**UNIVERSIDAD TECNICA DE BABAHOYO**

***FACULTAD DE ADMINISTRACIÓN FINANZAS E INFORMÁTICA***

***CARRERA DE SISTEMAS DE INFORMACIÓN***

**PROCESO DE TITULACION**

**DICIEMBRE 2021 – ABRIL 2022**

**EXAMEN COMPLEXIVO DE GRADO A FIN DE CARRERA PRUEBA PRÁCTICA**

**PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS DE INFORMACIÓN**

**TEMA:**

# ANALISIS Y DISEÑO DE UN MODELO PARA ESTABLECER UN SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION DENTRO DE UN AMBIENTE CLOUD COMPUTING, APLICANDO LA NORMA ISO 27001. EN LA EMPRESA DATA-FIBER

**ESTUDIANTE:**

Ronald Joel Mora Guaman

**TUTOR:**

Ing. Fabián Eduardo Alcoser Cantuña

**AÑO 2022**

# TABLA DE CONTENIDO

## JUSTIFICACIÓN

Se justifica el desarrollo de este proyecto ya que siempre se ha observado que compañías proveedores han sentido una incesante inquietud sobre la seguridad para la conversión a la nube, es decir que los datos que se transfieren al portal virtual sean confiables. De esta manera se ha pensado en la implementación de Sistema que posibiliten gestionar la seguridad de todos los datos con ello se brindaría la total confiabilidad y seguridad en la manipulación de los datos de clientes o usuarios.

Nuestro proyecto para la empresa DATA-FIBER plantea un modelo de gestión de seguridad de los datos procesados en la nube, mediante el cual se obtenga mayores posibilidades de protección y seguridad contra todo tipo de adversidades o vulnerabilidades que generalmente pudiesen presentarse durante la transferencia de datos o ya en ambiente de Cloud Computing que monitorea sus debilidades y riesgos que pueden darse en momentos determinados.

Es importante que, en el desarrollo de esta temática, los proveedores aborden temas de interés para capacitar a los usuarios en determinados aspectos, lo cual facilitaría el manejo de este ambiente en la nube, planteando de forma concreta un análisis minucioso y una evaluación globalizada, tomando como referencia principal la aplicación de la norma ISO 27001 relacionada con Seguridad de la Información, y que se refiere a nuestro tema de estudio.

## Línea de Investigación

El presente trabajo surge como un apoyo del proyecto de investigación denominado "Análisis 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" que se encuentra inscrito a la línea de investigación "Software inteligente y convergencia tecnológica" que se aplicará en la empresa DATA-FIBER.

## OBJETIVOS

### OBJETIVO PRINCIPAL

Diseñar un modelo para establecer un sistema de gestión de la seguridad de la información utilizando para ello como base fundamental la Norma ISO 270001 y creado bajo un ambiente “Cloud Computing” que permitirá a los clientes de la empresa DATA-FIBER facilidad y seguridad en el acceso a sus datos.

### 1.3.2. OBJETIVOS ESPECÍFICOS

- Valorar el contexto actual referente a la Seguridad de los datos, con ello determinar los puntos más bajos de fragilidad de la empresa DATA-FIBER que visualiza nuestra temática.

- Evaluar e identificar cuantificaciones (medidas) que actúen como fundamento para el proceso de valoración de seguridad de “Cloud Computing” hacia los clientes.

- Especificar las técnicas y demás componentes para establecer las razones a valorar en componentes de usabilidad de los datos, bajo la premisa de la Norma ISO 270001.

- Elaborar una propuesta de un sistema de gestión de la seguridad de la información dentro de un ambiente Cloud Computing que de facilidad y accesibilidad simple a los clientes.

**Planteamiento del Problema**.

Es importante, diseñar un modelo para establecer un sistema de gestión de seguridad de la información dentro de un ambiente Cloud Computing, basada en reglas instauradas, lo cual es de suma importancia en una compañía, con lo cual se gana seguridad y confiabilidad en sus datos. Por ello surgen a nivel internacional políticas normalizadas que en el transcurso podrían adaptarse para la manipulación de grandiosas y pequeñas cantidades de datos, las cuales son significativas para que una determinada compañía lleve a cabo sus actividades y transacciones diarias.

Tomando como ejemplo Europa, luego de tener problemas de hurto de datos a empresas como Yahoo, Uber, Sony entre otras, esto provocado por administraciones inadecuadas que, por muchos años, nunca se han actualizado y por supuesto esto trae como consecuencia la fuga de o manejo total de la información de los clientes. No contar con un modelo para establecer un sistema de gestión de seguridad, en un ambiente Cloud Computing; los países europeos y demás, estudian la reglamentación de normas y leyes que resguarden y principalmente sobrelleven castigos a quienes estén involucrados en operaciones ilegales en contra de compañías a nivel internacional y nacional de cualquier país.

En los sufragios electorales del año 2019 en Ecuador, en CNE (Consejo Nacional Electoral), encontró algunos sitios críticos de control de información durante el proceso de transferencia de datos equivalente a resultados de actas de escrutinios, este problema surgió ya que no se aplicó ningún modelo para establecer un sistema de gestión de seguridad informático, que certifique y asegure a los electores gozar de una transparente seguridad de datos procesados, así como considerar todas las etapas de los comicios electorales.

Este organismo, así como otros siempre deben contar con diseño de un modelo de gestión y seguridad de datos, esto con el fin de resguardar los datos y puntos críticos posibles.

En conclusión, el problema que radica en las compañías es la falta de reglamentaciones que estén fundamentadas en el estricto control de las reglas normalizadas a nivel internacional que protejan y den seguridad a los datos que son trasferidos o almacenados en la nube, esto

provoca desconfianza de las personas, ya que no se garantiza la confiabilidad, disposición y seguridad de la información que generalmente es dueña la compañía o empresa.

