ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA EN SISTEMAS

IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI), BAJO LA NORMA ISO/IEC 27001:2013, EN UNA EMPRESA DE SERVICIOS

PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

CHRISTIAN MANUEL RÍOS CRIOLLO
christian.rios@hotmail.com

HUGO PAÚL TINOCO SILVA
paul.tinocosilva@gmail.com

Director: ING. JUAN HERRERA, MSc.
juan.herrera@leveltech.com.ec

DECLARACIÓN

Nosotros, Christian Manuel Ríos Criollo y Hugo Paúl Tinoco Silva, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____	_____
Christian Manuel Ríos Criollo	Hugo Paúl Tinoco Silva

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Christian Manuel Ríos Criollo y Hugo Paúl Tinoco Silva bajo mi supervisión.

Ing. Juan Herrera, MSc.

DIRECTOR DE PROYECTO

AGRADECIMIENTOS

Agradecemos a nuestra familia que siempre estuvo junto a nosotros y a todas las personas que hicieron posible el desarrollo de este proyecto.

DEDICATORIA

Esta tesis la dedicamos a nuestra familia que nos supo guiar por un buen camino para poder alcanzar nuestras metas, objetivos en nuestra vida y no rendirnos frente a las adversidades que se nos presentaron.

ÍNDICE DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

RESUMEN

El objetivo del presente Proyecto de Titulación es desarrollar y marcar las directrices para la implementación de un Sistema de Gestión de Seguridad de Información (SGSI) para un servicio de “Levantamiento Catastral Automatizado” (al que a partir de este momento, por motivos de confidencialidad, será llamado “Censos de Información Comercial”), brindado por una empresa de servicios “XYZ” a una Distribuidora de Energía.

En el primer capítulo, se describe cómo será diseñado e implementado el SGSI bajo la norma ISO/IEC 27001:2013 siguiendo el Ciclo de Deming, para alcanzar este objetivo se realiza un reconocimiento panorámico detallado del desarrollo del servicio en función de los procesos que lo componen y los activos de información involucrados.

En el segundo capítulo, se realizará el reconocimiento, análisis y evaluación de las amenazas, vulnerabilidades y riesgos a los que se ve expuesto el servicio, mediante el uso de una metodología de evaluación de riesgos escogida al realizar un análisis comparativo previo. También se recomendarán los controles necesarios para mitigar los riesgos de seguridad de información. Finalmente, se analizarán los requerimientos de seguridad de información del servicio tomando en cuenta tres áreas: operacional, técnica y administrativa.

El tercer capítulo describe el análisis de los controles de la norma ISO/IEC 27001:2013 que serán aplicados, una vez que se han identificado y definido: requerimientos legales y organizacionales del servicio, su alcance y límites, la política del SGSI y el enunciado de aplicabilidad, que especifica formalmente los controles aplicables de la norma.

El capítulo cuatro abarca la implementación del SGSI desarrollado hasta el momento, que incluye: la selección e implementación de los controles de la norma que serán implementados mediante políticas o procedimientos formales.

Finalmente el capítulo cinco especifica las conclusiones y recomendaciones obtenidas por parte de los autores del presente proyecto de titulación.

CAPÍTULO 1. INTRODUCCIÓN

En la actualidad, se considera que el principal activo para cualquier empresa es la información que maneja para el desarrollo de sus actividades, por tal motivo, el avance de la tecnología enfocado principalmente en el manejo de información puede ofrecer grandes beneficios, pero también puede ocasionar diversos tipos de problemas, desde la aparición de riesgos y vulnerabilidades que pueden desembocar en pequeños inconvenientes hasta desastres que pueden ser catastróficos para los dueños de la información y la empresa en sí, precisamente porque este avance también presenta nuevos riesgos y vulnerabilidades de diversa naturaleza.

Para poder controlar de forma efectiva todos los posibles problemas identificados con la seguridad de información en los procesos y actividades de una empresa, es necesario implementar un Sistema de Gestión de Seguridad de Información (SGSI), cuyas condiciones de desarrollo e implementación son claramente explicadas por la norma ISO/IEC 27001:2013.

En el presente proyecto de titulación se describirá un servicio de manejo de información de una Distribuidora de Energía, al cual se lo denominará Levantamiento Catastral Automatizado (llamado a partir de ahora “Censos de Información Comercial”); este servicio se caracteriza principalmente por la obtención y depuración de información de clientes de dicha distribuidora, utilizando tanto medios tecnológicos como conocimiento y capacidad humana. Como se mencionó anteriormente, un mal uso de los recursos tecnológicos, sumado a los riesgos inherentes que presenta el servicio con respecto al manejo real de información puede ocasionar problemas de integridad, confidencialidad y disponibilidad de la misma, por esta razón, se tomará como referencia a una Empresa de Servicios “XYZ” cuyo servicio a fortalecer con el SGSI bajo la norma ISO 27001:2013 está relacionado al tema “Censos de Información Comercial” mencionado anteriormente.

Para realizar la implementación del SGSI en el servicio, primero se debe revisar las siguientes definiciones de los procesos comerciales:

PREDIO

Es un bien inmueble que pertenece legalmente a un individuo; este bien inmueble es principalmente una extensión de terreno del cual se conoce su ubicación geográfica y delimitación.

"PROCESO DEL SERVICIO DE CENSOS DE INFORMACIÓN COMERCIAL

Este servicio se divide en cuatro fases:

a. **Planificación de Rutas:** se diseña las rutas de la manera más conveniente para la toma de datos de catastro.
b. **Levantamiento de Información:** es el proceso por el cual se recopila la información del catastro mediante la utilización de una aplicación móvil.
c. **Procesamiento de Información:** a través de este proceso la información recolectada es verificada y ordenada según la necesidad.
d. **Afinamiento de Información:** mediante este proceso se corrige (si es necesario) la información para posteriormente cargarla al Sistema de Catastro Automatizado."[1]

CATASTRO DE LOS CLIENTES

La Distribuidora de Energía tiene la necesidad de llevar un registro de la ubicación, registro catastral e información de sus clientes, para lo cual debe tener identificadas las características y ubicación de los predios y el estado del servicio que recibe cada uno de ellos. Esta información es de base para la planificación global de la empresa y del área comercial.

---

[1] Fuente: Información Comercial brindada por la empresa de servicios "XYZ".

De acuerdo a la información obtenida mediante la investigación de campo, los tipos de clientes son los siguientes:

a. **"Reales:** son los predios que tienen junto a ellos una red matriz de energía eléctrica, poseen una conexión domiciliaria desde la matriz y tienen registrado una cuenta o contrato con la empresa.
b. **Factibles:** son los predios que tienen junto a ellos una red matriz de energía eléctrica pero no poseen una conexión domiciliaria desde la matriz y no tienen registrado una cuenta o contrato con la empresa.
c. **Potenciales:** son los predios que no tienen junto a ellos una red matriz de energía eléctrica, no poseen una conexión domiciliaria desde la matriz y no tienen registrado una cuenta o contrato con la empresa.**"**[2]

GEOCÓDIGO

Es un identificador único de la localización comercial para cada cliente real, factible o potencial. Está conformado por seis campos de datos numéricos (Sector – Ruta – Manzana – Secuencia – Piso – Departamento), cada uno de ellos representa la ubicación e identificación geográfica del predio dentro de una zona definida. Por lo general el área de cobertura total, la cual es abastecida del servicio de energía eléctrica, se divide en varios sectores como se muestra en la Figura 2, para agrupar e identificar la ubicación de cada cliente. Este dato está representado en el primer campo del geocódigo llamado "Sector".

Ejemplo de Geocódigo:

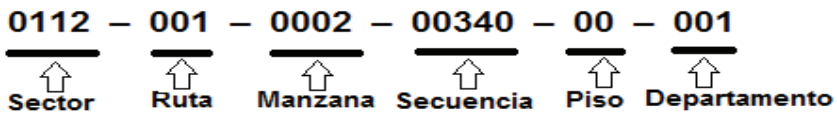

Figura 1 – Geocódigo
Fuente: Empresa de servicios "XYZ"

[2] Fuente: Proyecto de Titulación: *"Solución Móvil para Facturación y Recaudación en un Ambiente Distribuido"*, pág. 71. Escuela Politécnica Nacional, Ayala Vargas William Raúl. Ing. Juan Herrera, MSc, 2010.

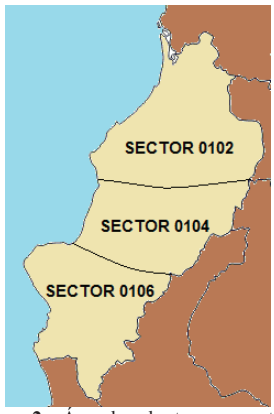

Figura 2 – Área de cobertura por sectores
Fuente: Empresa de servicios "XYZ"

A continuación, por cada Sector se realiza una división por rutas como se muestra en la Figura 3, que es representada por el segundo campo del geocódigo denominado "Ruta".

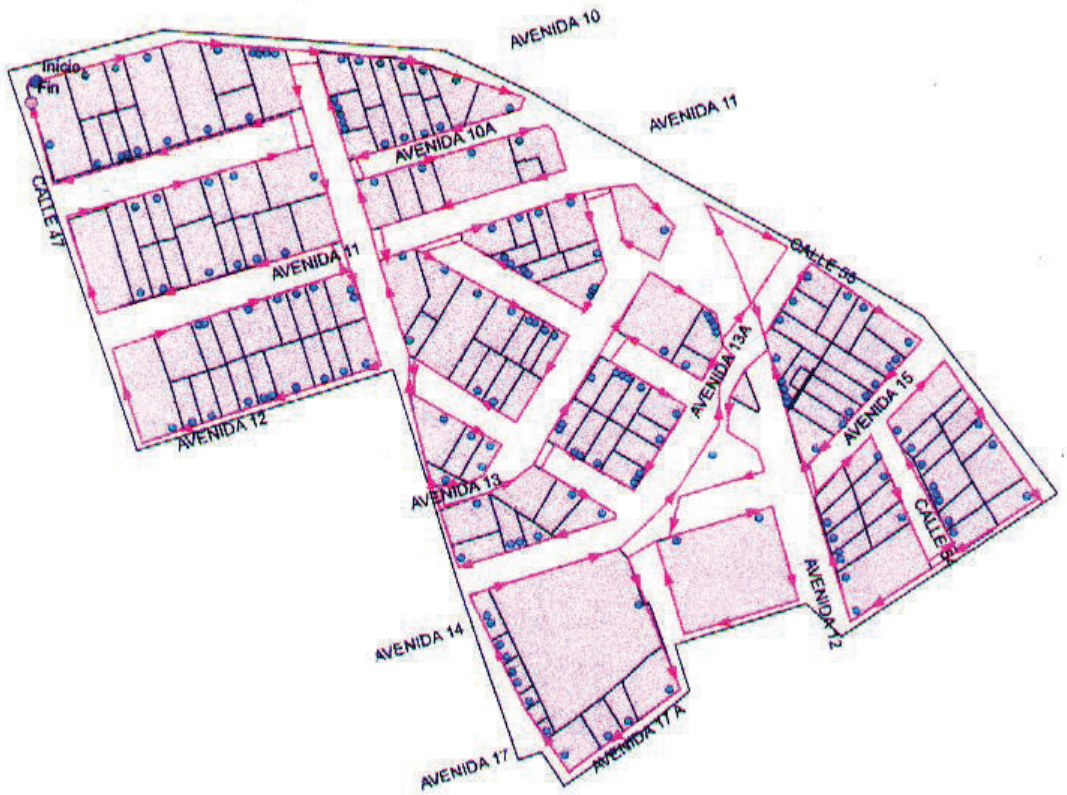

Figura 3 - Área de cobertura por rutas
Fuente: Empresa de servicios "XYZ"

Luego, por cada Sector y Ruta se realiza una nueva división, la cual está representada por el tercer campo del geocódigo denominado “Manzana”, como se muestra en la Figura 4.

Figura 4 - Área de cobertura por manzanas en base a la ruta
Fuente: Empresa de servicios “XYZ”

Los tres primeros campos del geocódigo (Sector, Ruta y Manzana) son utilizados para determinar la ubicación geográfica de un medidor del servicio de energía. Por medio de esta clasificación de información se puede organizar mejor el trabajo de campo para la toma de lecturas de medidores.

