momento ya que es requerida para las otras áreas de la empresa.

4.3.2. Comprender las necesidades y expectativas de las partes interesadas

El personal de las áreas comercio exterior y financiera son los interesados en disponer de la información en el momento que sea pertinente, ya que en el GIT ingresa información como la utilización de repuestos y equipos que deben ser facturados o no a las empresas que se brinda el servicio (información requerida por el área financiera), y por otro lado permite abastecer de repuestos para que se pueda brindar una atención optima al cliente (información requerida por el área de comercio exterior).

4.3.3. Determinar el alcance del sistema de gestión de seguridad de la información.

La Gestión de Seguridad de la Información se enfoca en la Gestión de Informes Técnicos poniendo énfasis en la información ingresada por el personal técnico con respecto al consumo de repuestos y equipos.

4.3.4. Sistema de Gestión de Seguridad de la Información

Para que la empresa de tecnología pueda establecer, implementar, mantener y mejorar la seguridad de la información debe cumplir con los requisitos de actualizar continuamente el inventario físico.

4.4. Liderazgo

Con el fin que la información se encuentre disponible para los usuarios interesados las gerencias de las áreas involucradas serán responsables de la actualización de la información específicamente del inventario físico y del registro de los informes.

4.4.1. Liderazgo y compromiso

La gerencia del departamento administrativo será la responsable de realizar la actualización permanente del inventario físico para que esté disponible y el personal técnico pueda visualizarlo en el momento que es requerido.

Por otro lado, la Gerencia del departamento técnico será responsable de exigir y comprobar que el personal técnico realice el ingreso en línea de los informes técnicos.

Mientras que la gerencia Financiera será responsable de dar de baja del inventario físico a los repuestos y equipos que han sido facturados.

4.4.2. Política

En la empresa de tecnología se define la política de seguridad con el fin de mantener y proteger los activos de la información involucrados en la Gestión de Informes Técnicos.

Los objetivos son:

- Fortalecer la seguridad de la información mediante la implementación de un sistema de Gestión para la Seguridad de la Información.
- Ejecutar programas de capacitación y concientización sobre la importancia del registro y actualización de la información. al personal involucrado en la Gestión de Informes Técnicos (GIT).

4.4.3. Roles organizacionales

Al ser el área técnica la parte más involucrada en la Gestión de Informes Técnicos se asigna a la Gerencia técnica el control permanente para la correcta ejecución de este proceso y de e acuerdo al requerimiento de la información en la Gestión de Informes Técnicos (GIT) se determinan los siguiente roles y responsabilidades.

Rol	Responsabilidad	Autoridad
personal Técnico	Ingresar informe Técnico	Gerencia Técnica
Gerencia Financiera	Dar de baja repuestos y equipos facturados	Gerencia General

Personal Comercio Exterior	Actualizar inventario físico	Gerencia General

Tabla 6: Definición de roles (Peñafiel, 2019)

4.5. Planificación

Para realizar una evaluación a los riegos y su tratamiento primero se deben identificar los activos de información que tiene la empresa de tecnología.

4.5.1. Acciones para abordar riesgos y oportunidades

4.5.1.1. Identificación de Activos

El activo que ya se encuentra en el ambiente Cloud Computing de la empresa de tecnológica es de tipo Información y Datos.

ACTIVO			
DESCRIPCIÓN	**TIPO**	**PROPIETARIO**	**PROCESO**
Aplicación	Datos / Información	Personal técnico	GIT
Base de Datos	Datos / Información	Personal técnico	GIT
Manuales de Equipos	Información	Personal técnico	GIT
Datashed	Información	Personal técnico	GIT
Inventarios Físicos	Datos / Información	Personal técnico / Administrativo	GIT
Contratos Clientes	Datos / Información	Personal técnico / Administrativo	GIT

Tabla 7: Identificación de activos en la empresa tecnológica (Peñafiel, 2019)

4.5.1.2. Tasación de Activos

La tasación de activos se realiza de acuerdo a la confidencialidad, integridad y disponibilidad.

ACTIVOS	CRITERIOS DE EVALUACION			TOTAL
	Confidencialidad	Integridad	Disponibilidad	
Aplicación	5	5	5	5
Base de Datos	5	5	5	5
Manuales de Equipos	2	4	5	3,66666667
Datashed	1	4	5	3,33333333
Inventarios Físicos	5	5	5	5
Contratos Clientes	5	5	5	5

Tabla 8: tasación de activos en la empresa tecnológica (Peñafiel, 2019)

4.5.1.3. Evaluación de Riesgos de seguridad de la información

La evaluación de los riesgos se levantará de acuerdo a la siguiente tabla

RIESGO	EVALUACIÓN				GRUPO
	NIVEL DE PROBABILIDAD	GRADO DE IMPACTO	ACTIVO AFECTADO	NIVEL DE RIESGO	

Tabla 9: formato para la evaluación de riesgos (Peñafiel, 2019)

Donde:

Nivel de probabilidad:

- Bajo: la probabilidad que el riesgo suceda es bajo
- Medio. La probabilidad que el riesgo suceda es medio
- Alto. La probabilidad que el riesgo suceda es alta.