## MARCO CONCEPTUAL

### Conceptos de seguridad de la información

La información actualmente es el elemento más trascendental de cualquier compañía, se visualiza que en los estados, entidades bancarias, entre otras sociedades públicas y privadas efectúan incalculables esfuerzos para la sistematización de sus procesos manuales llevados a cabo dentro de la empresa, el objetivo de esto es adquirir una eficacia y rentabilidad más alta, lo cual conlleva a obtener una solicitud para generar un gran monto de información que debe ser procesada y mantenida bajo seguridad, lo cual generalmente es privada, que contiene datos de tipo administrativo que se maneja internamente información de sus consumidores, servicios, situación bancaria, información de email etc. (García & Alegre, 2014).

Es habitual que la mayoría de empresas conservan un gran porcentaje de datos, ya sea a través de impresiones de documentos, en un sitio web o correo electrónico, dispositivos de almacenamiento externo, se debe a que cada compañía tiene sus políticas y deben realizar actividades que deben ser analizadas e investigadas a tiempo y de manera profunda.

Además se considera que son un grupo de escritos que pertenecen a la parte administrativa, en la cual se involucra de forma directa a los departamentos de Talento Humano, Administrativo y Financiero de las cuales se generan y se almacenan un gran volumen de documentos y transacciones que son propiamente consignadas para dichos eventos.

Se considera siempre a la información como la parte más importante de mayor validez en la compañía, por lo cual es tan importante el uso que se le pueda dar; por ello estos datos debe ser confiables y confidenciales, que debe estar a cargo del responsable de la información sistematizada, casi siempre son los que se relacionan con procesos administrativos, de la misma forma a como se accede a la plataforma o manipulación de los datos. Se considera uno de los problemas más comunes, cuando se instaura políticas de seguridad incorrectas, es la usurpación de la información confidencial del cliente, con fines de réditos económicos

ya sea en territorio nacional o en el extranjero considerado además para actividades ilícitas o ilegitimas que no son moralmente correctas.

Es tan necesario que se asegure la información y de esta manera resguardarla hacia los posibles eventos y amenazas que podrían acontecer. Esta información puede permanecer en los accesorios o dispositivos de almacenamiento o respaldo, pero muy aparte de esta situación, es obligatorio que las empresas certifiquen que la protección de los datos debe ser primordial, en todas sus etapas: recolección, procedimiento y manipulación del mismo.

Podemos mencionar que la seguridad de la información como meta de primer orden, menciona o es la de proteger la confiabilidad, integridad y disponibilidad de la información; a través de la agregación de un grupo acertado de técnicas, pautas y materiales para la gestión enérgica de acceso a los datos en sus varias vías hacia la seguridad, además implementando elementos y medidas de seguridad que van desde lo lógico a lo físico, esto permitirá detectar y prevenir males o amenazas que poder ser internas o muchas veces externas, las cuales pueden atentar contra la seguridad de la empresa o productividad que pueda generar un negocio ya asentado.

Para toda empresa el término seguridad de la información, es un hecho que paso a paso se debe mejorar, y en la cual toda la compañía debe participar y estar involucrada activamente para que se reduzcan los riesgos de violación de datos. Por lo general hay varias áreas que tienen relación con los famosos sistemas de información dentro del cual está incluida la seguridad informática que es primordial para toda empresa. Estas áreas cubren desde la salvaguardia física de los equipos o hardware, de su ambientación, hasta la misma protección del contenido que se mantiene en la red.

Tenemos varias cualidades que debe cubrir la seguridad de la información que son:

**Critica:** Es indispensable para la manipulación y transacciones de la empresa.

**Valiosa:** Es un activo o bien lógico único e irremplazable de la compañía.

**Sensible**: Generalmente la conocen las personas o miembros que tienen autorización.

Además se considera las palabras riesgo y seguridad claves e importantes:

**Riesgo**: Son debilidades, hechos negativos o amenazas de las transacciones que se pueden producir en un negocio de la compañía.

**Seguridad:** Es la forma de resguardarse contra los anomalías o amenazas, la integridad de los datos es primordial evitando que sufran alteraciones que no son autorizadas, es en sí, uno de los elementos fundamentales de la seguridad de la información, con ello demostrando que es precisa, oportuna y confidencial.

Se considera de gran importancia atesorar la confiabilidad esto significa, impedir que la información transite con clientes, personas comunes o sistemas que no están acreditados bajo las normas de la compañía. Es importante tener medidas de seguridad en los cajeros automáticos, ya que cuando alguien observa por arriba de su hombro, mientras usted coloca o escribe su clave de forma confidencial, también se debe tener cuidado cuando se publica en redes sociales información privada valiosa o en el peor de los casos el hurto de información de un dispositivo móvil o electrónico; estableciéndose estos casos que se mencionaron como desfalco a la confiabilidad de la información personal del cliente.

Por último se debe mencionar que la información siempre debe estar disponible, esto significa que las los usuarios o clientes, procesos o demás aplicaciones consigan tener acceso de forma segura, estable y confidencial.

Este punto de disponibilidad en los sistemas más importantes cumple uno de los propósitos que estar siempre disponible cuando se lo requiera, con ello se evita dificultades en el servicio, anomalías o la actualización del sistema, esto implica que deben estar resguardados y que funcionen de forma correcta a cada instante que lo requieran.

Es importante mencionar en el procedimiento de seguridad de información, el tema variedad es vital ya que pueden existir un sinfín de mecanismos, formas o niveles de servicio que se pueda requerir para su protección, como puede ser: una gran infraestructura de la tecnología, grandes servidores de correo o email, gestores de bases de datos, servidores web, redes de almacenamiento virtual y otros.

Todo esto será posible o depende del nivel de prestación que se podría proporcionar al cliente.