Con los campos expuestos hasta el momento sólo se ha ubicado al cliente en un área pequeña con respecto al área de cobertura total; los siguientes campos sirven para obtener la ubicación exacta de cliente:

Primero es la “Secuencia”, que identifica al predio donde se encuentra el cliente, que puede ser una casa o un edificio. La Secuencia indica al encargado de las tomas de lecturas como debe realizar su recorrido. Con esta información se obtiene la ubicación exacta de cada cliente de la Distribuidora de Energía. Un predio puede tener más de un medidor, por ejemplo en los departamentos de un edificio, por lo cual se utilizan los dos últimos campos del geocódigo, para ubicar el “Piso” y “Departamento” donde existe más de un medidor de energía eléctrica a continuación se muestra un ejemplo de secuencia en la Figura 5.

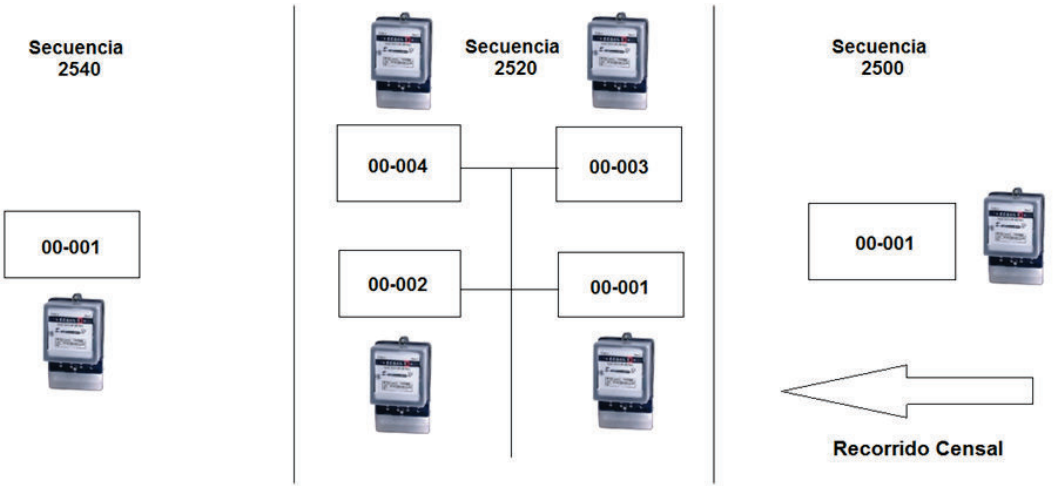

Figura 5 – Secuencia de Predios
Fuente: Empresa de servicios "XYZ"

1.1 DEFINICIÓN DEL PROBLEMA

La empresa a ser evaluada provee servicios principalmente de Levantamiento Catastral Automatizado (Censos de Información Comercial), que consiste en un proceso que recolecta información de campo para los clientes y usuarios del servicio público de energía eléctrica y genera una base de datos alfanumérica y cartografía en formato digital, registrando todos los datos e información necesarios acerca de los predios y clientes reales, factibles y potenciales, respecto a la disponibilidad del servicio de energía eléctrica, así como de su ubicación geográfica exacta a través de códigos numéricos predefinidos y georreferenciados; por tanto el tratamiento, manejo y distribución de dicha información debe estar enmarcada en un Sistema de Gestión de Seguridad de la Información (SGSI) que garantice la confidencialidad, integridad y disponibilidad acorde a estándares de seguridad como la ISO/IEC 27001:2013.

1.2 OBJETIVOS Y ALCANCE

1.2.1 OBJETIVO GENERAL

- Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) bajo las normativas de la ISO/IEC 27001:2013 en una empresa de servicios.

1.2.2 OBJETIVOS ESPECÍFICOS

- Recopilar y evaluar la documentación existente que ha sido desarrollada por la empresa de servicios sobre la Gestión de Seguridad de Información.
- Generar una Matriz de Riesgos que permita identificar, analizar y evaluar los riesgos a los que se expone las TICs de la empresa de servicios.
- Analizar y definir los requerimientos de seguridad para el servicio de Levantamiento Catastral Automatizado.
- Identificar y evaluar los objetivos de control que requieren ser implementados acorde a las necesidades del servicio de Levantamiento Catastral Automatizado como parte de un SGSI.
- Implementar un SGSI en una empresa de servicios para el servicio de Levantamiento Catastral Automatizado.

1.2.3 ALCANCE

El proyecto de titulación tiene como objetivo inicial generar un análisis sobre el nivel de seguridad del servicio de “Censos de Información Comercial” basado en la evaluación de la documentación proporcionada por una empresa de servicios, para posteriormente determinar los riesgos a los que se expongan los TICs en la empresa frente al estándar ISO/IEC 27001:2013. Con base en estos resultados identificar los requerimientos y controles de seguridad más apropiados para la empresa acorde a las necesidades de negocio; finalmente se establecerán la

documentación y procedimientos requeridos como parte de la implementación de un SGSI.

El SGSI ayuda a mantener un alto nivel de administración de la seguridad de información, la forma en que se lo implemente a la realidad de la empresa influirá directamente en el éxito de su funcionamiento y actualización continua. Por este motivo, a continuación se describirá la metodología de implementación del SGSI a utilizarse para el desarrollo del presente trabajo de titulación.

1.3 METODOLOGÍA DEFINIDA PARA LA IMPLEMENTACIÓN DE UN SGSI

Un requisito indispensable que propone ISO (International Organization for Standarization) para la implementación de la norma ISO 27001:2013, es el enfoque de mejora continua, el cual puede ser alcanzado utilizando diversas metodologías, como Six Sigma (6õ) o PDCA. En el presente proyecto de titulación se utilizará PDCA, por la experiencia de su uso en la implementación de esta norma, además del enfoque a procesos que brinda, siendo igualmente la más utilizada por ISO en versiones anteriores de la norma en cuestión.

1.3.1 CICLO DE DEMING

La implementación y control de un SGSI al servicio de Censo de Información Comercial se realiza en función del Ciclo de Mejora Continua o Ciclo de Deming. El Ciclo de Deming es continuo, se realiza en cuatro pasos (Figura 6) y operan constantemente para lograr cada vez una mejor calidad del proceso en el que se implemente. Los cuatro pasos del Ciclo de Deming son:

1. Plan (Planificar)
2. Do (Hacer)
3. Check (Revisar)
4. Act (Actuar)

Figura 6 – Ciclo de Deming
Fuente: Empresa de servicios "XYZ"

1.3.2 DESCRIPCIÓN DE LOS PASOS PARA EL DESARROLLO E IMPLEMENTACIÓN DEL SGSI

La aplicación del Ciclo de Deming en el desarrollo del SGSI para servicio de "Censos de Información Comercial" se realiza de la siguiente forma (revisar "**Anexo A - Diagrama de Implementación SGSI"**):

1.3.2.1 Plan (Planificar)

La planificación del SGSI para el servicio comprende:

a. **OBTENCIÓN DEL SOPORTE DIRECTIVO:** la implementación de un SGSI debe contar con el respaldo de la dirección administrativa: Gerente de Proyecto y Líder de Proyecto, que deben aportar su conocimiento y experiencia en el manejo del servicio para obtener una visión panorámica de su funcionamiento.
b. **ALCANCE DEL SGSI:** Para definirlo se tomará en cuenta las siguientes actividades derivadas de las fases mencionadas anteriormente:
   - **Características de los procesos de captura y procesamiento de datos:** son las siguientes:
     - Origen de datos de entrada

  - Tipos de datos de entrada
  - Procesamiento de los datos
  - Tipos de datos de salida.
- Pasos de desarrollo de toma, registro y procesamiento de datos.
- Activos y tecnologías utilizados para el desarrollo del servicio.
- Excepciones de registro de datos.
- **Políticas del SGSI:** serán diseñadas en función del alcance que tenga el SGSI para el servicio y su principal objetivo será la protección de la disponibilidad, integridad y confidencialidad de la información. La creación de políticas considera:
  - El marco de funcionamiento del servicio en base a los objetivos de seguridad de información de la empresa de servicios XYZ.
  - El marco legal bajo el que se trabaja.
  - Concordancia entre estas políticas y las estrategias de tratamiento de riesgos de seguridad de información utilizadas.

c. **INVENTARIO DE LOS ACTIVOS DE INFORMACIÓN:** debe considerar el registro y procesamiento de los datos de información comercial implicados en el desarrollo del servicio.

   El nivel de detalle al que se llegue en el desarrollo del inventario influirá de manera directa y tendrá un alto impacto en los resultados obtenidos, esto ocurre porque aquí se registrarán todos los activos utilizados en el desarrollo del servicio.

d. **METODOLOGÍA DE GESTIÓN DE RIESGOS:** implica escoger y ejecutar procedimientos adecuados para llevar a cabo un tratamiento efectivo de los riesgos que pueden afectar al servicio. El ciclo de desarrollo de una metodología sigue las siguientes etapas:

   - **Definición de la Metodología:** en función de:
     - Requerimientos del desarrollo del servicio.
     - El establecimiento de niveles de estudio y tratamiento del riesgo.
   - **Valoración de los riesgos de seguridad de información:** se realizará luego de identificar los riesgos y analizar su impacto en el desarrollo del servicio.

- **Definición de la Declaración de Aplicabilidad:** esta declaración de aplicabilidad deberá incluir:
  - Objetivos de control y controles seleccionados.
  - Análisis de calidad de los objetivos de control existentes, en el caso que hayan sido implementados anteriormente.
- **Definición del Plan de Tratamiento de Riesgos:** una vez identificados los riesgos existentes y los controles adecuados para el tratamiento de los mismos, se definirá el procedimiento adecuado para su control.

  Este plan debe contemplar acciones, recursos, responsabilidades y prioridades de gestión de tratamiento de riesgos de seguridad de información.

e. **IDENTIFICACIÓN DE CONTROLES APLICABLES DE LA ISO 27001:** el desarrollo de este plan se basa principalmente en la implementación de controles escogidos de la ISO/IEC 27001:2013, luego de ser analizados y adecuados a la realidad del servicio.

1.3.2.2 Do (Hacer)

Luego de identificar los riesgos, controles y activos de información del servicio, se procede con la implementación, la cual se detalla a continuación:

a. **IMPLEMENTACIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS:** este plan sirve principalmente para alcanzar los objetivos de control identificados anteriormente, mediante la asignación de recursos y responsabilidades en función de prioridades de seguridad de información.
b. **IMPLEMENTACIÓN DE CONTROLES:** los controles identificados en la actividad e "*IDENTIFICACIÓN DE CONTROLES APLICABLES DE LA ISO 27001"* de la etapa anterior serán implementados en el servicio.
c. **DEFINICIÓN DE UN SISTEMA DE MEDICIÓN DE EFECTIVIDAD DE LOS CONTROLES:** se deberán definir rangos comparativos para analizar los resultados obtenidos por el impacto que tienen los controles sobre el

desarrollo del servicio y la seguridad de información que se maneja en el mismo.

d. **GESTIÓN DE LAS OPERACIONES DEL SGSI:** se debe considerar:
   - La gestión de recursos que se deben asignar al SGSI para mantener la seguridad de información.
   - La implementación de procedimientos y controles para detectar y procesar incidentes de seguridad.