Grado de impacto

- Bajo: si el riesgo sucede el grado de impacto es bajo
- Medio. si el riesgo sucede el grado de impacto es medio
- Alto. si el riesgo sucede el grado de impacto es alto

Nivel de riesgo:

- Bajo: el nivel de riesgo es bajo
- Medio. el nivel de riesgo es medio
- Alto. el nivel de riesgo alto

Grupo

Hacer referencia a la agrupación de riesgos descrita en el capítulo 3.

4.5.1.4. Tratamiento de riesgos de seguridad de la información

Para el tratamiento de riesgos se aplicará la siguiente tabla.

RIESGO		CRITERIOS DE EVALUACION		RESULTADO	
		Impacto Económico	Tiempo de Recuperación	Total	Opción de Tratamiento
ACTIVO	AMENAZA	40%	60%	100%	

Tabla 10: Formato para el tratamiento de riesgos (Peñafiel, 2019)

El impacto económico se evalúa como un máximo de 40% sobre 100% y el tiempo de recuperación con un máximo de 60% sobre 100%.

Estos valores se toman en referencia a que la perdida de la información no representa un valor económico alto en comparación al tiempo que toma en obtener la información.

La opción de tratamiento que se aplicara es: tratar, no tratar, aceptar

4.5.2. Objetivos de seguridad de la información y planes para alcanzarlos

Los objetivos definidos por la empresa de tecnología para la seguridad de la información son:

- Actualizar la información de del inventario físico cada vez que se adquiera o se realicen importaciones de repuestos y equipos.
- Realizar la baja del inventario físico de un repuesto o equipo sea por facturación o garantía.
- Realizar el ingreso en línea del informe técnico.

Para verificar que los objetivos planteados se cumplan y con el fin de asegurar la información se realizaran auditorías internas a nivel contable y físico.

4.6. Apoyo

Con el fin de que el proceso de Gestión de Informes Técnicos implementado en el ambiente Cloud Computing se cumpla sin ninguna novedad, la empresa de tecnología proveerá de los recursos necesarios al personal involucrado en el proceso.

4.6.1. Recursos

Al cada personal del área técnica involucrada en el proceso de Gestión de Informes Técnicos se asignará un dispositivo móvil que permita la conexión a internet, así mismo de un plan de datos para que pueda ingresar el informe técnico una vez finalizado el mantenimiento.

4.6.2. Competencia

El área de recursos humanos será la encargada de entregar los dispositivos al personal, del mismo modo se encargará de receptar el dispositivo cuando este sea reportado como dañado o el personal se desvincule de la empresa de tecnología.

4.6.3. Conciencia

Con el fin de que el sistema de Gestión de la Seguridad de la Información sea efectivo, se difundirá al personal las ventajas y beneficios de contar con el sistema de Gestión de Informes Técnicos en un ambiente Cloud Computing.

4.6.4. Comunicación

En la empresa de tecnología, la Gerencia General conjuntamente con el área de soporte técnico comunicara la importancia o problemas de mantener los procesos en el ambiente Cloud Computing, sea por correos electrónicos o reuniones generales.

4.7. Funcionamiento

4.7.1. Planificación y control operacional

Para que la Gestión de Seguridad de la Información en un ambiente Cloud Computing se efectiva, la empresa de tecnología ha implementado los siguientes controles.

- Registro de acceso validando usuario, clave y dispositivo
- Registro de fecha y hora de llegada y salida a sitio, hora de inicio y fin del mantenimiento.

4.7.2. Evaluación de riesgos de seguridad de la información

La evaluación de riesgos se realiza en base a los riesgos identificados en el ambiente Cloud Computing descritos en el capítulo 3

RIESGO	EVALUACIÓN				GRUPO
	NIVEL DE PROBABILIDAD	GRADO DE IMPACTO	ACTIVO AFECTADO	NIVEL DE RIESGO	
Pérdida de Gobernanza	alta	medio	Aplicación	bajo	Riesgo Técnico
			Base de Datos	bajo	Riesgo Técnico
Riesgo de cumplimiento Normativo	bajo	medio	Aplicación	bajo	Riesgo Técnico
Protección de datos	bajo	medio	Base de Datos	bajo	Riesgo Técnico
Vinculación	bajo	medio	Aplicación	medio	Riesgo Técnico
			Base de Datos	medio	Riesgo Técnico
Supresión de datos incompleta	bajo	alto	Base de Datos	bajo	Riesgo Técnico
Fallo de aislamiento	bajo	alto	Base de Datos	bajo	Riesgo Técnico
Miembro malicioso	bajo	medio	Base de Datos	medio	Riesgo Técnico
	bajo	alto	Inventarios físicos	bajo	Riesgo Técnico
Comprometimiento de la interfaz	bajo	medio	Aplicación	bajo	Riesgo Técnico

Tabla 11: Evaluación de riesgos (Peñafiel, 2019)