**Plataforma como un servicio (PaaS)**

Cuando hablamos de esta plataforma cuyo modelo concede un ambiente o plataformas que fueron anteriormente diseñadas y alineadas hacia el progreso, expansión, almacenamiento, sostenimiento y aplicaciones que son propias del usuario o cliente, estas se distribuyen a través de la web como medio más apropiado.

Esta interfaz proporciona que las aplicaciones creadas por el cliente nunca se asocien a las complicaciones e inquietudes de su servicio, con esto facilita que todos los recursos y servicios que requiera, serán configurados por el proveedor de manera rápida y precisa.

Esta plataforma (PaaS) incluye las siguientes características:

- ✓ Un entorno de programación amigable
- ✓ Funcionamiento de Sistemas Operativos compatibles
- ✓ Gran ayuda y soporte al cliente de manera permanente
- ✓ Completo almacenamiento de datos
- ✓ Acceso a Hosting permanente
- ✓ Indudable Sistema de administración y Gestión bases de datos

Los ambientes **platforms** as a **service** personifican una coyuntura atractiva en el instante de usar aplicaciones que en su mayoría siempre están conectadas a la web, aunque, existen numerosos usuarios que todavía no han utilizado este medio, ya que no conocen a la perfección, y les genera varias dudas e inquietudes, o en algunas ocasiones no conocen como arrancar con su funcionamiento, mencionamos algunas ventajas de uso del **PaaS** en el usuario:

**Desarrollo de Software**: Usa ambientes individuales para los distintos procesos de desarrollo de la mayoría de sus aplicaciones implementadas.

**Ser ubicuo** para la asistencia de proyectos y capacidad de alojarlos y con ello su progreso asegurado.

**Flexibilidad**: Inspección de los instrumentos o equipo y ajuste a las necesidades determinadas de las mismas y prioritarias.

**Maximizar el tiempo**: Esto es para impedir un tiempo improductivo en la manipulación de los equipos, en otras palabras evitar dificultades que no fueron planeadas.

**Escalabilidad**: Cambiar las particularidades si las condiciones así lo necesitan.

Y como todo tiene su desventaja que, depende del proveedor de **PaaS**, el cliente se puede ver restringido en su módulo de interfaz, lenguaje o ambiente de software logrado.

Esta plataforma (PaaS) está encaminado a abastecer API´s en los espacios que el cliente solicite según sus necesidades a cubrir.

**Software como un servicio (SaaS)**

Este es un modelo de entrega de aplicaciones como servicio, a través del cual el proveedor entrega la utilización bajo petición y luego sencillamente borra dicha instalación de la petición que fue solicitada en todos los dispositivos electrónicos que exista.

El usuario puede acceder a estos beneficios manipulando cualquier navegador de internet, con mucha habilidad no se necesita malgastar demasiados recursos en su ejecución, lo cual ofrece una magnifica optimización de su manejo apropiado.

Cabe recalcar algo importante, la clave en esto es que el usuario o cliente no necesita gestionar la infraestructura inferior, solo aprovecha su uso para cubrir sus necesidades principales.

Podemos mencionar las principales ventajas de este servicio:

- ✓ Es dúctil: Un servicio que se usa bajo demanda de los clientes.
- ✓ Estable: Todos los proveedores tienen su reputación ganada y con protección.
- ✓ Despliegue rápido de todos sus recursos al servicio del usuario.
- ✓ Asequible: Muy fácil solo con una conectividad a internet y listo.
- ✓ Versiones: posibilidad de actualizar siempre.

Encontramos una desventaja muy notable que se refiere a la poca velocidad de las aplicaciones **SaaS**, pero con el avance de las nuevas tecnologías, esta dificultad pasará a segundo plano.

## ¿Qué es Cloud Computing?

Según Benioff (2017), de una manera simple, la computación en la nube (cloud computing) es una tecnología que permite acceso remoto a software, almacenamiento de archivos y procesamiento de datos por medio de Internet, siendo así, una alternativa a la ejecución en una computadora personal o servidor local. En el modelo de nube, no hay necesidad de instalar aplicaciones localmente en computadoras. La computación en la nube ofrece a los individuos y a las empresas la capacidad de un pool de recursos de computación con buen mantenimiento, seguro, de fácil acceso y bajo demanda.

## ¿Cómo funciona el Cloud Computing?

De acuerdo a Einatec (2018), el Cloud Computing es un servicio de tecnología y negocios que permite que el usuario pueda acceder a una amplia variedad de funcionalidades, software y aplicaciones para gestionar sus datos o los de su empresa de forma más eficiente, almacenando su información en servidores remotos en vez de hacerlo en un equipo local. Para hacerlo más sencillo vamos a poner un ejemplo, piensa en un servicio como Gmail. Puedes tener acceso a él desde cualquier dispositivo sin necesidad de descargarlo en tu ordenador, tablet o móvil ni preocuparte por la capacidad de almacenamiento de tu equipo. Todo se procesa, se gestiona, se actualiza y se guarda en la nube a través de Internet.

## Principales características de la computación en la nube

De acuerdo a Sas (2014) las principales características de computación en la nube son:

**1. Autoservicio a demanda**. El consumidor puede acceder y utilizar los servicios en función de sus necesidades.

**2. Amplio acceso de rojo**. Una característica clave de la computación en la nube es que los servicios se encuentran disponibles en una red que puede ser privada, compartida o pública.

**3. Fondo de recursos**. La mayoría de las veces esta característica se refiere a los recursos de hardware, como la capacidad de procesamiento, la conservación de memoria o el almacenamiento.

**4. Elasticidad**. La escalabilidad en los métodos de uso tradicionales exige planificación para los recursos tanto físicos como financieros

**5. Medición de servicios**. El control y la elaboración de informes sobre el uso del servicio, contribuyen al control y optimización de los recursos por parte de los proveedores de servicios en la nube.