1.3.2.3 Check (Revisar)

Este paso implica el análisis de los resultados obtenidos luego de implementar los controles para el manejo de riesgos. La revisión incluye:

a. **REVISIÓN DEL CUMPLIMIENTO:** la revisión del cumplimiento de políticas, procedimientos y controles implementados para la gestión del SGSI se la realizará en función de:
   - **Ejecución de los procedimientos de monitorización y revisión:** la utilidad de estos procedimientos se encuentra en:
     - La detección oportuna de errores en el funcionamiento de los procesos de información.
     - Identificación de la posible aparición de nuevos riesgos que puedan comprometer la seguridad de información.
   - Analizar los resultados obtenidos luego de implementar los controles para gestionar el riesgo existente.

b. **REVISIÓN PERIÓDICA DE LA EFECTIVIDAD DEL SGSI:** esta revisión deberá evaluar la efectividad del SGSI para gestionar el riesgo; para realizarla se deberán definir indicadores y métodos de evaluación para analizar el funcionamiento que han tenido los controles, políticas y procedimientos que han sido implementados tomando en cuenta los resultados que se hayan obtenido.

c. **VALORACIÓN PRE-CERTIFICACIÓN:** para poder certificar al servicio, se deberá realizar una revisión periódica de las evaluaciones de todos los

riesgos. Esta revisión debe tomar en cuenta cambios en el servicio, la efectividad de los controles implementados, etc.

d. Ejecución de auditorías internas periódicas del SGSI.

e. REGISTRO DE EVENTOS DE SEGURIDAD DE INFORMACIÓN: finalmente se deberá llevar registros de cualquier evento sospechoso que pueda afectar a la seguridad de información y a la efectividad del funcionamiento del SGSI.

1.3.2.4 Act (Actuar)

En este punto se harán correcciones o actualizaciones, según sea el caso, del SGSI para manejar los riesgos de seguridad de información del servicio de manera efectiva:

a. ACTUALIZACIÓN DE LOS PLANES DE SEGURIDAD EN FUNCIÓN DE CAMBIOS Y/O NUEVOS EVENTOS: tomando en cuenta los resultados obtenidos en las evaluaciones realizadas en la etapa anterior, se tomarán medidas correctivas de los planes de seguridad. Estas acciones consideran la implementación, actualización, cambio o eliminación de nuevos controles, políticas o procedimientos según cambios planificados o fortuitos en el desarrollo del servicio a nivel operativo, técnico o administrativo.

b. Implementación de mejoras, tomando en cuenta proyecciones de la realidad del entorno donde se desarrolla el proceso.

c. Ejecución de medidas preventivas y/o correctivas para la seguridad de la información.

d. Revisión de resultados de las mejoras implementadas.

Una vez descrita la metodología de implementación, el siguiente paso es detallar el sistema utilizado para el desarrollo del servicio de “Censos de Información Comercial”, así como de los diferentes procesos que lo componen.

1.4 CARACTERIZACIÓN DEL SISTEMA DEL SERVICIO DE LEVANTAMIENTO CATASTRAL AUTOMATIZADO

El funcionamiento del servicio de Levantamiento Catastral Automatizado (Censos de Información Comercial) se desarrolla según se muestra en el siguiente diagrama de procesos en la Figura 7:

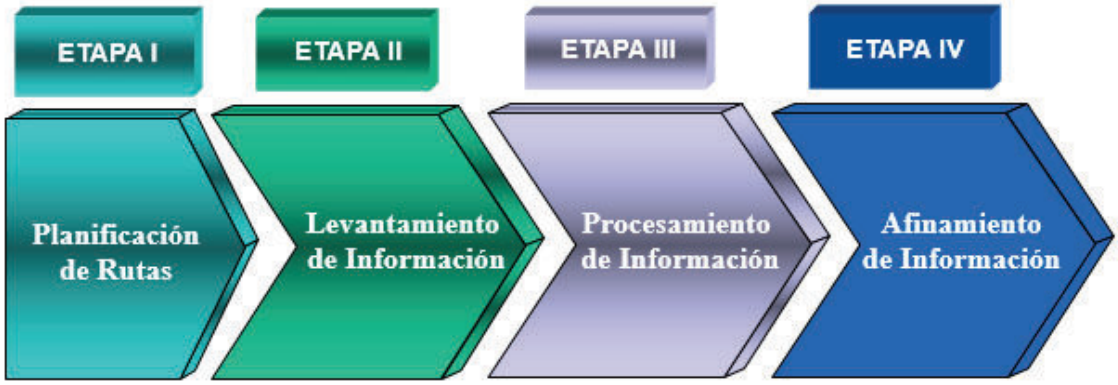

Figura 7 – Procesos de Censos de Información Comercial para Distribuidoras de Energía
Fuente: Empresa de servicios "XYZ"

A continuación se realizará una descripción de los procesos involucrados en el servicio:

1.4.1 PLANIFICACIÓN DE RUTAS

Es el ingreso de las rutas al Sistema de Catastro Automatizado (ver punto 1.4.6.3 *"Sistema de Catastro Automatizado (Sistema de Censos de Información Comercial)"*) de acuerdo a las zonas geográficas donde se realizará la recolección de datos; se diseña las rutas de la manera más adecuada para la toma de datos de catastro.

En el sistema se procede a ingresar las rutas, para esto se accede al módulo "Administrar" donde se procede a seleccionar el "Gestor de Campo" a quien se le asigna un sector y se establece la secuencia.

Se imprime el plano de las rutas que fueron asignadas en el sistema con sus respectivas hojas de planificación.

En la Figura 8 se muestra la secuencia de las actividades antes descritas:

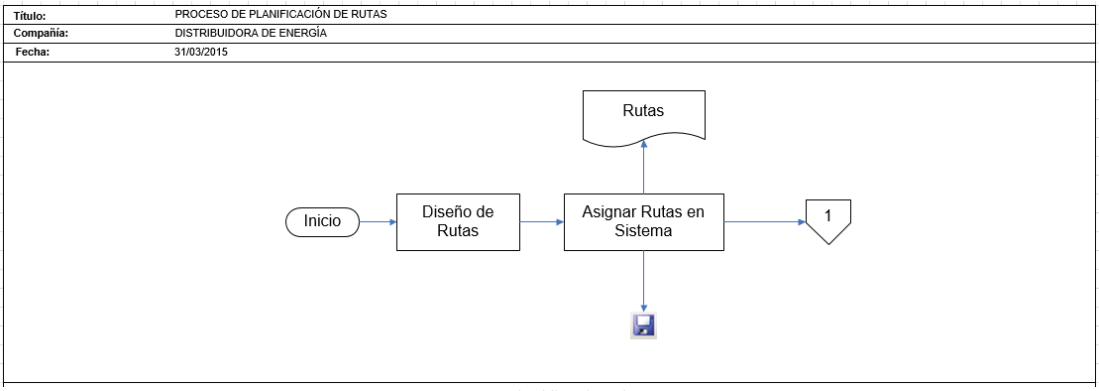

Figura 8 – Planificación de Rutas
Fuente: Empresa de servicios "XYZ"

1.4.2 LEVANTAMIENTO DE INFORMACIÓN

1.4.2.1 Cargar Datos a la Pocket

Es el almacenamiento de la base de datos en la PocketPC, con la planificación de las rutas para la recolección de datos e información base del cliente. En la PocketPC (memoria SD) se crea dos carpetas: la primera para la base de datos, y la otra para guardar las fotos tomadas al momento del levantamiento de datos.

Una vez ingresado a la planificación en el sistema se genera la base móvil con la herramienta de datos SQL y luego se copia a la PocketPC.

1.4.2.2 Recolección de Datos

Es el levantamiento físico de los datos realizado por los "Gestores de Campo" en el lugar asignado para el efecto, para lo cual se realiza el siguiente procedimiento:

- Asignar a los “Gestores de Campo” una PocketPC y el plano físico de la ruta definiendo direcciones.
- Los gestores de campo se trasladan al lugar donde se les ha asignado la ruta.
- Se procede a censar los medidores señalando el punto de carga en el plano físico.
- Los gestores de Campo recolectan los siguientes datos mediante la aplicación móvil:
    - Datos del propietario del medidor.
    - Fotografía de la cédula del propietario de frente y reverso.
    - Dirección del Catastro.
    - Datos del medidor (número del medidor, marca, etc.)
    - Fotografía el medidor.
    - Estatus del medidor (conexiones clandestinas en el caso que existan).
    - Posición geográfica del medidor usando el GPS.
    - Fotografía de la casa (o terreno) del catastro.

Nota: En caso que el gestor de campo encontrara algún obstáculo en el recorrido podría cambiar su sentido según le convenga.

1.4.2.3 Respaldo de Datos Censados

Esta actividad se realiza luego de que el “Gestor de Campo” entrega la recolección de datos; se respalda la base de datos y las fotos tomadas copiándolas en la carpeta creada para el efecto.

En la Figura 9 se muestra la secuencia de las actividades descritas:

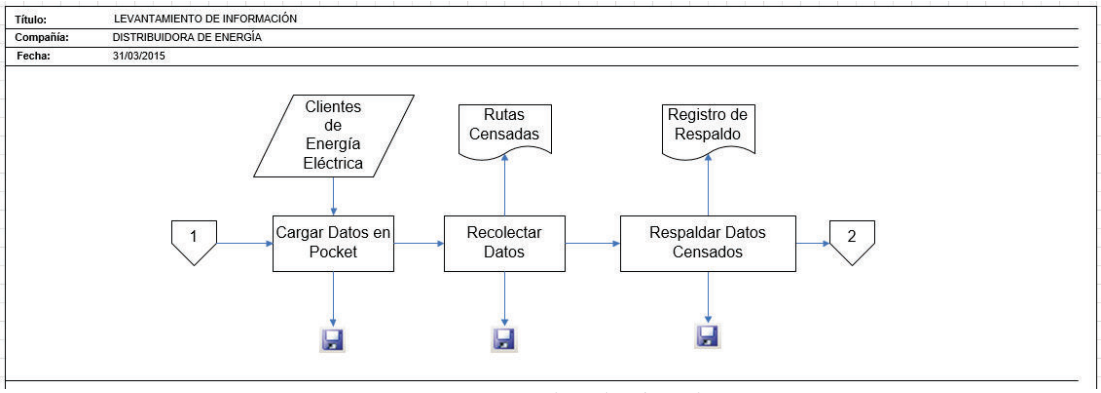

Figura 9 – Levantamiento de Información
Fuente: Empresa de servicios "XYZ"

1.4.3 PROCESAMIENTO DE INFORMACIÓN

1.4.3.1 Replicación de Datos Mediante la base Móvil

Es el traslado de la información de la base de datos móvil al Sistema de Catastro Automatizado.

Es probable que con el proceso de replicación de datos ocurran errores, los mismos que pueden ser tratados de la siguiente manera:

- Buscar la solución de acuerdo un análisis de información previa, por ejemplo:
    a. Errores de digitación con el número de medidor.
    b. Diferencia de nombres del cliente.
    c. Geocódigo duplicado (dos personas censan distintos lugares con la misma ruta lógica - entraron con el mismo usuario).
- Ejecutar la solución más conveniente, por ejemplo, validar el número de medidor con la fotografía para aceptar el registro.
- Documentar el problema y la solución aplicada.

En la Figura 10 se muestra la secuencia de las actividades descritas:

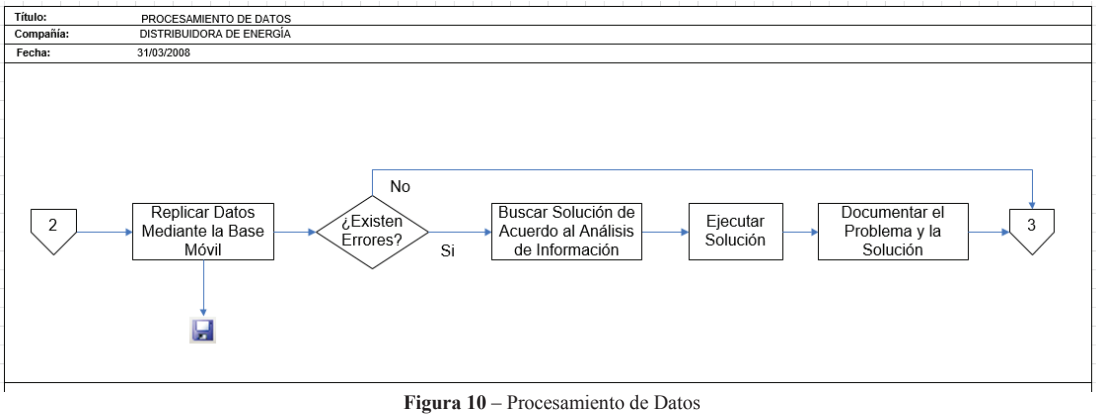

Figura 10 – Procesamiento de Datos
Fuente: Empresa de servicios "XYZ"

1.4.4 AFINAMIENTO DE LA INFORMACIÓN

1.4.4.1 Validación de Rutas en el Campo

Es la verificación de los datos tomados en primera instancia, recorriendo nuevamente la ruta. En el caso de encontrar inconsistencias ya sea con el recorrido o por varios obstáculos, se puede modificar la ruta y reordenar el listado de la misma. La validación de las rutas en el campo se realiza mediante los siguientes pasos:

- **Planificación de Rutas:** es re-secuenciar las rutas censadas anteriormente en una recolección de datos, para esto se debe ingresar al sistema en el módulo "Administrar" donde se procede a seleccionar el "Gestor de Campo" al cual se le va a asignar un sector y se establece la secuencia.
- **Cargar Datos a la Pocket:** es el almacenamiento de la base de datos en la PocketPC, con la planificación de las rutas para la recolección de datos e información base del cliente. En la PocketPC (memoria SD) se crean dos carpetas; la primera para la base de datos, y la otra para guardar las fotos tomadas al momento del levantamiento de información.
  Una vez ingresado a la planificación en el sistema se genera la base móvil con la herramienta de datos SQL y se la copia a la PocketPC.