4.7.3. Tratamiento de riesgos de seguridad de la Información

RIESGO		CRITERIOS DE EVALUACION		RESULTADO	
		Impacto Económico	Tiempo de Recuperación	Total	Opción de Tratamiento
ACTIVO	AMENAZA	40%	60%	100%	
Aplicación	Acceso no autorizado	4	4	4	Transferido
Aplicación	Disponibilidad	3	2	2,4	Transferido
Base de Datos	Divulgación de la Información	3	4	3,6	Mitigado
Base de Datos	Modificación de la Información	1	3	2,2	Mitigado
Base de Datos	Ingreso de Información Falsa	3	5	4,2	Transferido
Base de Datos	Disponibilidad	4	4	4	Mitigado
Manuales de Equipos	Disponibilidad	2	2	2	Aceptar
Datasheet	Disponibilidad	2	2	2	Aceptar
Inventarios Físicos	Divulgación de la Información	3	5	4,2	Mitigado
Inventarios Físicos	Acceso no autorizado	2	2	2	Aceptar
Inventarios Físicos	Modificación de la Información	2	2	2	Aceptar
Contratos Clientes	Acceso no autorizado	1	2	1,6	Aceptar
Contratos Clientes	Eliminación de la Información	3	2	1,8	Aceptar
Contratos Clientes	Escapes de Información	1	1	1	Aceptar

Tabla 12: Tratamiento de riesgos (Peñafiel, 2019)

ACTIVO	AMENAZA	TOTAL	ACCION
Aplicación	Acceso no autorizado	55%	TRATAR
Aplicación	Disponibilidad	29%	TRATAR
Base de Datos	Divulgación de la Información	35%	TRATAR
Base de Datos	Modificación de la Información	34%	TRATAR
Base de Datos	Ingreso de Información Falsa	48%	TRATAR
Base de Datos	Disponibilidad	43%	TRATAR

Manuales de Equipos	Disponibilidad	60%	TRATAR
Datasheet	Disponibilidad	60%	TRATAR
Inventarios Físicos	Divulgación de la Información	52%	TRATAR
Inventarios Físicos	Acceso no autorizado	40%	TRATAR
Inventarios Físicos	Modificación de la Información	40%	TRATAR
Contratos Clientes	Acceso no autorizado	22%	TRATAR
Contratos Clientes	Eliminación de la Información	22%	TRATAR
Contratos Clientes	Escapes de Información	29%	TRATAR

Tabla 13: Evaluación de amenazas (Peñafiel, 2019)

5. CAPÍTULO IV: CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- Cada vez más organizaciones públicas o privadas optan por los servicios que ofrece la tecnología Cloud Computing, sin embargo, para que los recursos sean aprovechados de forma eficiente, se debe realizar una capacitación y una concientización a los usuarios involucrados sobre los beneficios y riesgos que ofrece dicha tecnología.

- Todos los procesos para implementar la seguridad en un ambiente Cloud Computing se deben realizar conjuntamente entre el proveedor del servicio en la nube y el cliente, ya que de esta manera se pueden establecer responsabilidades.

- La seguridad y la integridad de los datos es una preocupación latente para las organizaciones que desea migrar de un ambiente tradicional a un ambiente Cloud Computing, así también la pérdida de control o la disponibilidad de la información, ya que esta última afecta directamente a la ejecución de las operaciones propias de las organizaciones.

- En un ambiente tradicional o en un ambiente Cloud Computing se deben definir claramente los procesos y responsables siempre orientándose a la confidencialidad, Integridad, y disponibilidad de la información.

- Tomar medidas preventivas ayudara a las organizaciones a proteger el activo más importante que posee y que es la información, ya que la pérdida o la fuga de la misma puede ocasionar la paralización de una o varias operaciones de la empresa, causando pérdidas económicas significativas.

- La ISO 27001 brinda al proveedor la opción de controlar los recursos sin dejar que la información se encuentre comprometida como resultado el aplicar la norma ISO 27001:2013 en ese aspecto es muy factible.

5.2. Recomendaciones

- Las organizaciones no deberían escatimar en gastos al momento de proteger la información, especialmente cuando por disminuir gastos confían cierto tipo de información a personas que no se encuentran capacitadas.

- No se debe minimizar ningún proceso, pues todos son importantes y ayudan para que las operaciones dentro de una organización no se detengan, por lo que se debe documentar y difundir entre el personal involucrado.

- La asignación de un único usuario privilegiado para un proceso es muy riesgosa pues en ausencia del mismo se puede detener la ejecución de algunos procesos.

- Realizar auditorías internas sin prevenir a los responsables de los procesos, permite verificar si los procesos se ejecutan de la forma defina correcta.

- Con la finalidad que tenga un mayor control de la seguridad dentro de una empresa se recomienda la norma ISO 27001 Anexo A, al igual que la nueva norma ISO 27017 las cuales permiten una mejor resolución de la protección de la información y todos los requisitos de seguridad que implica.

BIBLIOGRAFIA

(ISO/IEC 27000: 2014 - 3.2.1. (2014). *Online Browsing Platform (OBP).* Obtenido de https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en

©ISO/IEC 2012- All rights reserved. (2013). *Information technology — Security techniques — Information.*

Advisera. (2019). *¿Qué es norma ISO 27001?* Obtenido de https://advisera.com/27001academy/es/que-es-iso-27001/

Albert de la Cruz, M. (03 de 06 de 2010). *Privacidad y seguridad Informática*. Obtenido de https://es.slideshare.net/alu4albertde/privacidad-y-seguridad-informtica

Cierco, D. (2011). *Cloud Computing.* Madrid: Fundación ideas.es.