**Siete motivos para utilizar la Computación en la Nube**

Según BeServices (2021) existen 7 motivos principales para utilizar de manera eficiente la Computación en la nube (Cloud Computing):

**1. Escalabilidad**. Si durante un período de tiempo concreto un negocio necesita de más recursos en la nube, las soluciones de Cloud Computing están preparadas para asumir este incremento. O si por el crecimiento de la empresa, se requiere más capacidad de forma permanente.

**2. A medida**. Cada empresa puede escoger qué funcionalidades quiere utilizar en un entorno Cloud. Por lo que las soluciones en la nube se adaptan a los requisitos de cada negocio.

**3. Sin restricciones de equipos**. Dado que trabajaremos en un entorno Cloud, muchas de las limitaciones de ordenadores y otros equipos de trabajo desaparecerán. El caso más común es el almacenamiento de archivos: en la nube tendremos acceso a una capacidad ilimitada para almacenar información.

**4. Seguridad**. Tanto nuestros datos como las conexiones que realicemos con las herramientas de Cloud Computing estarán cifradas y bajo altas medidas de seguridad. Además, nuestra información estará protegida ante pérdidas de datos gracias a sistemas de copias de seguridad y restauración.

**5. Movilidad**. Para acceder a los servicios de Cloud Computing que tengamos contratados sólo necesitaremos un equipo con conexión a Internet. Por lo que desde cualquier dispositivo podremos conectarnos a nuestra nube.

**6. Mantenimiento y actualizaciones incluidas**. Todo el conjunto de operaciones vinculadas al mantenimiento de las soluciones de Cloud Computing contratadas, así como su actualización, correrá a cargo de nuestro proveedor.

**7. Conciencia ecológica.** La computación en la nube utiliza sólo el espacio necesario en el servidor, reduciendo la huella de carbono de la empresa.

## ¿Qué es un Sistema de Gestión de Seguridad de la Información?

Un Sistema de gestión de seguridad de la información (SGSI) es, básicamente, un conjunto de políticas de administración de la información. Para entender más a profundidad en qué consiste un SGSI debemos partir de la definición dada por el estándar internacional ISO/IEC 27000:

Un SGSI consiste en el conjunto de políticas, procedimientos y directrices junto a los recursos y actividades asociados que son administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información esenciales.
(Alvarado, 2002)

## ¿Qué es un Activo de Información?

Un Activo de información en el contexto del estándar ISO/IEC 27001 es: “algo que una organización valora y por lo tanto debe proteger”. La protección de estos activos está destinada a preservar la confidencialidad, la integridad y la disponibilidad de la información. Además, puede abarcar otras propiedades como la autenticidad, la responsabilidad y la fiabilidad.

A continuación, discutiremos de qué representan término relacionada con la información:

**Confidencialidad**: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. Es necesario acceder a la información mediante autorización y control.

**Integridad:** debe mantenerse la exactitud y completitud de la información y sus métodos de proceso. Su objetivo es prevenir modificaciones no autorizadas de la información.

**Disponibilidad**: Garantizar el acceso y la utilización de la información y los sistemas de tratamiento de la misma, por parte de los individuos, entidades o procesos autorizados cuando lo requieran. Su objetivo es prevenir interrupciones no autorizadas de los recursos informáticos. (Isowin, 2017)

Figura 1.1


**Protección de los activos**

De acuerdo a Incibe (2016) menciona que para lograr esta protección de los activos se debe establecer, implantar, mantener y mejorar un SGSI, el cual puede desarrollarse según el conocido enfoque de mejora continua denominado Ciclo de Deming. Este enfoque está constituido por cuatro pasos:

**Planificar:** es una fase de diseño del SGSI en la que se evalúan los riesgos de seguridad de la información y se seleccionan los controles adecuados.

**Hacer:** es una fase que envuelve la implantación y operación de los controles.

**Verificar:** es una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI.

**Actuar:** en esta fase se realizan cambios periódicamente para mantener el SGSI al máximo rendimiento.

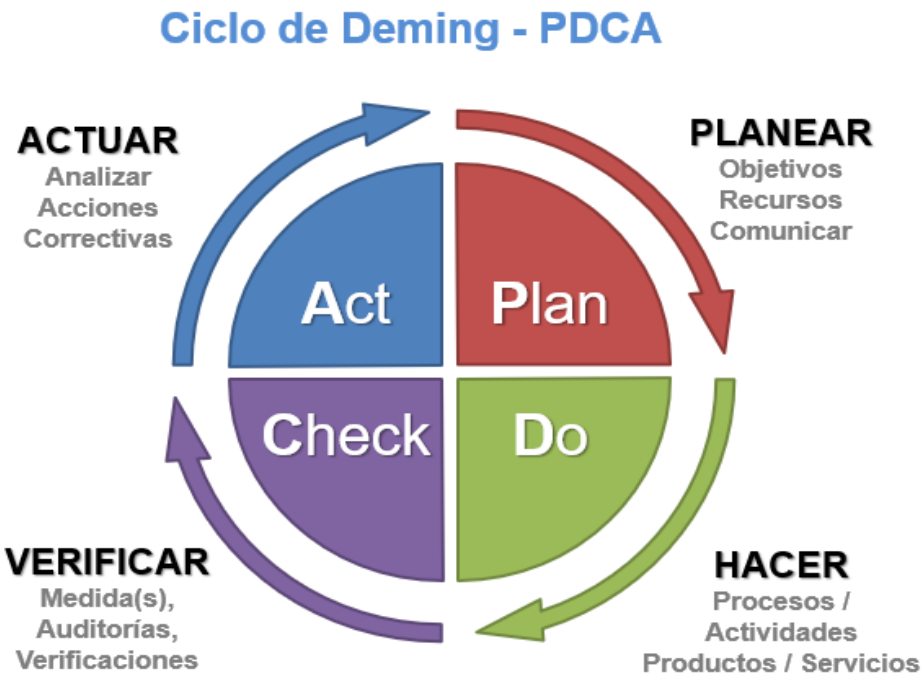



Figura 1.2

**Beneficios de un SGSI**

Conforme menciona Firma-e (2014), los principales beneficios de un SGSI son:

- ✓ Confianza y satisfacción de los requisitos de seguridad de la información por los clientes y otras partes interesadas.
- ✓ Establecimiento de una metodología de gestión de la seguridad clara y estructurada cumpliendo con los reglamentos, la legislación y las exigencias de la industria.
- ✓ Gestionar los activos de información de manera organizada que facilite la mejora continua y el ajuste a los objetivos organizacionales en cada momento sin una compra sistemática de productos y tecnologías.