- **Recolección de Datos:** es el levantamiento físico de los datos realizado por los “Gestores de Campo” en el lugar asignado para el efecto, considerando el siguiente procedimiento:
    - Asignar a los Gestores de Campo una PocketPC y el plano físico de la ruta definiendo direcciones.
    - Los Gestores de Campo se trasladan al lugar donde se les ha asignado la ruta.
    - Los Gestores de Campo comenzarán a verificar los datos comparándolos con los que fueron registrados en la anterior Recolección de Datos en el listado de ruta.
    - En el caso de encontrar predios que no han sido censados, se procederá a realizar un nuevo censo tomando los siguientes datos:
        - Se llena el listado de ruta con los datos correspondientes.
        - Se marca el punto de carga en el plano de la ruta.
    - Los Inspectores de Campo mediante la PocketPC recolectan los siguientes datos mediante la aplicación móvil:
        - Datos del propietario del medidor.
        - Fotografía de la cédula del propietario de frente y reverso.
        - Dirección del Catastro.
        - Datos del medidor (número del medidor, marca, etc)
        - Fotografía del medidor.
        - Estatus del medidor (conexiones clandestinas en el caso que existan).
        - Posición geográfica del medidor usando el GPS.
        - Fotografía de la casa (o terreno) del catastro.
    - Se entrega al Líder del Proyecto el listado de ruta, el plano y la PocketPC con las respectivas novedades encontradas.

Nota: En caso de que el gestor de campo encontrara un obstáculo en el recorrido podría cambiar el sentido del recorrido según convenga.

1.4.4.2 Respaldo de Datos Censados

Es la actividad que se realiza luego de que el “Gestor de Campo” entrega la recolección de datos, se respalda la base de datos y las fotos tomadas copiándolas en la carpeta creada para el efecto.

1.4.4.3 Replicación de Datos Mediante la base Móvil

Es el traslado de la información de la base de datos móvil al sistema de “Censos de Información Comercial”. Es probable que con el proceso de replicación de datos ocurran errores los cuales se resuelven de la siguiente manera:

- Buscar la solución de acuerdo a un análisis de información previo, por ejemplo:
    a. Errores de digitación con el número de medidor.
    b. Diferencia de nombres del cliente.
    c. Geocódigo duplicado (dos personas censan distintos lugares con la misma ruta lógica - entraron con el mismo usuario).
- Ejecutar la solución más conveniente, por ejemplo, validar el número de medidor con la fotografía para aceptar el registro.
- Documentar el problema y la solución aplicada.

1.4.4.4 Verificación y Validación de Datos (Sistema vs. Escritorio)

Es la validación de los datos de catastro obtenidos en la recolección de datos con los que tiene la Distribuidora de Energía; se corrobora que los datos del propietario del medidor estén completos.

1.4.4.5 Generación de Reportes

Es la obtención de reportes de las rutas generadas, el total de censos diarios por usuario, comparación del status, novedades, conexiones clandestinas y mala

ubicación de medidores. Estos reportes sirven para llevar un control del trabajo que se va desarrollando en el proyecto.

En la Figura 11 se muestra la secuencia de las actividades antes descritas.

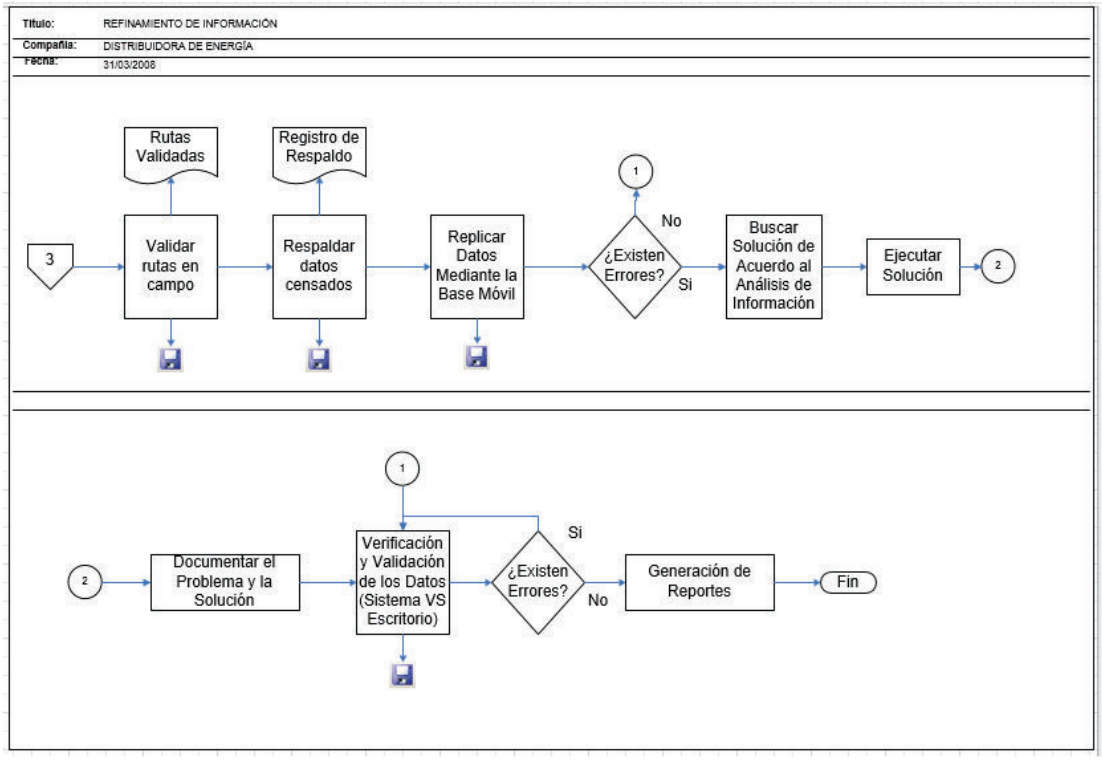

Figura 11 – Refinamiento de Información
Fuente: Empresa de servicios "XYZ"

1.4.5 RED

Para realizar el desarrollo de los procesos "Levantamiento de Información", "Procesamiento de Información" y "Afinamiento de Información" para la obtención de los "Censos de Información Comercial" se ha implementado una topología de red tipo estrella, la cual consta de un Servidor de Impresión, un Servidor de Base de Datos, un Servidor de Aplicaciones y un Servidor de Dibujo como se muestra en la Figura 12:

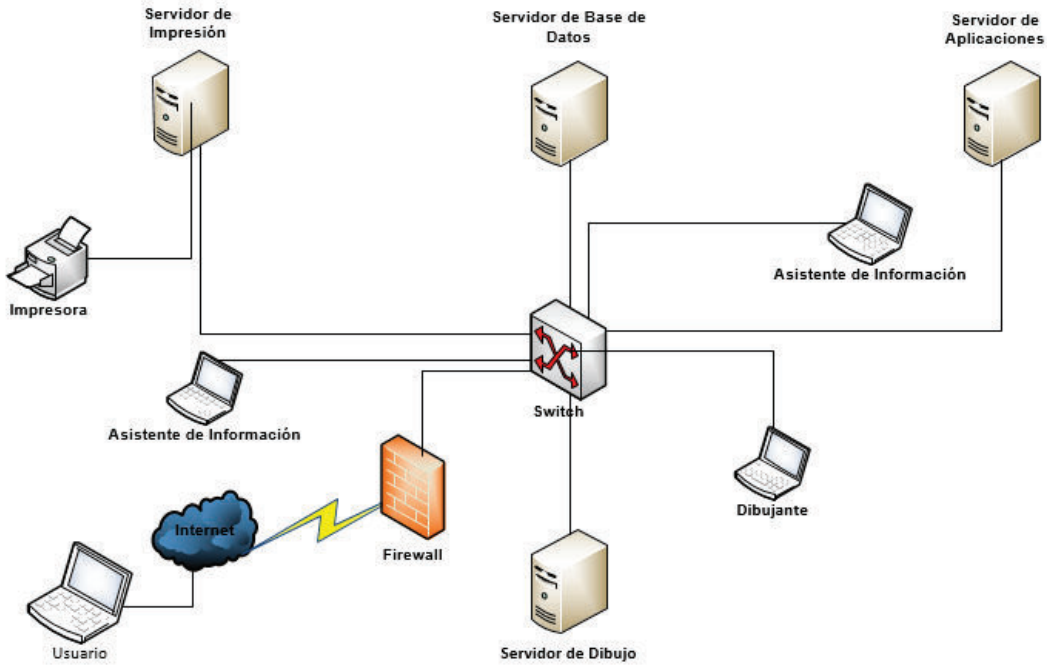

Figura 12 – Topología de Red
Fuente: Empresa de servicios "XYZ"

El siguiente punto crítico en el desarrollo del proceso mencionado es la descripción de los activos de información que intervienen, la misma que se desarrolla a continuación:

1.4.6 ACTIVOS DE INFORMACIÓN

Para realizar un estudio detallado del servicio de "Censos de Información Comercial", se describirán los activos que posee la empresa para llevar a cabo estas actividades.

1.4.6.1 Inventario de Recursos Humanos

Para definir el Inventario de Recursos Humanos la empresa plantea una estructura organizacional jerárquica en un escenario hipotético, para obtener un promedio de 120.000 censos de información en un tiempo estimado de 5 meses a

nivel de una provincia donde una Distribuidora de Energía brinda sus servicios. La estructura se describe a continuación en la Figura 13:

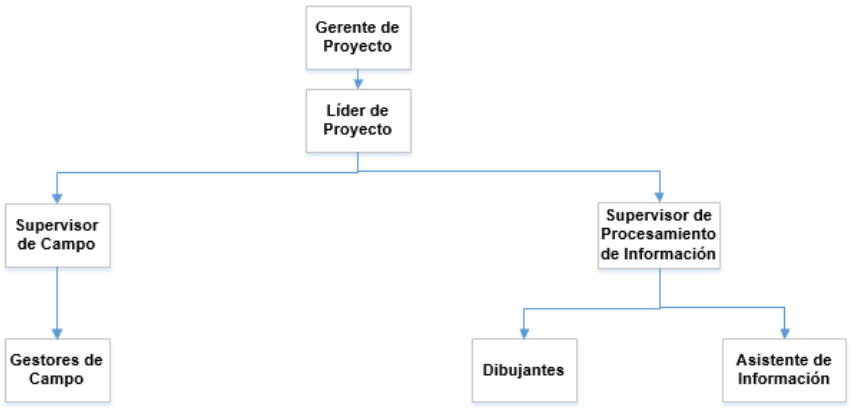

Figura 13 – Estructura Jerárquica Organizacional del Proceso
Fuente: Empresa de servicios "XYZ"

En la realización de las actividades del servicio, la empresa tiene a su disposición 15 personas, distribuidos como se muestra en la Tabla 1:

CARGO	NÚMERO DE EMPLEADOS
Gerente de Proyecto	1
Líder de Proyecto	1
Supervisor de Campo	1
Supervisor de Procesamiento de Información	1
Gestores de Campo	15
Dibujantes	2
Asistentes de Información	2
TOTAL DE EMPLEADOS	**23**

Tabla 1 - Inventario de Recursos Humanos.
Fuente: Empresa de servicios "XYZ"

Se estima un promedio de 80 encuestas diarias realizadas por gestor de campo, teniendo en cuenta que son 22 días laborables mensuales. Tomando en cuenta esta información, en cinco meses se obtendrían aproximadamente 132000 encuestas.