COMUNICACION ONLINE. (03 de 02 de 2016). *¿Qué es un software como servicio (SAAS)?* Obtenido de http://www.naiarafernandez.com/que-es-un-software-como-servicio-saas/

Digimarketing Copyrigth©. (2016). *Seguridad Informática*. Obtenido de https://www.nedetel.net/seguridad-informatica/

EVALUANDO CLOUD.COM. (14 de 10 de 2015). *7 beneficios y 9 riesgos de Cloud Computing*. Obtenido de https://evaluandocloud.com/7-beneficios-y-9-riesgos-del-cloud-computing/

GADAE NETWEB. (17 de 08 de 2019). *5 Riesgos de seguridad informática en tu empresa que podrías evitar*. Obtenido de http://www.gadae.com/blog/riesgos-de-seguridad-informatica/

García , A., & Alegre, M. (2011). *Seguridad Informática.* Madrid: Paraninfo.

García, F., & Albarran, S. (2015). *Guía para Implantar un Sistema de Gestión de Seguridad de Información: Basada en la Norma ISO/IEC 27001.* (EAE, Ed.)

Gonzáles Hernández, L. F. (2016). *Aspectos de Seguridad Informática en la Utilización de Cloud Computing.* Cúcuta: Universida Nacional Abierta y a Distancia UNAD.

Herrera Salazar, V. (2016). *Seguridad y protección de la Información en la Nube de Cómputo.* Revista Académica EAC. Loja - Ecuador: Latindex. Obtenido de https://revistas.unl.edu.ec/index.php/eac/issue/view/34

INCIBE Instituto Nacional de Cyberseguridad. (17 de 08 de 2019). *PROTECCIÓN DE LA INFORMACIÓN.* Obtenido de https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

IONOS España. (24 de 06 de 2019). *IaaS: Infraestructura escalable en la nube*. Obtenido de https://www.ionos.es/digitalguide/servidores/know-how/que-es-iaas/

IONOS España. (21 de 06 de 2019). *PaaS: plataforma como servicio*. Obtenido de https://www.ionos.es/digitalguide/servidores/know-how/paas/

ISO 27000.ES. (20 de 07 de 2006). *Prodcast: Historia de ISO 270001 e ISO 17799.* Obtenido de http://www.iso27000.es/articulos.html

ISO TOOLS. (17 de 08 de 2019). *La norma ISO 27001 Aspectos clave de su diseño e implantación*. Obtenido de https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

ISOTools. (24 de 07 de 2017). *¿Cuál es la estructura de la nueva norma ISO 27001 2013?* Obtenido de https://www.isotools.com.mx/la-estructura-la-nueva-norma-iso-27001-2013/

Mayevsky, M. (2013). *Economía de las Nubes.* Alemania: National Library.

Peñafiel, C. (2019). *Diseño de un modelo para establecer un sistema de gestión de la seguridad de la información dentro de un ambiente Cloud Computing, aplicando la Norma ISO 27001:2013.* Quito: PUCE.

Ramos, B., & Ribagorda, A. (2004). *Seguridad de la Información.* Madrid: Diazdesantos.

Red Hat . (2019). *¿Que es multicloud?* Obtenido de https://www.redhat.com/es/topics/cloud-computing/what-is-multicloud

Red Hat Enterprise. (17 de 08 de 2019). *Controles de Seguridad*. Obtenido de http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-sgs-ov-controls.html

RedHat. (2019). *El concepto de cloud computing*. Recuperado el 15 de enero de 2019, de https://www.redhat.com/es/topics/cloud

Tendencias & Innovación. (2019). *OBS Business School*. Obtenido de Seguridad de la Información, un conocimiento imprescindible: https://www.obs-edu.com/int/blog-investigacion/sistemas/seguridad-de-la-informacion-un-conocimiento-imprescindible

Torres, J. (2011). *Empresas en la nube.* Barcelona: Cabecera S.L.

WordPress.com. (17 de 08 de 2019). *Computación en la Nube*. Obtenido de https://computacionube.wordpress.com/

ANEXOS

ANEXOS 1: CATALOGO DE AMENAZAS EN UN AMBIENTE CLOUD COMPUTING

Errores y Fallo no intencionados: estos errores son causados por usuarios sin el afán de dañar a la organización.

Errores de usuarios	
Tipos de activos:	**Dimensiones**
Servicios Datos Aplicaciones	Integridad Disponibilidad
Descripción: errores que comenten los usuarios sin tener la intención de causar daños al momento de usar datos o aplicaciones	

Errores de Administrador	
Tipos de activos:	**Dimensiones**
Servicios Datos Software Hardware Rede de comunicación	Disponibilidad Integridad Confidencialidad Autenticidad del Servicio Autenticidad de los datos Trazabilidad de los servicios Trazabilidad de los datos
Descripción: errores de usuarios responsables de instalaciones y operaciones.	

Errores de Configuración	
Tipos de activos:	**Dimensiones**
Servicios Datos Software Hardware Rede de comunicación	Disponibilidad Integridad Confidencialidad Autenticidad del Servicio Autenticidad de los datos Trazabilidad de los servicios Trazabilidad de los datos
Descripción: datos mal configurados, los activos dependen exclusivamente de la configuración como: privilegios de acceso, registros de actividades, etc.	

Difusión de Software dañino	
Tipos de activos:	**Dimensiones**
Software	Disponibilidad Integridad Confidencialidad Autenticidad del Servicio Autenticidad de los datos Trazabilidad de los servicios Trazabilidad de los datos
Descripción: propagación de programas maliciosos, virus, spyware.	