- ✓ Reducción del riesgo de pérdida, robo o corrupción de información con la posibilidad de continuar la actividad después de un incidente grave (debido cuidado y diligencia).


Figura 1.3

**Historia de la norma ISO 27001**

De acuerdo a IT Service (2017), la norma fue publicada en octubre de 2005 por la Organización Internacional de Estandarización y por la Comisión Electrónica Internacional. Se considera como un estándar internacional, debido a que hace referencia a un compendio de requisitos que exige que los sistemas de seguridad de la información en la organización garanticen la mejora continua y la administración adecuada de la información.

El interés por gestionar la seguridad de la información surgió por los riesgos a los que está expuesta en medio del tránsito hacia la digitalización; el principal problema fue la forma en la que se manejó la información y su control público-privado, independientemente de su formato: datos, video y voz, en medios tradicionales o en medios magnéticos.

**Aspectos importantes de una evaluación de riesgos ISO 27001**

Según ISOTools (2018), la norma ISO 27001 permite a las empresas definir ampliamente sus propios procesos de gestión de riesgos. Los métodos comunes analizan todos los riesgos para activos específicos o riesgos presentados en escenarios específicos.

Existen cinco aspectos importantes de una evaluación de riesgos ISO 27001:

1. Establecer el marco de evaluación de riesgos
2. Identificar los riesgos
3. Analizar dichos riesgos
4. Evaluar los riesgos
5. Seleccionar las opciones de gestión de riesgos

**Consideraciones previas a la implementación del SGSI**

Según Mendoza (2017), menciona que si bien no existe un procedimiento que describa paso a paso cómo implementar el estándar, existen factores que resultan fundamentales para tener una mejor proyección de los esfuerzos necesarios y para la obtención de resultados aceptables, mismos que se describen a continuación:

1. Respaldo y patrocinio
2. Estructura para la toma de decisiones
3. Análisis de brecha (GAP)
4. Análisis de Impacto al Negocio (BIA)
5. Recursos: tiempo, dinero y personal
6. Revisión de los estándares de seguridad

**Modelos de implementación Cloud Computing**

De acuerda a Cloud (2020), existen 3 modelos fundamentales de implementación:

**Cloud Pública**

Se trata de infraestructura tecnológica (hardware, software de BD, aplicaciones y servicios) que está disponible para el uso público en general. Este tipo de "nube" puede estar gestionado por una empresa, entidad académica o gubernamental o combinaciones de ellas.

**Cloud privada**

La infraestructura de una nube privada es gestionada y utilizada por una única organización. La gestión puede estar delegada en un tercero, pero bajo supervisión directa de la organización. Asimismo la nube puede estar dentro de los límites físicos de la organización o fuera de la misma.

**Cloud Híbrida**

Es la composición de dos o más nubes (ej. privada y pública), que siguen siendo entidades únicas, pero que se integran entre ellas por tener tecnologías compatibles que les permiten compartir datos y aplicaciones, y ser portables entre ellas.

# MARCO METODOLOGICO.

## Metodología de la Investigación

### Modalidad de la Investigación.

El presente trabajo investigativo es de tipo Analítico cualitativo ya que se fundamenta en el estudio del 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 para la empresa DATA-FIBER. Este proyecto tiene en mente ampliar la capacidad de proyección hacia un SGSI compacto utilizando para ello métodos de resolución prácticos, que facilitará la gestión de quienes lo manejen o apliquen, dando como resultado satisfacción al cliente o usuario en la nube.

## TIPOS DE INVESTIGACIÓN

Podemos resumir en los siguientes tipos de investigación:

### Analítica o Descriptiva.

En esta fase se realiza una recopilación, análisis e interpretación de datos, para luego determinar (describir) el problema encontrado en esta etapa de investigación realizada.

**Detallada o Explicativa**.- Al concluir la fase anterior es decir conocer los pormenores de los resultados de la investigación realizada, se detalla que motivos producen los problemas o fenómenos descubiertos en la investigación de la fase inicial.

### Documental o Escrita.

Toda Investigación se basa en el uso de documentos o materiales diseñados e impresos como libros, folletos, revistas, tutoriales reglamentos y demás materiales que se utilizan como soporte para una buena investigación, estos ayudaran en el análisis interpretativo del problema a investigar y nos dará claridad para proyectar una gran propuesta de nuestro trabajo, que por supuesto ira dirigido específicamente a la satisfacción de nuestros clientes.

## METODOS Y TÉCNICAS

Como todo trabajo investigativo se utilizan métodos y técnicas de investigación que permiten ver con claridad el problema a solucionar, se utilizaran los siguientes métodos:

**Método descriptivo.**

Se encarga de la descripción de los datos y características de la población a investigar. La meta es obtener datos claros, precisos y concisos los cuales se usaran cálculos aritméticos y los estadísticos según la necesidad.

**Método Inductivo.**

Permite obtener conclusiones generales a partir de antecedentes particulares. Es el método científico más común que se utiliza en casi toda investigación, y del cual nuestro proyecto lo toma como parte esencial de la investigación.

**Método Analítico y Sintético.**

Este método permite llegar a la veracidad de las situaciones o cosas, primero se apartan los elementos que se incluyen en la observación de un determinado fenómeno, luego se unen con los elementos que tienen relación lógica entre ellos hasta completar y aclarar la veracidad del conocimiento tratado.