1.4.6.2 Inventario de Hardware y Software

Para desarrollar las actividades del servicio la empresa posee algunos servidores y estaciones de trabajo descritos a continuación:

NOMBRE	MODELO	CARACTERÍSTICAS	SW. INSTALADO
Servidor de Impresión	HS23	CPU: 4 Cores RAM :4 GB STORAGE: 375	Server 2008
Servidor de Bases de Datos	HS23	CPU: 4 Cores RAM :8 GB STORAGE: 375	Server 2008 SQL Server 2008 R2 Sistema de Catastro
Servidor de Aplicaciones	HS23	CPU: 4 Cores RAM :8 GB STORAGE: 375	Server 2008 Plataforma .NET Sistema Catastral
Servidor de Dibujo	HS23	CPU: 4 Cores RAM :8 GB STORAGE: 375	Server 2008 ArcGis 10

Tabla 2 - Inventario de Hardware y Software de Servidores.
Fuente: Empresa de servicios "XYZ"

NOMBRE	MODELO	CARACTERÍSTICAS	SW INSTALADO
Dibujante #1	Sony VAIO VPC-CW1S1E	CPU: 4 Cores RAM :4 GB STORAGE: 375 GB	Windows 7
Dibujante #2	Sony Vaio VPC-CW1S1E	CPU: 4 Cores RAM :4 GB STORAGE: 375 GB	Windows 7
Líder del proyecto	Sony VAIO T	CPU: 8 Cores RAM :8 GB STORAGE: 250 GB	Windows 7
Asistente de Información #1	Acer Ferrari One.	CPU: 2 Cores RAM :3 GB STORAGE: 500 GB	Windows 7
Asistente de Información #2	Acer Ferrari One.	CPU: 2 Cores RAM :3 GB STORAGE: 500 GB	Windows 7

Tabla 3 - Inventario de Hardware y Software de Estaciones de Trabajo.
Fuente: Empresa de servicios "XYZ"

DISPOSITIVO	MODELO	NÚMERO DE EQUIPOS
Switch	D-LINK	1

Tabla 4 - Inventario de Equipos de Red.
Fuente: Empresa de servicios "XYZ"

DISPOSITIVO	MODELO	NÚMERO DE EQUIPOS
Impresora	Epson L200	1

Tabla 5 - Inventario de Equipos de Impresión.
Fuente: Empresas de servicios "XYZ"

DISPOSITIVO	MODELO	NÚMERO DE EQUIPOS
PDA	Honeywell Dolphin 6000	15
GPS	Wintec WBT-201	15

Tabla 6 - Inventario de Dispositivos Móviles.
Fuente: Empresas de servicios "XYZ"

Para mayor información de las características de PocketPC, GPS, impresora y Switch revisar el **"Anexo B - Caracterización de los dispositivos computacionales de trabajo utilizados en el desarrollo del servicio de "Censos de Información Comercial".**

Finalmente, el activo y herramienta fundamental para realizar el trabajo operativo del levantamiento de información catastral, llamado "Censos de Información Comercial", será descrito a continuación:

1.4.6.3 Sistema de Catastro Automatizado (Sistema de Censos de Información Comercial)

"Es un sistema de información que utiliza una base de datos alfanumérica y cartográfica en formato digital, en el que se registran todos los datos e información necesarios acerca de los predios y clientes reales, factibles y potenciales, respecto a la disponibilidad del servicio de energía, así como de la ubicación geográfica exacta del predio a través de códigos numéricos predefinidos y georreferenciados"[3]. En la Figura 14 se muestra su arquitectura:

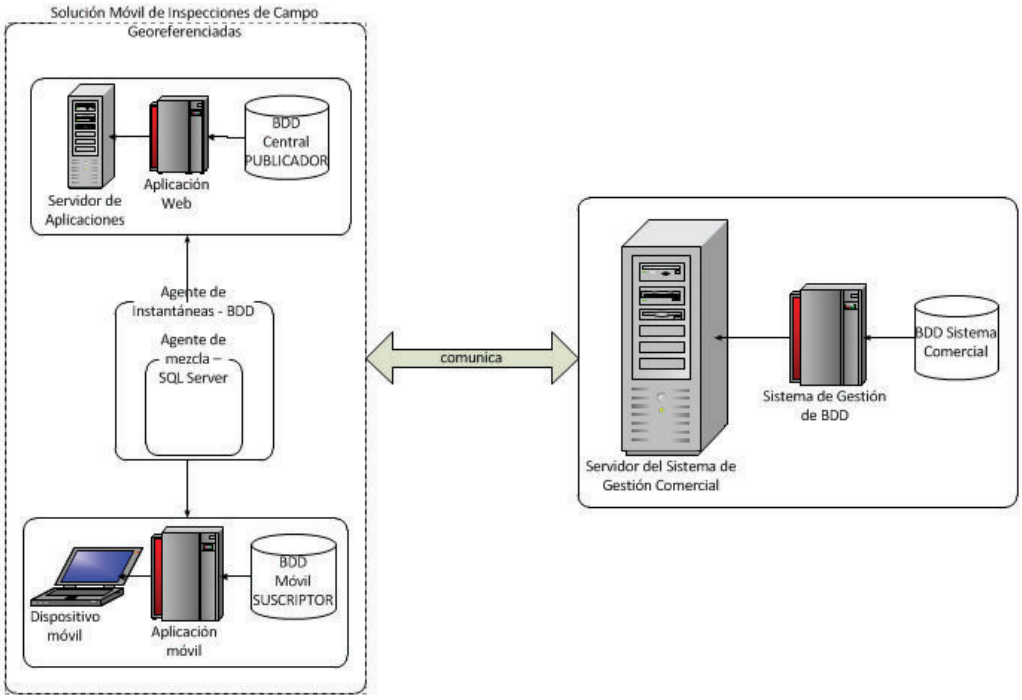

Figura 14 – Arquitectura del Sistema Catastral
Fuente: Empresa de servicios "XYZ"

Como se ha podido apreciar hasta el momento, el desarrollo del servicio "Censos de Información Comercial" comprende un proceso complejo donde intervienen diversos factores, los cuales en un sentido general se pueden dividir en humanos

[3] Fuente: Proyecto de Titulación: *"Solución Móvil para Facturación y Recaudación en un Ambiente Distribuido"*, pág. 71. Escuela Politécnica Nacional, Ayala Vargas William Raúl. Ing. Juan Herrera, MSc, 2010.

y tecnológicos; a pesar de esta clasificación, los activos no son pocos y el nivel de afectación de cada uno de estos al desarrollo del servicio puede ser variado, por esta razón se ha optado clasificarlos dependiendo de su criticidad para el proceso, esto es, en función de su Nivel de Importancia.

1.4.7 NIVEL DE IMPORTANCIA DE ACTIVOS DE INFORMACIÓN (NI)

Para evaluar los riesgos del servicio "Censos de Información Comercial" se deberá definir el nivel de importancia de los activos utilizados basándonos en la confidencialidad, integridad y disponibilidad de información, definidas a continuación[4]:

- **"Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad:** acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando se requiera."

Para poder evaluar el nivel de importancia de los activos se definirán escalas de confidencialidad (Tabla 7), integridad (Tabla 8) y disponibilidad (Tabla 9):

ESCALA DE CONFIDENCIALIDAD		
NIVEL	**CARACTERIZACIÓN**	**DESCRIPCIÓN**
1	Bajo	Cualquier persona puede tener acceso a esta información.
		En caso que la información sea divulgada, no existiría ninguna repercusión en el servicio.
2	Medio	Sólo empleados de la empresa puede tener acceso a esta información.
		En caso que la información sea divulgada, las consecuencias en el servicio serían moderadas.
3	Alto	Sólo el gerente y el líder del proyecto de la empresa pueden tener acceso a esta información.
		En caso que la información sea divulgada, las consecuencias en el servicio serían altas.
4	Muy Alto	Sólo el gerente del proyecto de la empresa puede tener acceso a esta información.

[4] Fuente: *"ISO 27000.ES EL PORTAL DE ISO 27001 EN ESPAÑOL"*. http://www.iso27000.es/sgsi.html

ESCALA DE CONFIDENCIALIDAD		
NIVEL	**CARACTERIZACIÓN**	**DESCRIPCIÓN**
		En caso que la información sea divulgada, las consecuencias en el servicio serían muy altas.

Tabla 7- Escala de Confidencialidad.
Fuente: Proyecto de Titulación "Desarrollo de un plan de continuidad del negocio de TI para el ISP "Megadatos S.A." de la ciudad de Quito", pág.41-43. Escuela Politécnica Nacional. Taxi Cali Glenda Soraya. Ing. Gustavo Samaniego, MSc. 2013

ESCALA DE INTEGRIDAD		
NIVEL	**CARACTERIZACIÓN**	**DESCRIPCIÓN**
1	Bajo	Sí esta información es modificada, no existiría ninguna repercusión en el servicio.
2	Medio	Sí esta información es modificada, las consecuencias en el servicio serían moderadas.
3	Alto	Sí esta información es modificada, las consecuencias en el servicio serían considerables.
4	Muy Alto	Sí esta información es modificada, las consecuencias en el servicio serían muy notables.

Tabla 8- Escala de Integridad.
Fuente: Proyecto de Titulación "Desarrollo de un plan de continuidad del negocio de TI para el ISP "Megadatos S.A." de la ciudad de Quito", pág.41-43. Escuela Politécnica Nacional. Taxi Cali Glenda Soraya. Ing. Gustavo Samaniego, MSc. 2013

ESCALA DE DISPONIBILIDAD		
NIVEL	**CARACTERIZACIÓN**	**DESCRIPCIÓN**
1	Bajo	Sí esta información no se encuentra disponible, las consecuencias en el servicio serían mínimas.
2	Medio	Sí esta información no se encuentra disponible, las consecuencias en el servicio serían moderadas.
3	Alto	Sí esta información no se encuentra disponible, las consecuencias en el servicio serían considerables.
4	Muy Alto	Sí esta información no se encuentra disponible, las consecuencias en el servicio serían muy notables.

Tabla 9 - Escala de Disponibilidad.
Fuente: Proyecto de Titulación "Desarrollo de un plan de continuidad del negocio de TI para el ISP "Megadatos S.A." de la ciudad de Quito", pág.41-43. Escuela Politécnica Nacional. Taxi Cali Glenda Soraya. Ing. Gustavo Samaniego, MSc. 2013

Para poder calcular el NI de los activos de información se debe hacer uso de la Ecuación 1:

$$NI = Confidencialidad * Integridad * Disponibilidad$$

Ecuación 1 - Nivel de Importancia de los Activos de Información.
Fuente: Proyecto de Titulación "Desarrollo de un plan de continuidad del negocio de TI para el ISP "Megadatos S.A." de la ciudad de Quito", pág.41-43. Escuela Politécnica Nacional. Taxi Cali Glenda Soraya. Ing. Gustavo Samaniego, MSc. 2013

Después de categorizar en los puntos anteriores la confidencialidad, integridad y disponibilidad, se continuará con el NI de los activos de información del servicio, como se indica en la Tabla 10:

ESCALA DE NIVEL DE IMPORTANCIA		
VALOR	**CARACTERIZACIÓN**	**DESCRIPCIÓN**
1 a 4	Bajo	El Activo de información tiene una importancia baja para precautelar la seguridad de la información del servicio.
5 a 16	Medio	El Activo de información tiene una importancia media para precautelar la seguridad de la información del servicio.
17 a 36	Alto	El Activo de información tiene una importancia alta para precautelar la seguridad de la información del servicio.
37 a 64	Muy Alto	El Activo de información tiene una importancia muy alta para precautelar la seguridad de la información del servicio.