Escapes de información	
Tipos de activos:	**Dimensiones**
Datos / información Software Redes de comunicación	Confidencialidad
Descripción: la información se propaga accidentalmente a personas que no deben tener acceso, la información no se ve alterada.	

Modificación de la Información	
Tipos de activos:	**Dimensiones**
Datos / información	Integridad
Descripción: aplica a datos generales, se altera accidentalmente la información.	

Introducción de Información Incorrecta	
Tipos de activos:	**Dimensiones**
Datos / información	Integridad
Descripción: aplica a datos generales, se ingresa accidentalmente la información.	

Degradación de la Información	
Tipos de activos:	**Dimensiones**
Datos / información	Integridad
Descripción: aplica a datos generales, se degrada o modifica accidentalmente la información.	

Destrucción de la Información	
Tipos de activos:	**Dimensiones**
Datos / información	Disponibilidad
Descripción: aplica a datos generales, pérdida accidentalmente la información.	

Divulgación de la Información	
Tipos de activos:	**Dimensiones**
Datos / información	Confidencialidad
Descripción: revelación de la información sea por indiscreción, medios electrónicos o soporte en papel.	

Vulnerabilidad de software	
Tipos de activos:	**Dimensiones**
Aplicaciones / software	Integridad Disponibilidad Confidencialidad
Descripción: errores de código que originan una operación defectuosa, pero que pesan sobre la integridad o disponibilidad de los datos.	

Ataques Intencionados: errores cometidos por los usuarios con el afán de dañar a la organización.

Suplantación de Identidad	
Tipos de activos:	**Dimensiones**
Servicios Datos / Información Aplicaciones Software Redes de comunicación	Confidencialidad Integridad Autenticidad de los datos Autenticidad del Servicio
Descripción: se puede realizar por personal interno o personas ajenas a la organización.	

Abuso de privilegios asignados	
Tipos de activos:	**Dimensiones**
Servicios Hardware Aplicaciones Software Redes de comunicación	Confidencialidad Integridad
Descripción: se asignan los privilegios con el fin de cumplir una determinada función, pero se realiza actividades que no son de competencia	

Uso no previsto	
Tipos de activos:	**Dimensiones**
Servicios Soportes de información Aplicaciones Software hardware Redes de comunicación Equipamiento Auxiliar Instalaciones	Disponibilidad
Descripción: utilización de activos con beneficios personales.	

Alteración de secuencia	
Tipos de activos:	**Dimensiones**
Servicios Redes de comunicación Aplicaciones Software	Integridad
Descripción: Alteración del orden en la transmisión de mensajes	

Acceso no autorizado	
Tipos de activos:	**Dimensiones**
Servicios Soportes de información Aplicaciones Software hardware Redes de comunicación Equipamiento Auxiliar Datos / Información Instalaciones	Confidencialidad Integridad Autenticidad del Servicio
Descripción: acceso a los recursos del sistema sin autorización, se aprovechan fallas del sistema.	

Intercepción de Información	
Tipos de activos:	**Dimensiones**
Datos Redes de comunicación Aplicaciones Software Hardware	Confidencialidad
Descripción: accede a la información que no le corresponde, sin que la información se ve alterada.	
Modificación de la información	
Tipos de activos:	**Dimensiones**
Datos / Información	Integridad
Descripción: alteración de información falsa con el fin de causar daño u obtener algún beneficio.	

Ingreso de Información Falsa	
Tipos de activos:	**Dimensiones**
Datos / Información	Integridad
Descripción: ingreso de información falsa con el fin de causar daño u obtener algún beneficio.	

Corrupción de Información	
Tipos de activos:	**Dimensiones**
Datos / Información	Integridad
Descripción: degradación de información intencional con el fin de causar daño u obtener algún beneficio.	

Destrucción de Información	
Tipos de activos:	**Dimensiones**
Datos / Información	Disponibilidad
Descripción: eliminación de información intencional con el fin de causar daño u obtener algún beneficio.	

Ataque Destructivo	
Tipos de activos:	**Dimensiones**
Soportes de Información Redes de comunicación Equipamiento Auxiliar	Disponibilidad
Descripción: vandalismo, terrorismo; puede ser realizada por el personal interno o personas ajenas a la organización.	

ANEXO 2. REGISTROS DESARROLLADOS

MATRIZ PARA LA IDENTIFICACIÓN DE ACTIVOS

ACTIVO			
DESCRIPCIÓN	**TIPO**	**PROPIETARIO**	**PROCESO**

MATRIZ PARA LA TASACIÓN DE ACTIVOS

ACTIVOS	**CRITERIOS DE EVALUACION**			**TOTAL**
	Confidencialidad	**Integridad**	**Disponibilidad**	

RESULTADOS EVALUACIÓN AMENAZA – VULNERABILIDAD

RIESGOS A TRATAR

ACTIVO	AMENAZA	TOTAL	ACCION

MATRIZ DE EVALUACIÓN DE SIGNIFICANCIA DEL RIESGO

RIESGO		CRITERIOS DE EVALUACION		RESULTADO	
		Impacto Económico	Tiempo de Recuperación	Total	Opción de Tratamiento
ACTIVO	AMENAZA	40%	60%	100%	

MATRIZ DE ROLES Y RESPONSABILIDADES

RESPONSABILIDAD / FUNCION	AREAS	
	GERENCIA TECNICA	TECNICO

ANEXO 3: DOCUMENTOS APLICABLES EN UN AMBIENTE CLOUD COMPUTING

Aunque la norma ISO 27001:2013 agrupa a los documentos en obligatorios y no obligatorios, en un ambiente Cloud Computing algunos de los documentos agrupados en no obligatorios deben considerarse como obligatorio por lo que a continuación, se describe el contenido de los documentos obligatorios que deben aplicarse en el ambiente Cloud Computing.