**Resultados y Discusiones**

Obtenemos como resultados de nuestro estudio de caso con el Gerente de la Empresa DATA-FIBER lo siguiente:

- En la actualidad, existen un gran número de empresas, ya sean públicas o particulares que prefieren utilizar los servicios que brinda la tecnología Cloud Computing, pero es necesario analizar que para el uso de estos recursos sean beneficiados al máximo y de manera eficaz, debemos capacitar y concientizar a todos los clientes o usuarios implicados acerca de los beneficios y conflictos que brinda esta tecnología en la actualidad.
- Para implantar el plan de seguridad en un ambiente Cloud Computing, la gran mayoría de operaciones se la realizan en conjunto entre las empresas proveedoras de la utilidad en la web y por otro lado el usuario o cliente, estableciendo de esta forma responsabilidades y derechos compartidos.
- Una inquietud muy importante es la seguridad y la integridad de los datos para las empresas que requieren migrar de una interfaz habitual a un ambiente tecnológico Cloud Computing, con ello se garantiza en gran porcentaje la fuga o pérdida de control o la disponibilidad de los datos, conocemos que la última afecta de forma directa en la ejecución de los procesos de las empresas relacionadas.
- Al relacionar el ambiente habitual con el ambiente Cloud Computing, en ambos casos se definen de forma clara los procesos y responsables, permanentemente guiados a la confiabilidad, Integridad, y disponibilidad de los datos, bases fundamentales en la cual se cimenta este proyecto.
- La concientización de las medidas preventivas permitirá guiar a las compañías sobre la protección del activo más significativo que tienen, que es la “información total”, y en este caso nuestra empresa DATA FIBER considerando que, si se produce una fuga de esta información valiosa, podría provocar la suspensión parcial o total de una o un grupo de procesos de la compañía, lo cual ocasionaría sin lugar a dudas una gran debacle económica en las arcas de la empresa.

## 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.

## 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.

## Referencias Bibliográficas

**Alvarado, C. (02 enero de 2002).** Pensemos. Recuperado el 17 de marzo del 2022 de: https://gestion.pensemos.com/sistema-de-gestion-de-seguridad-de-la-informacion-que-es-etapas

**Benioff, M. (03 enero de 2017).** Salesforce. Recuperado el 17 de marzo del 2022 de: https://www.salesforce.com/mx/cloud-computing/

**Iso27000 (marzo de 2005).** SGSI Iso27000. Recuperado el 18 de marzo del 2022 de: https://www.iso27000.es/sgsi.html

**Tesis y Máster (enero de 2021).** Tesis y Máster. Recuperado el 18 de marzo del 2022 de: https://tesisymasters.com.ar/tesis-marco-metodologico/

**Tesis doctoral (09 junio de 2009).** Tesis doctoral. Recuperado el 19 de marzo del 2022 de: https://www.tdx.cat/bitstream/handle/10803/8931/7RESULTADOSDELAINVESTIGACIONVI.pdf;sequence=8

**SAS Colombia (05 junio de 2014).** SasColombia. Recuperado el 19 de marzo del 2022 de: https://blogs.sas.com/content/sasla/2014/06/05/cinco-caracteristicas-esenciales-de-la-computacion-en-lanube/

**BeServices (02 enero de 2020).** Salesforce. Recuperado el 21 de marzo del 2022 de: https://www.beservices.es/porque-utilizar-cloud-computing-n-5377-es

**ISOwin S.L. (11 junio de 2017).** ISOwin S.L. Recuperado el 21 de marzo del 2022 de: https://isowin.org/blog/activos-ISO-27001/

**Incibe. (28 noviembre de 2016).** Incibe. Recuperado el 21 de marzo del 2022 de: https://www.incibe.es/protege-tu-empresa/blog/las-5-medidas-basicas-proteger-tu-principal-activo-informacion

**Firma-e (11 octubre de 2021).** Firma-e. Recuperado el 22 de marzo del 2022 de: https://www.firma-e.com/blog/beneficios-de-implantar-un-sgsi-en-su-empresa/

**Einatec (10 abril de 2018).** Einatec. Recuperado el 22 de marzo del 2022 de: https://einatec.com/como-funciona-el-cloud-computing/

**IT Service (12 Abril de 2020).** IT Service. Recuperado el 22 de marzo del 2022 de: https://itservice.com.co/iso-27001-una-breve-historia-de-la-norma/

**ISOTools Excellence (24 mayo de 2018).** ISOTools Excellence. Recuperado el 23 de marzo del 2022 de: https://www.pmg-ssi.com/2018/05/importancia-implementar-norma-iso-27001/

**ISOTools Excellence (22 Agosto de 2019).** ISOTools Excellence. Recuperado el 23 de marzo del 2022 de: https://www.pmg-ssi.com/2019/08/iso-27001-aspectos-claves-y-relacion-con-las-normas-iso-22301-e-iso-iec-20000/

**Mendoza, M. (06 noviembre de 2017).** WeliveSecurity. Recuperado el 24 de marzo del 2022 de: https://www.welivesecurity.com/la-es/2017/11/06/consideraciones-implementacion-del-sgsi/

**Cloud (02 mayo de 2020).** Cloud.com. Recuperado el 24 de marzo del 2022 de: https://evaluandocloud.com/modelos-de-implementacion-del-cloud/

## Resumen y Palabras Claves.


**RESUMEN**

La tecnología está en pleno auge, y los cambios son notorios a nivel de hardware y software, esto implica también grandes transformaciones en la instalaciones lo cual sin duda hace factible que las compañías brinden sus productos y servicios de manera fácil y confiable; hoy en día las organizaciones en su gran porcentaje, han resuelto migrar todos sus datos de manera cómoda, a un ambiente Cloud Computing por las grandes ventajas y posibilidades que esta interfaz brinda, como base principal, quita la enorme responsabilidad a las compañías de actualizar sus equipos y es especial el software para poder competir y estar acorde a los nuevos adelantos tecnológicos.