Tabla 10 - Escala del Nivel de Importancia de los Activos de información.
Fuente: Proyecto de Titulación "Desarrollo de un plan de continuidad del negocio de TI para el ISP "Megadatos S.A." de la ciudad de Quito", pág.41-43. Escuela Politécnica Nacional. Taxi Cali Glenda Soraya. Ing. Gustavo Samaniego, MSc. 2013

La calificación de la criticidad de los activos del servicio para la seguridad de información ha sido asignada en función de entrevistas previas al Líder de Proyecto, quien aportó fundamentalmente su conocimiento y experiencia laboral con este tipo de proyectos en lo referente a la gestión de la integridad, disponibilidad y confidencialidad de información.

Para la evaluación de los riesgos se necesitará saber el NI de los activos de información, y así reconocer su criticidad en la gestión de seguridad de información, la cual se describe en la Tabla 11:

NIVEL DE IMPORTANCIA DE LOS ACTIVOS DE INFORMACIÓN						
ACTIVO	**DESCRIPCIÓN**	**C**	**I**	**D**	**NI**	
Servidores	Servidor de Impresión	2	4	2	16	Medio
	Servidor de Bases de Datos	4	4	4	64	Muy Alto
	Servidor de Dibujo	4	4	4	64	Muy Alto
	Servidor de Aplicaciones	4	4	4	64	Muy Alto
Estaciones de Trabajo	Dibujante #1	2	3	4	24	Medio
	Dibujante #2	2	3	4	24	Medio
	Líder del proyecto	4	4	4	64	Muy Alto
	Asistente de Informacion#1	2	3	3	18	Alto
	Asistente de Información#2	2	3	3	18	Alto
Redes	Switch	2	4	4	32	Alto
Equipo Computacional Secundario	Impresora	2	2	2	8	Medio
Aplicaciones	Sistema Catastral	4	4	4	64	Muy Alto
Dispositivos Móviles	PDA	3	4	4	48	Muy Alto
	GPS	3	4	4	48	Muy Alto

Tabla 11- Nivel de Importancia de los Activos de información del servicio de "Censos de Información Comercial".
Fuente: Empresa de servicios "XYZ"

CAPÍTULO 2. ANÁLISIS Y EVALUACIÓN DE RIESGOS

En el capítulo anterior, se han descrito los procesos, tecnologías y en general todos los activos que intervienen en el desarrollo del servicio de "Censos de Información Comercial", así como el nivel de importancia de cada uno en función de la administración de la información; también se ha explicado la importancia de un SGSI para el servicio y la metodología de implementación del mismo.

En este nuevo capítulo, se detallará la identificación de todas las amenazas y vulnerabilidades inherentes a un servicio de esta naturaleza, utilizando una metodología de evaluación de riesgos previamente escogida en función de un análisis comparativo. También se analizará el nivel de impacto y riesgo que implican estas vulnerabilidades y los controles para su mitigación.

2.1. IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

Para realizar la identificación de las amenazas y vulnerabilidades primero se definirá la metodología de evaluación de riesgos a utilizar, para ello se realizará un análisis comparativo de las metodologías más utilizadas.

2.1.1 ANÁLISIS Y COMPARACIÓN ENTRE METODOLOGÍAS DE EVALUACIÓN DE RIESGO

2.1.1.1 Activos Claves para la Evaluación

Para determinar la metodología de evaluación de riesgos más adecuada, se realizará un análisis comparativo entre NIST 800-30, OCTAVE y MAGERIT en función de los elementos y activos de TI que intervienen en el servicio, los cuales son:

- Hardware (Hw).

- Software (Sw).
- Bases de datos (BD).
- Redes y Telecomunicaciones (R&C).
- Recursos Humanos (RH).
- Legal.
- Servicios.

El tipo de evaluación a realizarse es cuantitativa, es decir, se asignarán valores porcentuales en función del nivel de control y cumplimiento de las metodologías mencionadas sobre los activos del servicio. La Tabla 12 describe de forma detallada las escalas de calificación que se utilizarán:

PORCENTAJE (%) DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO	DESCRIPCIÓN
0% a 40%	Nulo o bajo	El activo o recurso no cumple con los requisitos o no cuenta con los controles de seguridad de información necesarios.
41% a 70%	Medio	Los controles de seguridad implementados no son suficientes para mantener un alto nivel de seguridad de información.
71% a 100%	Alto	Los activos o recursos cuentan con los controles suficientes para poder controlar la seguridad de la información de manera efectiva.

Tabla 12 - Escala de Medición de Cumplimiento de Controles de Seguridad de Información
Fuente: Los Autores

2.1.1.2 Metodología de Evaluación de Riesgos

2.1.1.2.1 Evaluación de Riesgos

Para evaluar de manera adecuada el riesgo y minimizar su impacto en el servicio, se establece tres etapas:

a. **Identificación de riesgos:** contempla la búsqueda de todas las posibles fuentes de riesgos que pueden afectar al servicio; existe una infinidad de fuentes de riesgos potenciales, en el presente proyecto de titulación serán analizadas y clasificadas en función de la realidad del servicio.
b. **Análisis de riesgos:** luego de identificadas las fuentes, se realizará una valoración en función de la criticidad de afectación de dichos riesgos al

desarrollo del servicio. La probabilidad de ocurrencia y el impacto de los riesgos son factores clave al momento de realizar este análisis.

c. **Respuesta y manejo de riesgos:** son acciones y medidas necesarias que se deben implementar al servicio, de manera que se puedan controlar y mitigar los riesgos a niveles aceptables.

2.1.1.3 Tipos de Metodologías de Evaluación de Riesgos

Para realizar la evaluación de riesgos de manera aceptable, existen varias metodologías que pueden ser acopladas sin problemas al desarrollo de un SGSI utilizando ISO 27001:2013, entre las principales están:

2.1.1.3.1 NIST 800-30 – Guía de Administración de Riesgos para Sistemas de Tecnologías de Información

Esta metodología de evaluación de riesgos se realiza en dos etapas:

a. **VALORACIÓN DE RIESGOS:** se desarrolla siguiendo los siguientes pasos:
   - **Paso 1.** Caracterización del servicio.
   - **Paso 2.** Identificación de amenazas.
   - **Paso 3.** Identificación de vulnerabilidades.
   - **Paso 4.** Análisis de controles.
   - **Paso 5.** Determinación de probabilidades.
   - **Paso 6.** Análisis de impacto.
   - **Paso 7:** Determinación del riesgo.
   - **Paso 8:** Recomendación de controles.
   - **Paso 9:** Documentación de resultados.
b. **MITIGACIÓN DE RIESGOS:** para lo cual se debe determinar:
   - Opciones de mitigación de riesgos.
   - Estrategia de mitigación de riesgos.
   - Enfoque para la implementación de controles.

- Categorías de controles.
- Análisis costo – beneficio.
- Riesgos residuales.

NIST 800-30 nos da un enfoque bastante completo para la evaluación de riesgos en la parte técnica y en lo referente a servicios. Por otro lado, el análisis de aspectos legales es bastante amplio en cuanto a revisiones, pero no profundiza al nivel de proponer implementaciones.

2.1.1.3.2 OCTAVE – Evaluación Operacional de Amenazas, Riesgos y Vulnerabilidades Críticas

Esta metodología comprende tres fases:

I. **FASE 1. CONSTRUIR PERFILES DE LAS POSIBLES AMENAZAS EN FUNCIÓN DE LOS ACTIVOS:** esta fase se despliega mediante los siguientes procesos:
   - **Proceso 1.** Identificación del conocimiento de la administración.
   - **Proceso 2.** Identificación del conocimiento del área operativa.
   - **Proceso 3.** Identificación del conocimiento del personal técnica.
   - **Proceso 4.** Creación de perfiles de amenazas.

II. **FASE 2. IDENTIFICAR VULNERABILIDADES EN LA INFRAESTRUCTURA:** los procesos que se desarrollan en esta fase son:
   - **Proceso 5.** Identificación de componentes clave.
   - **Proceso 6.** Evaluación de componentes seleccionados.

III. **FASE 3. DESARROLLAR PLANES Y ESTRATEGIAS DE SEGURIDAD:** se compone de dos procesos:
   - **Proceso 7.** Dirección del análisis del riesgo.
   - **Proceso 8.** Desarrollo de la estrategia de gestión de riesgo.

Esta metodología, de manera similar a NIST 800-30, se enfoca principalmente en los aspectos técnicos del proyecto para la evaluación de riesgos, dejando al

aspecto legal en un ámbito secundario, llegando a realizar solamente la parte de análisis.

2.1.1.3.3 MAGERIT – Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Esta metodología se enfoca esencialmente en la evaluación de riesgos en función de los activos de TI utilizados para el desarrollo del servicio; el desarrollo de esta metodología se describe en los siguientes libros:

I. **MÉTODO:** en este libro se describen los pasos fundamentales para llevar a cabo la evaluación de riesgos de seguridad de información del servicio; también define formalmente las bases teóricas y prácticas de los procedimientos a seguir para realizar la gestión mencionada.
II. **CATÁLOGO DE ELEMENTOS:** estos elementos sirven principalmente para clasificar y categorizar todos los elementos de TI utilizados en el servicio, y las guías para desarrollar los reportes de observaciones y hallazgos respecto a riesgos y controles de seguridad de información.
III. **GUÍA DE TÉCNICAS:** finalmente este libro describe las técnicas de búsqueda, análisis y cuantificación de riesgos, así como técnicas para desarrollar la evaluación más adecuada según sea la realidad del servicio.

A diferencia de las metodologías mencionadas anteriormente, MAGERIT sí considera al aspecto legal como una parte sustancial para la evaluación de riesgo, referenciando leyes y normas para el manejo seguro de información. Aunque la evaluación de la parte legal se realiza tomando en función de leyes y normas españolas, puede servir como una guía para el ambiente donde se desarrolle el servicio.

De forma general, se puede decir que las tres metodologías funcionan bien al momento de trabajar en el ámbito técnico y operativo del servicio. En lo referente al ámbito legal, MAGERIT ofrece una evaluación más completa en comparación

NIST 800-30 y OCTAVE, porque no se limita a realizar análisis y estudios referentes al riesgo de seguridad de información, sino también abarca referencias y sugerencias para actuar según el caso.

En la Tabla 13 se encuentra un análisis comparativo entre las diferentes metodologías de evaluación de riesgos, en función del nivel de cobertura que cada una de estas realiza según los activos del servicio:

Metodología	Nivel de Cobertura						
	Hardware	Software	Bases de Datos	Redes y Telecomunicaciones	Recursos Humanos	Legal	Servicios
NIST 800-30	75%	75%	75%	75%	75%	50%	75%
OCTAVE	75%	75%	75%	75%	75%	25%	50%
MAGERIT	75%	75%	75%	75%	75%	75%	75%

Tabla 13 – Nivel de Cobertura de las metodologías de gestión de riesgo analizadas en función de los activos clave del servicio.
Fuente: Proyecto de Titulación: "Guía de Análisis de Gestión de Riesgos en la Adquisición e Implantación de Equipamiento y Servicios de Tecnologías de Información y Comunicaciones para Proyectos de Alcance Nacional". pág. 42. Escuela Politécnica Nacional. Carrillo Sánchez Jonathan Patricio. PhD. Enrique Mafla. 2012.

En el presente trabajo de titulación, se utilizará la metodología de evaluación de riesgos NIST 800-30, por la siguiente razón:

En la tabla 13, se puede ver que aunque las tres metodologías trabajan bien en función de los elementos que intervienen en el desarrollo del servicio, MAGERIT y NIST 800-30 llevan la ventaja respecto a OCTAVE en cuanto a la evaluación de aspectos legales y servicios. Ahora, al tratarse de la implementación de un SGSI en un servicio eminentemente técnico, se escoge NIST 800-30 para realizar la evaluación de riesgos con mayor enfoque en la parte tecnológica.