Alcance del SGSI

Es un documento corto que se redacta cuando se inicia la implementación de la norma ISO27001:2013 y se puede unificar con la política de seguridad de la información.

Políticas y objetivos de la seguridad de la información

Es un documento breve de alto nivel y detalla el principal objetivo de un SGSI. Se detalla como un documento independiente, pero al igual que el alcance del SGSI puede ser unificado con la política de seguridad de la información.

Metodología e informes de evaluación y tratamiento de riesgos

Es un documento de máximo 5 páginas, se redacta antes de la realización de evaluación y tratamiento de riesgos.

Declaración de aplicabilidad

Este documento se redacta basándose en los resultados del tratamiento de riesgos, describe controles, la manera en la que se implementarán y el estado actual de los mismos. En resumen, muestra un perfil de la seguridad de la organización.

Plan de tratamiento de riesgos

Es un plan de acción, y muestra la forma de implementar los controles definidos en la Declaración de Aplicabilidad, este documento debe usarse y actualizarse continuamente en el transcurso de la implementación del SGSI.

Funciones y responsabilidades de seguridad

La descripción de funciones y responsabilidades deben ser claras y precisas para los usuarios que pertenecen a la organización mientras que para terceros estas funciones y responsabilidades deben definirse mediante contratos.

Inventario de activos

Se puede realizar en base del resultado de evaluación de riesgos, pues en este punto se debe identificar tanto activos como propietarios.

Política de control de acceso

Se define después de la evaluación y tratamiento de riesgos, se describe el acceso a determinada información y sistemas incluyendo el aspecto técnico de control de acceso, se definen reglas para el acceso lógico.

Procedimientos operativos para la gestión de ti

Son procedimientos aplicables para la gestión de cambios, servicios a terceros, seguridad de red, códigos maliciosos, copias de seguridad, transferencia de información, eliminación y destrucción.

Principios de ingeniería para sistemas seguros

Es un control de ISO 57001:2013, se definen las técnicas de seguridad en toda la arquitectura: negocio, datos, aplicaciones y tecnología, en si los principios de ingeniería de seguridad, estos principios incluyen validación de datos, controles de sesión, técnicas para la autenticación.

Política de seguridad para proveedores

Es un control de ISO 57001-2013, abarca la evaluación de riesgos de un proveedor, cláusulas que se deben incluir en los contratos, supervisión de cumplimiento de las cláusulas establecidas, modificación de contrato, cierre del acceso en el caso de cancelar un contrato.

Procedimiento para la gestión de incidentes

Explica la gestión para las debilidades, incidentes o eventos de seguridad. Se puede decir que permite aprender de los incidentes de seguridad de la información para evitarlos en el futuro.

Política de claves

Indica la forma en la que se deben generar las claves para los usuarios, Las claves deben ser complejas, sin palabras comunes y obligatoriamente se debe cambiar al primer inicio de sesión.

Política de eliminación y destrucción

Aplicar técnicas para la eliminación segura de la información, a través de herramientas o procesos que ayuden a eliminar toda la información que se encuentre en un dispositivo.