El proyecto a continuación presentado relata los requerimientos que se necesitan 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, creando la necesidad de detallar y especificar al ambiente Cloud Computing, las funcionalidades ventajas, desventajas y características que muestra este modelo.

Considerando que la norma ISO27001 la podemos utilizar en cualquier tipo de organización sin excluir su naturaleza o tipo de donde proviene, por lo cual se elabora un estudio exhaustivo que determine orientar el uso de la norma mencionada al ambiente Cloud Computing, considerando con anterioridad los peligros, amenazas, vulnerabilidades y falencias que se pudiesen exteriorizan en mencionado ambiente que podría estabilizar la trasferencia de datos y su posterior almacenamiento en la empresa DATA-FIBER.

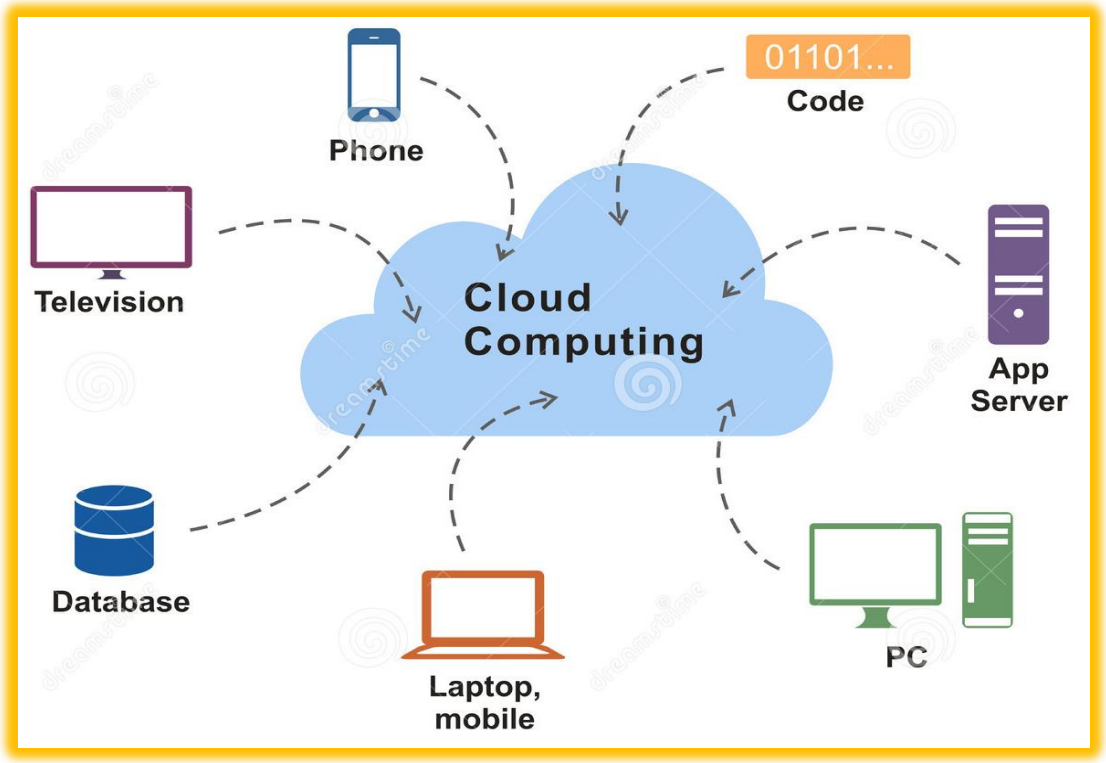

## Palabras Claves


Sistema de gestión de Seguridad Informática (SGSI), Computación de la Nube, Seguridad de la Información, activo de la información, Aplicación de la Norma ISO 270001.