2.1.2 IMPLEMENTACIÓN DE LA METODOLOGÍA SELECCIONADA

Ahora que se ha seleccionado a NIST 800-30 como la metodología para evaluar el riesgo en el servicio, el proceso de implementación se realizará tomando en cuenta los siguientes conceptos:

2.1.2.1 Organización, Activos, Vulnerabilidades y Amenazas

La implementación efectiva de NIST 800-30 debe contemplar un delineamiento preciso de la organización responsable del desarrollo del servicio, los activos implicados en la adquisición y tratamiento de la información (punto 1.4.6 *"ACTIVOS DE INFORMACIÓN"*), y las vulnerabilidades y amenazas (puntos 2.1.3 *"IDENTIFICACIÓN DE AMENAZAS"* y 2.1.4 *"IDENTIFICACIÓN DE VULNERABILIDADES"*) que implica la interacción entre los factores mencionados, para reconocer de forma clara los riesgos (punto 2.*3 "DETERMINACIÓN DEL RIESGO"*) que pueden afectar a la seguridad de información.

2.1.2.2 Tratamiento de Riesgos

Una vez identificados todos los factores implicados en el desarrollo del servicio y sus riesgos inherentes, se determinarán los controles necesarios para su gestión, de manera que su impacto sea mínimo a la seguridad de la información. Estos controles serán escogidos a partir del análisis realizado de la probabilidad e impacto de los riesgos de seguridad de información (puntos 2.2 *"ANÁLISIS DE IMPACTO, PROBABILIDAD Y CONTROLES"*, 2.3 *"DETERMINACIÓN DEL RIESGO"*, 2.4 *"RECOMENDACIONES DE CONTROL"* y 2.5 *"ANÁLISIS DE REQUERIMIENTOS DE CONTROL")* y en función de los controles existentes en la ISO 27001:2013.

2.1.2.3 Proceso de Implementación de NIST 800-30 para el Tratamiento de Riesgos

Las etapas de NIST 800-30 para evaluar el riesgo son:

a. **VALORACIÓN DE RIESGOS:** se determina a qué nivel puede verse afectado el servicio por las posibles amenazas existentes y su riesgo asociado. La valoración de riesgos se desarrolla en los siguientes pasos:
    - **Paso 1. Caracterización del sistema:** se define el alcance de los riesgos en función de los sistemas y procesos que intervienen en el

desarrollo del servicio, para esto es necesario definir su alcance y límites. El resultado de este paso, es una visión panorámica de la realidad actual del servicio.

- **Paso 2. Identificación de amenazas:** para lo cual se reconoce:
  - Todas las posibles fuentes de amenazas
  - Vulnerabilidades potenciales
  - Controles existentes
- **Paso 3. Identificación de vulnerabilidades:** que forma parte del análisis de amenazas identificadas que pueden afectar al desarrollo del servicio.

  Este paso tiene como salida una lista de las todas las amenazas reales y potenciales que pueden ocasionar vulnerabilidades; esta lista se obtiene como resultado de realizar:
  - Búsquedas de fuentes de vulnerabilidades
  - Testing de la seguridad del proceso
  - Desarrollo de un checklist de requerimientos de seguridad
- **Paso 4. Análisis de controles:** se evalúan posibles controles ya implementados, con la finalidad de minimizar la probabilidad de que una amenaza explote una o varias vulnerabilidades. Al terminar este paso, se obtiene una lista de todos los posibles controles que se pueden implementar, para reducir la probabilidad de que las amenazas identificadas exploten las vulnerabilidades del servicio.
- **Paso 5. Determinación de probabilidades:** esto se realiza considerando:
  - La motivación y capacidad de las fuentes de amenazas.
  - La naturaleza de la vulnerabilidad.
  - La existencia y efectividad de los controles actuales.

  Este paso da como resultado un ranking de probabilidad de ocurrencia de amenazas.
- **Paso 6. Análisis de impacto:** es el punto de partida para determinar el nivel de impacto que puede ocasionar la explotación de una

vulnerabilidad. En términos generales, las posibles consecuencias están abarcadas dentro de los siguientes dominios:

- Pérdidas de integridad de la información.
- Pérdidas de disponibilidad de servicios.
- Pérdidas de confidencialidad.

- **Paso 7. Determinación del riesgo:** se expresa en función de:
  - La probabilidad de una amenaza explotando una vulnerabilidad.
  - La magnitud del impacto.
  - La suficiencia de los posibles controles para reducir o eliminar el riesgo.

  Este paso da como resultado el nivel de riesgo que corre el servicio.
- **Paso 8. Recomendación de controles:** de manera que estos ayuden a mitigar el riesgo que corre el proceso a niveles manejables. Los controles recomendados deben escogerse en función de los siguientes factores:
  - Efectividad de los controles recomendados.
  - Legislación y regulación.
  - Políticas organizacionales.
  - Impacto operacional.
  - Seguridad y confiabilidad.
- **Paso 9. Documentación de resultados:** para darle un carácter oficial al trabajo hecho y los resultados obtenidos.

b. MITIGACIÓN DE RIESGOS: una vez determinados los controles de riesgos en la etapa anterior, se realizarán las actividades de priorización, evaluación e implementación de los mismos, para lo cual se determina:

- **Opciones de mitigación de riesgos:** se tienen las siguientes opciones:
  - **Admisión del riesgo:** es reconocer la existencia de riesgos que pueden afectar negativamente al desarrollo del servicio, de manera que se estudien e implementen las medidas de control adecuadas.
  - **Prevención del riesgo:** esto se logra atacando directamente la fuente del riesgo.

- **Limitación del riesgo:** es decir, minimizar el impacto de una amenaza explotando una vulnerabilidad utilizando los controles adecuados.
- **Planeación del riesgo:** desarrollar un plan de control de riesgos que considere la priorización, implementación y mantenimiento de controles.
- **Reconocimiento e investigación:** se debe hacer un reconocimiento de las vulnerabilidades en el desarrollo del proceso y una investigación para definir los mejores controles para las mismas.
- **Transferencia del riesgo:** principalmente para compensar pérdidas.

- **Estrategia de mitigación de riesgos:** sirve para definir cómo y cuándo actuar en caso de presentarse amenazas y se encuentren vulnerabilidades.
- **Enfoque para la implementación de controles:** para esto se aplica la siguiente regla: “Se debe abordar los riesgos más grandes y esforzarse por obtener la suficiente mitigación de riesgos al menor costo, con el impacto mínimo en otras capacidades de la misión”.

  La siguiente metodología tiene un enfoque para la implementación de controles dividido en 7 pasos:

  - **Paso 1. Priorización de acciones:** en función de los reportes de evaluación de riesgos. La salida es un ranking de posibles acciones a realizar desde la más alta a la más baja en cuanto a factibilidad.
  - **Paso 2. Evaluación de opciones de controles recomendados:** de manera que se encuentren los controles con mayor factibilidad para su implementación en función de las necesidades del proceso. La salida es una lista de los controles factibles.
  - **Paso 3. Conducción de análisis costo beneficio:** de manera que se encuentren los controles más factibles en cuanto a costos. Se obtiene un análisis costo – beneficio detallado de los controles según los posibles resultados si se los implementa.

- **Paso 4. Selección de controles:** a partir del análisis realizado en el paso anterior, para seleccionar los controles más beneficiosos para el proceso. La salida de este paso es una lista con los controles seleccionados.
- **Paso 5. Asignación de responsabilidades:** es decir, escoger el responsable entre el personal de acuerdo a sus capacidades para implementar los controles seleccionados.
- **Paso 6. Desarrollar un plan de implementación de salvaguardas:** el cual debe incluir:
  - Riesgos y su nivel asociado de riesgo.
  - Controles recomendados.
  - Priorización de acciones.
  - Planes de control escogidos.
  - Recursos necesarios para implementar los planes de control.
  - Listas de equipos responsables.
  - Fecha de inicio de implementación.
  - Fecha límite para finalizar la implementación.
  - Requerimientos de mantenimiento.
- **Paso 7. Implementación de controles seleccionados:** para minimizar los niveles de riesgo.

- **Categorías de controles:** se categoriza en función de la realidad del desarrollo del proceso, es decir, considerando sus ambientes técnicos, operativos y organizacionales.
- **Análisis costo – beneficio:** este análisis se realiza principalmente para determinar el tipo de control a aplicar en función del tipo de circunstancia o instancia del proceso. Este análisis debe considerar:
  - Determinación del impacto sobre el proceso del mejoramiento de controles existentes o la implementación de nuevos controles, o bien de la no realización de estas actividades.
  - Determinar el costo real de la implementación.
  - Determinar la importancia de la esta implementación para el desarrollo del proceso.

- **Riesgo residual:** la implementación o mejoramiento de controles tienen por objetivo principal minimizar el impacto de los riesgos del servicio; esta minimización generalmente deja como resultado riesgos residuales, los mismos que deben tener un seguimiento de manera que se tenga un control máximo sobre la seguridad del servicio.

En la Figura 15 se muestra la valoración del riesgo según la NIST 800-30.

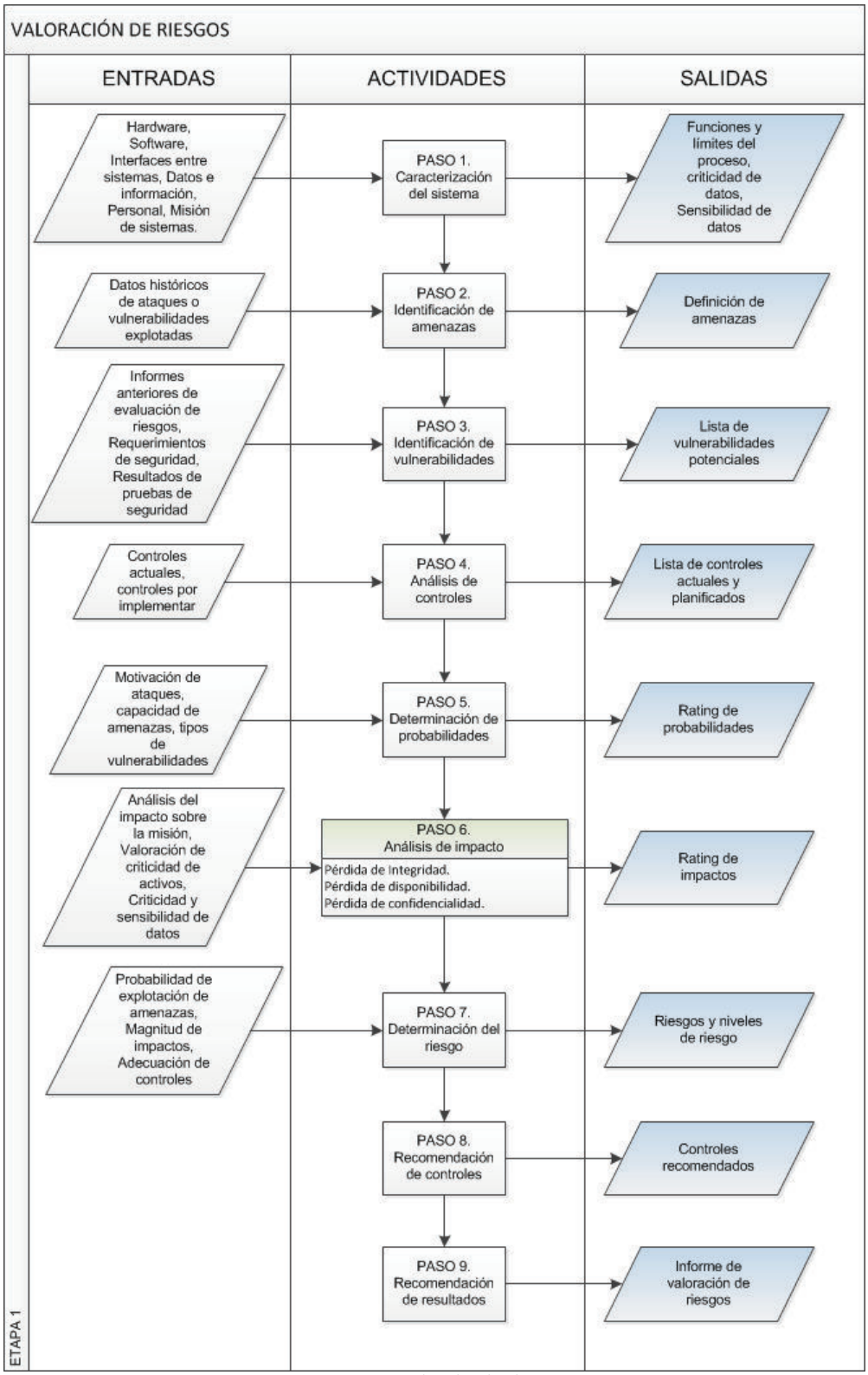

Figura 15 – Valoración de Riesgos
Fuente: NIST SP 800-30: Risk Management Guide for Information Technology Systems

En la Figura 16 se muestra la mitigación de riesgos según la NIST 800-30.