Política de creación de copias de seguridad

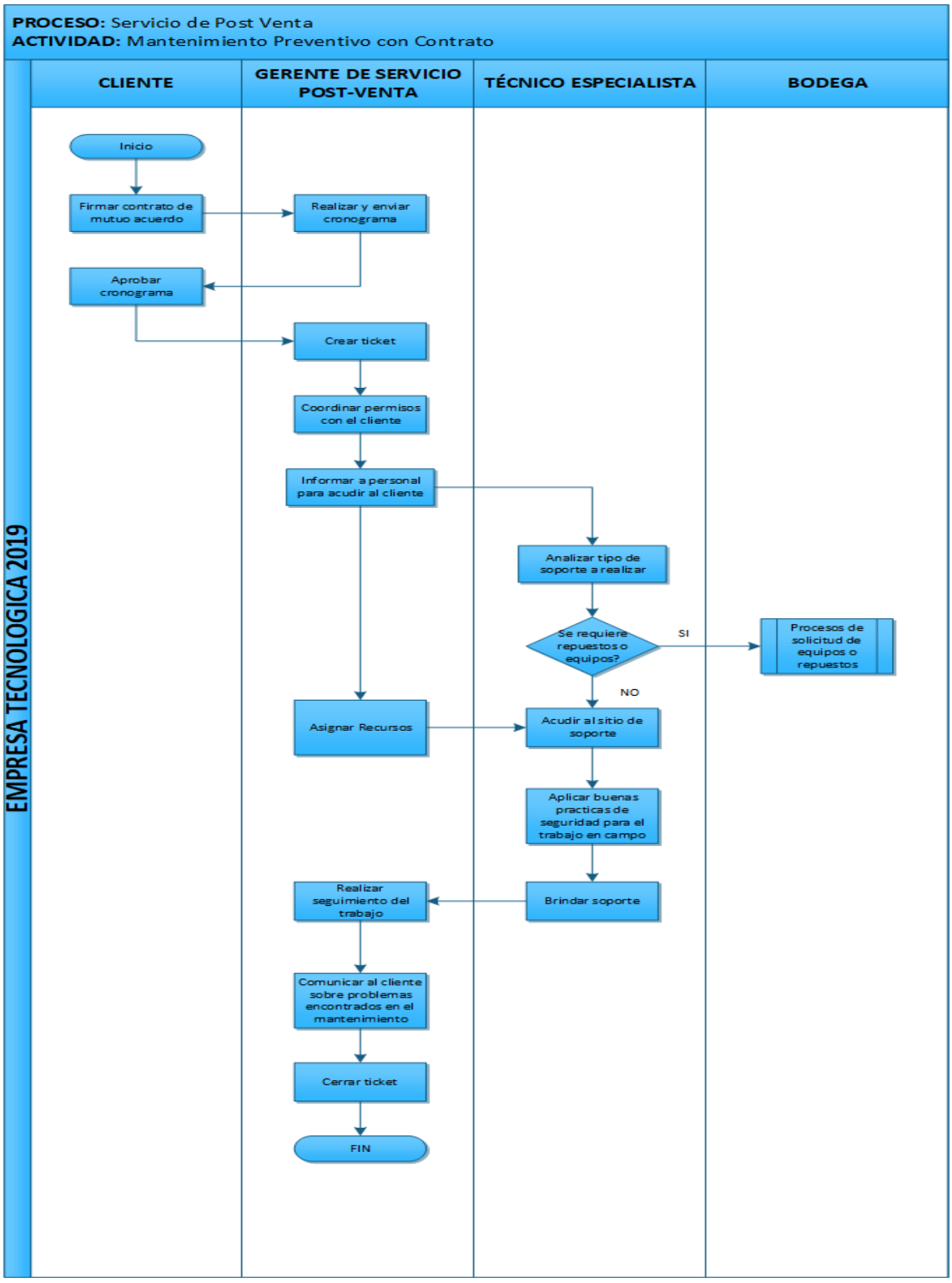
Permite proteger a la organización contra la perdida de datos, mediante la creación de copias de seguridad y almacenamiento de la información crítica, para esto se deben facilitar los recursos necesarios y establecer mecanismos para realizar dichas actividades.

ANEXO 4: PROCESOS QUE SE REALIZAN EN LA EMPRESA TECNOLÓGICA

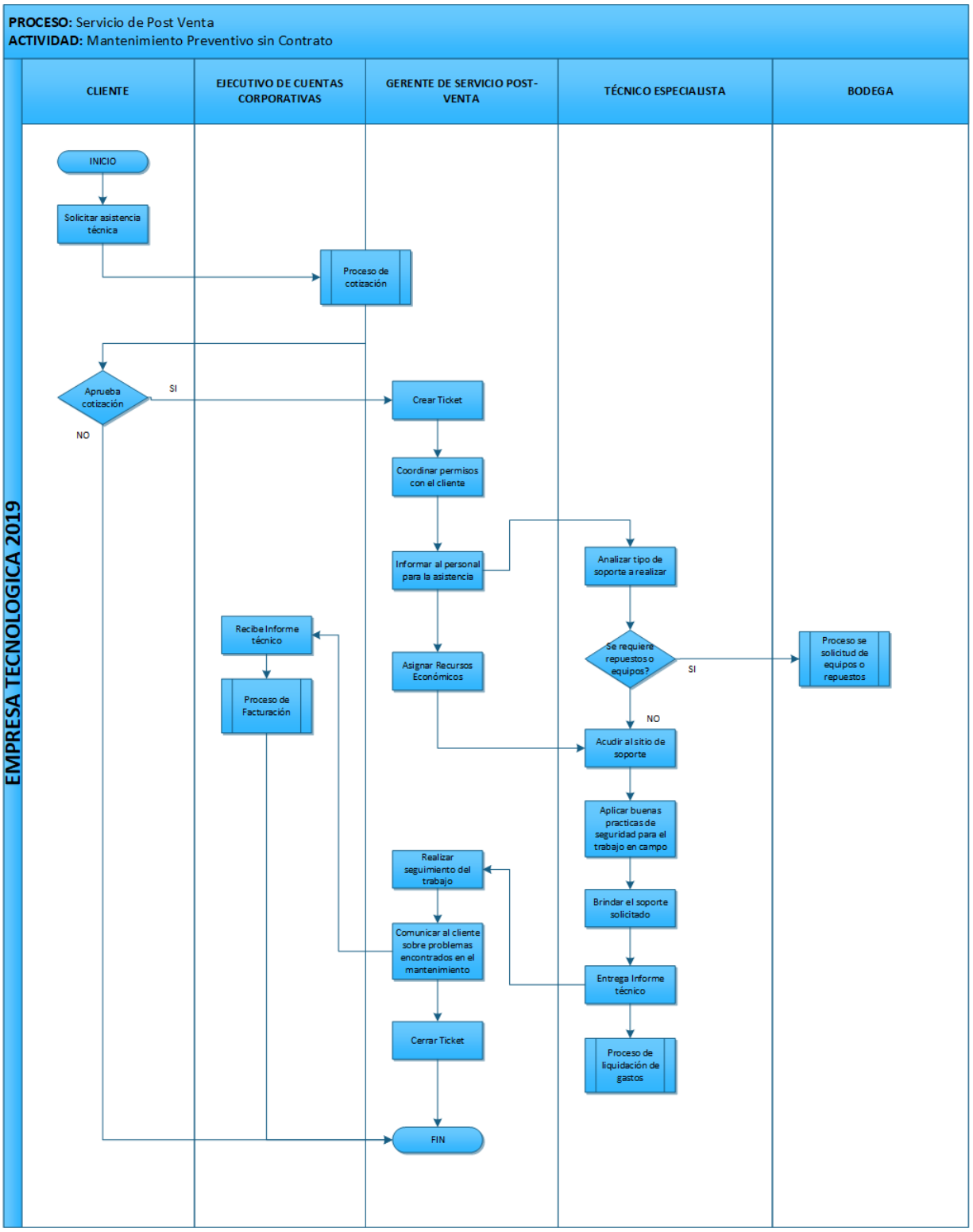
Entre los Procesos que se realizan en la empresa Tecnológica se encuentran