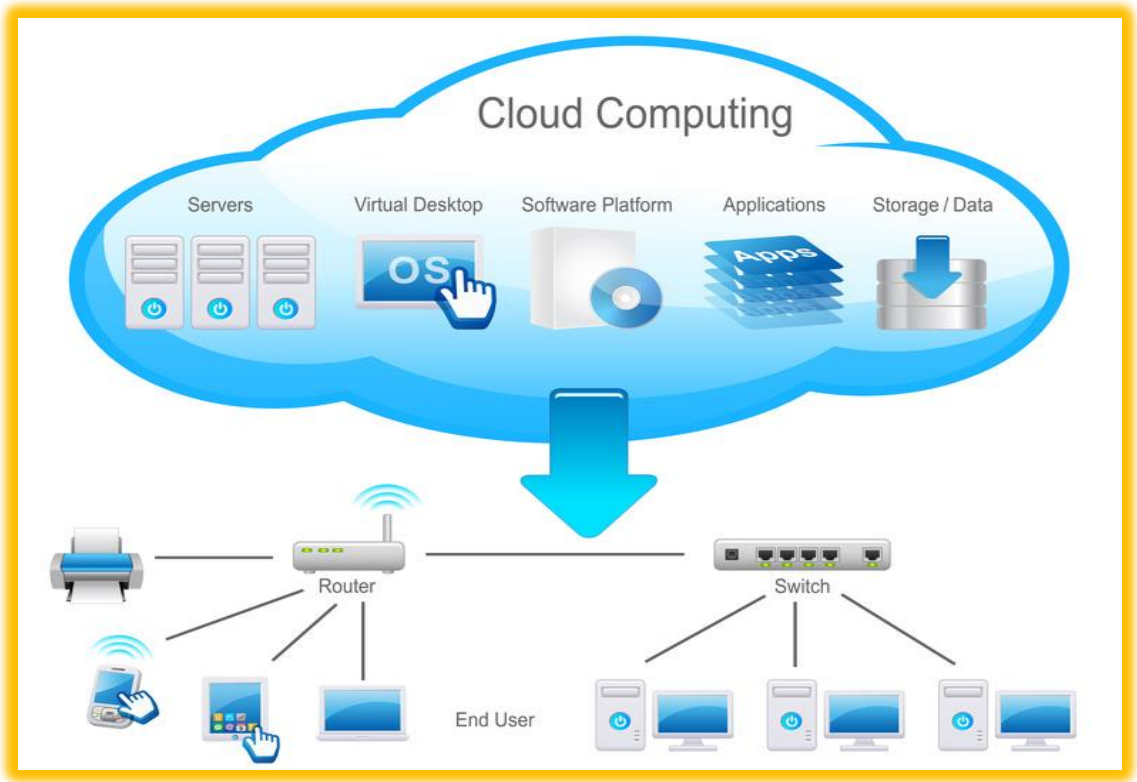
# Anexos


Este tipo de red de área local, su desarrollo comienza a partir de las necesidades de preparar la comunicación entre los dispositivos digitales presentes en el interior de la casa.

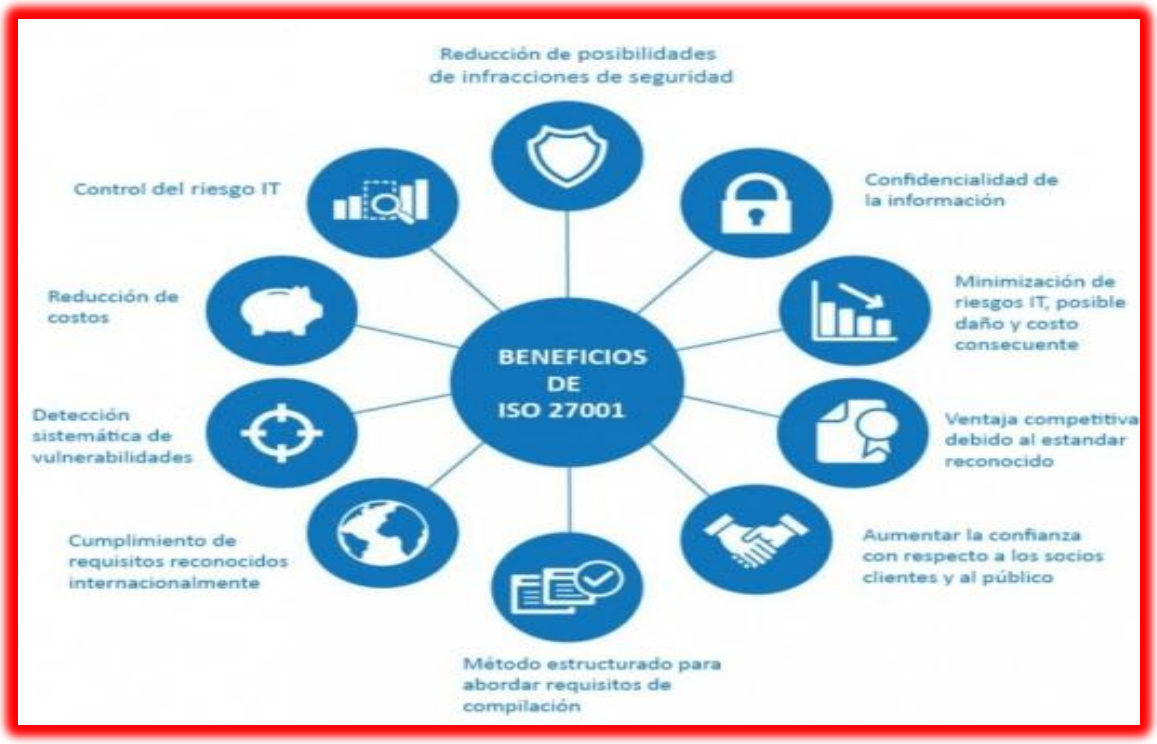
Los únicos en disfrutar esta red son los dispositivos inteligentes, como impresoras de red u ordenadores portátiles, la capacidad adicional que puedes utilizar es la calidad de vida dentro de tu hogar con diversas formas por ejemplo disfrutar de la red informática en el hogar.




El Cloud Computing o computación en la nube es una tecnología que permite el acceso remoto a softwares, procesamiento de datos y almacenamiento de archivos a través de Internet. No demanda la instalación de aplicaciones a nivel local, sino que ofrece los servicios a gran escala gracias a la conectividad.




Hay cuatro tipos principales de Cloud Computing: las nubes públicas, las nubes privadas, las nubes híbridas y las multiclouds.




## 4 BENEFICIOS DE IMPLEMENTAR ISO 27001 EN NUEVAS EMPRESAS

1. Obtener nuevos negocios y fidelizar clientes

2. Evitar las pérdidas financieras y las sanciones asociadas con las vulneraciones de datos

3. Proteger y mejorar la reputación de la organización

4. Cumplir con los requisitos comerciales, legales, contractuales y reglamentarios


La ISO 27001 es la norma internacional que proporciona un marco de trabajo para los sistemas de gestión de seguridad de la información (SGSI) con el fin de proporcionar confidencialidad, integridad y disponibilidad continuada de la información, así como cumplimiento legal. La certificación ISO 27001 es esencial para proteger sus activos más importantes, la información de sus clientes y empleados, la imagen corporativa y otra información privada. La norma ISO incluye un enfoque basado en procesos para lanzar, implantar, operar y mantener un SGSI.

La implantación de la ISO 27001 es la respuesta ideal a los requisitos legislativos y de los clientes, incluyendo el RGPD y otras amenazas potenciales, incluyendo: Crimen cibernético, violación de los datos personales, vandalismo / terrorismo, fuego / daños, uso malintencionado, robo y ataque de virus**.**