- Mantenimiento Preventivo con Contrato
- Mantenimiento Preventivo sin Contrato
- Mantenimiento Correctivo con Contrato
- Mantenimiento Correctivo sin Contrato

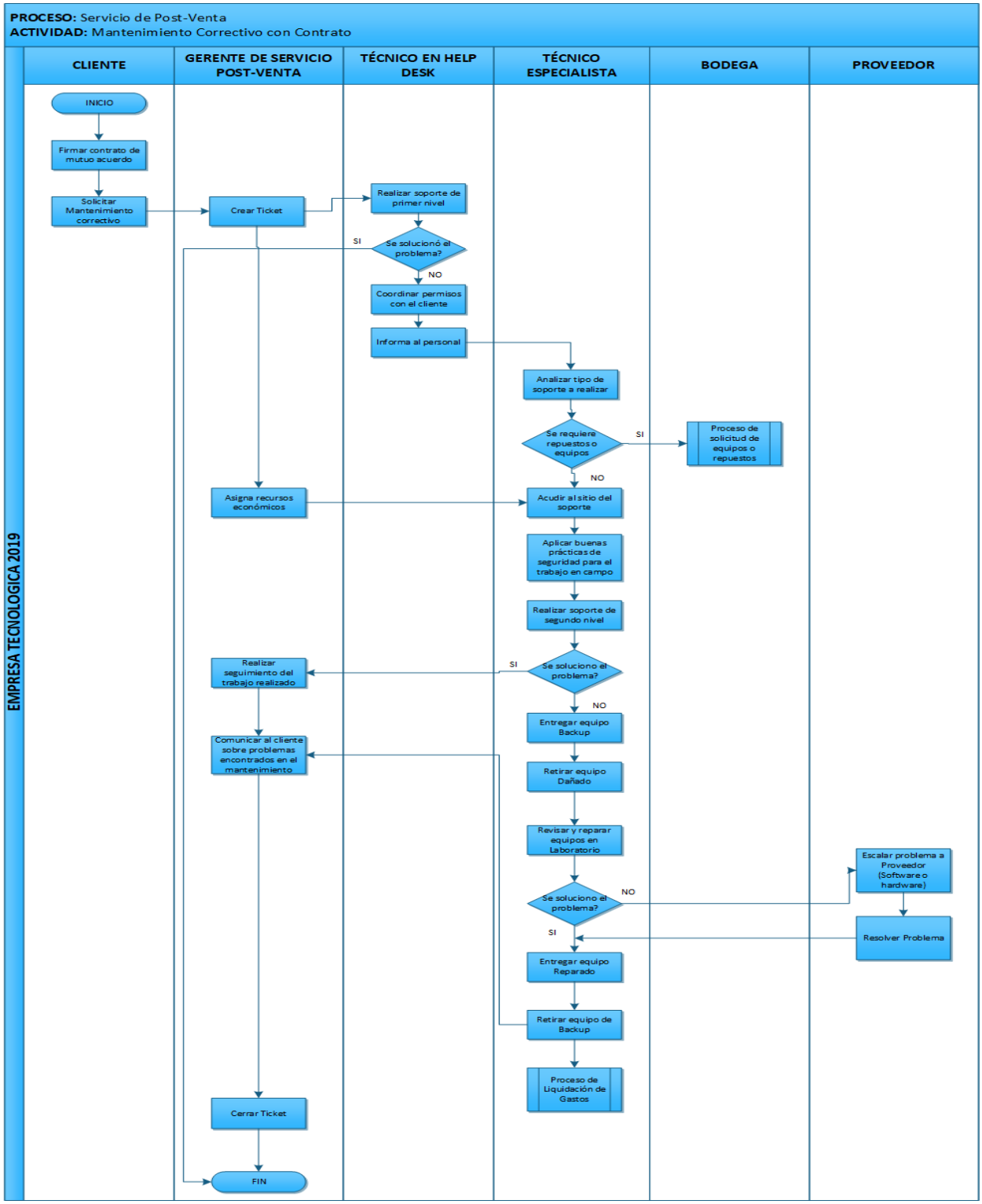
Mantenimiento Preventivo con Contrato



Mantenimiento Preventivo Sin Contrato



Mantenimiento Correctivo Con Contrato



Mantenimiento Correctivo sin Contrato