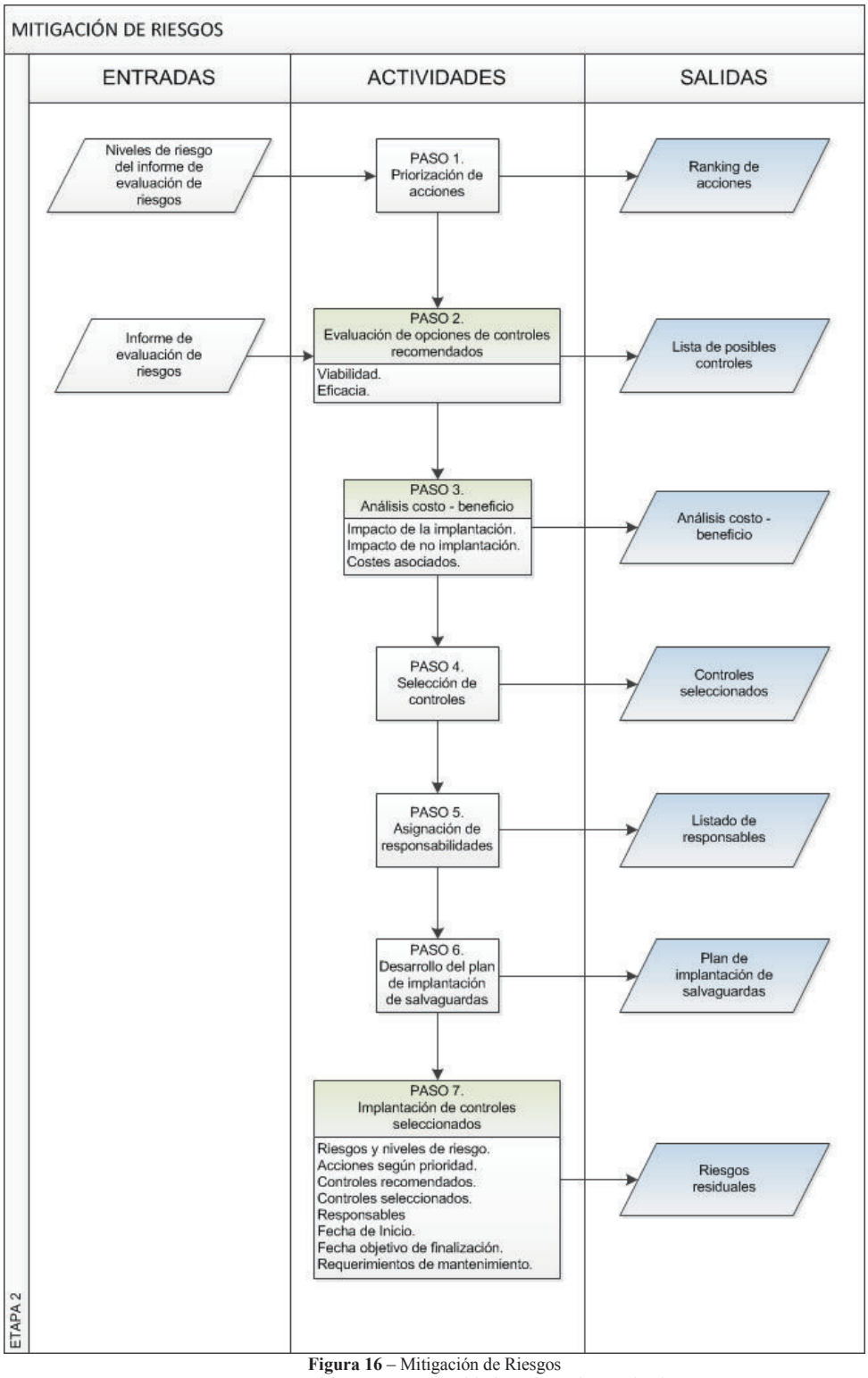

Figura 16 – Mitigación de Riesgos
Fuente: NIST SP 800-30: Risk Management Guide for Information Technology Systems

A continuación se definirán algunos conceptos importantes para comprender el contenido que se tratará a continuación en este capítulo[5]:

a. **"Vulnerabilidad.-** Es una debilidad o falla de los procedimientos de seguridad de un sistema, ya sea en el diseño, implementación o controles que puede ser utilizada para explorar y da lugar la violación de las normas de seguridad o infiltrarse en el sistema infraccionando su seguridad.
b. **Fuente de Amenaza.-** Son un conjunto de métodos que pueden ser usados para explotar las vulnerabilidades que han sido encontradas en un sistema.
c. **Amenaza.-** Es el potencial de que una fuente de amenaza explote (accidentalmente o intencionalmente) una vulnerabilidad específica.
d. **Impacto.-** Es el nivel de afectación causado, en caso de que sea explotada exitosamente una amenaza sobre una vulnerabilidad específica.
e. **Riesgo.-** Es la probabilidad de que una determinada amenaza explote una potencial vulnerabilidad y el impacto de este acontecimiento adverso en la organización."

Para realizar la identificación de las amenazas, riesgos y vulnerabilidades que afectan a la seguridad de información en el servicio, se han tomado en cuenta dos factores:

- Experiencia laboral en el desarrollo del servicio por parte de los autores.
- Entrevistas realizadas a trabajadores con funciones claves en los procesos del servicio.

Estas entrevistas y su respectivo análisis se encuentran detalladas en los siguientes anexos:

- **"Anexo C - Entrevista de Vulnerabilidades Ambientales y Humanas"**
- **"Anexo D - Entrevista de Vulnerabilidades Naturales"**

[5] Fuente: NIST SP 800-30: Risk Management Guide for Information Technology Systems.

- **“Anexo E - Entrevista de Vulnerabilidades Organizacionales”**
- **“Anexo F - Entrevista de Vulnerabilidades Técnicas”**

2.1.3 IDENTIFICACIÓN DE AMENAZAS

A continuación, se muestran los resultados de los análisis de amenazas, comprendidas en las siguientes tablas:

FUENTES DE AMENAZAS NATURALES	ACCIONES DE LA AMENAZA
Movimiento Telúrico	• Destrucción infraestructura física (edificación/hardware). • Daño al personal.
Tormenta Eléctrica	• Falla eléctrica (suspensión del servicio de energía eléctrica). • Daño de equipos.
Tsunami	• Destrucción infraestructura física (edificación/hardware). • Daño personal. • Muerte del Personal. • Suspensión de las actividades.

Tabla 14 – Fuentes de Amenazas Naturales.
Fuente: Empresa de Servicios “XYZ”

FUENTES DE AMENAZAS AMBIENTALES	ACCIONES DE LA AMENAZA
Falla Eléctrica/Suspensión del servicio de energía eléctrica	• Daño de equipos. • Indisponibilidad de los servicios. • Fallo en la integridad de la información. • Desconfiguración de aplicaciones y/o servicios.
Humedad/Sobrecalentamiento	• Daño de equipos. • Incomodidad para el personal y usuarios en el desenvolvimiento de sus actividades. • Suspensión de las actividades.
Animales (roedores, insectos, aves)	• Daños en equipos. • Suspensión de las actividades.
Condiciones de trabajo inadecuadas	• Problemas ergonómicos. • Decrecimiento de la eficiencia del personal. • Pérdida de la concentración. • Malestar al personal y usuarios.

Tabla 15 – Fuentes de Amenazas Ambientales.
Fuente: Empresa de Servicios “XYZ”

FUENTES DE AMENAZAS HUMANAS	ACCIONES DE LA AMENAZA
Pérdida de Personal	• Suspensión y desorganización del soporte y de las tareas que se encuentran a su cargo.
Hacker, cracker	• Ingeniería social. • Intrusión al sistema, allanamiento. • Acceso no autorizado al sistema.
Vandalismo	• Daño de equipos. • Penetración al sistema. • Manipulación al sistema.
Personal y usuarios internos (deficiente capacitación, descontento, malicia, negligencia, error, deshonestidad, o empleados cesados, limpieza incorrecta, frustración)	• Chantaje. • Abuso de computación. • Fraude y robo. • Pérdida de confidencialidad e integridad de los datos: entrada de datos falsificados, corrompidos. • Destrucción negligente de equipos, cables y datos. • Código malicioso (Ej. virus, bomba lógica, caballo de Troya). • Venta/intercambio de información personal. • Fallas del sistema.

FUENTES DE AMENAZAS HUMANAS	ACCIONES DE LA AMENAZA
	• Intrusión al sistema. • Sabotaje al sistema. • Acceso no autorizado al sistema.
Incorrecta administración del sistema y de los derechos de acceso a los datos	• Fallas en el sistema. • Accesos no autorizados. • Pérdida de confidencialidad. • Utilización innecesaria de recursos.
Divulgación de Información	• Mal uso de la información por terceras personas.

Tabla 16 – Fuentes de Amenazas Humanas.
Fuente: Empresa de Servicios "XYZ"

FUENTES DE AMENAZAS TÉCNICAS	ACCIONES DE LA AMENAZA
Falla en un componente	• Falla en las operaciones del sistema. • Daño en equipos.
Falla del proveedor de Internet	• Suspensión de aplicaciones y servicios (que dependan del servicio de Internet).
Inoperatividad de controles existentes	• Falta de protección de los activos/recursos. • Daño de los activos/recursos. • Accesos no autorizados. • Falla en el sistema
Vulnerabilidades o errores de software	• Falla en el sistema. • Falta de protección de los activos/recursos. • Pérdida de confidencialidad, integridad y disponibilidad.
Virus, bombas lógicas, caballo de Troya (código malicioso)	• Falla en el sistema. • Pérdida de confidencialidad, integridad y disponibilidad.

Tabla 17 – Fuentes de Amenazas Técnicas.
Fuente: Empresa de Servicios "XYZ"

FUENTES DE AMENAZAS ORGANIZACIONALES	ACCIONES DE LA AMENAZA
Falta o insuficiencia de reglas	• Deficiencia en la gestión de recursos y operaciones. • Pérdida de confidencialidad de la información.
Monitoreo insuficiente de las medidas de seguridad TI	• Incidentes que afecten a la imagen y seguridad de la organización.
Uso no controlado de recursos	• Falla o daño de los recursos y/o del sistema. • Mal uso de los recursos por parte del personal y usuarios.
Falta de, o inadecuada documentación	• Daños en la operación. • Mantenimiento inadecuado.
La estrategia para el sistema de red y el sistema de gestión no está establecida	• Problemas de instalación, configuración y operación de nuevos componentes en la red y en el sistema de gestión. • Conexiones no autorizadas a la red.
Falta de estaciones de trabajo estandarizadas	• Dificultad en la instalación y mantenimiento. • Dificultad en la seguridad TI.
Falta o insuficiencia de Gestión de la Seguridad de TI	• Falta de responsabilidad del personal. • Inadecuado soporte de gestión. • Inadecuados requerimientos estratégicos y conceptuales. • Impracticabilidad de conceptos de salvaguardas. • Falla para actualizar los procesos TI.
Falta de licencias de software propietario y/o violación de derechos de autor	• Sanciones legales.

Tabla 18 – Fuentes de Amenazas Organizacionales.
Fuente: Empresa de Servicios "XYZ"

2.1.4 IDENTIFICACIÓN DE VULNERABILIDADES

Se realizó un análisis de las amenazas y sus posibles vulnerabilidades, el mismo que se describe a continuación:

VULNERABILIDAD	FUENTE DE AMENAZA
No se cuenta con un plan de evacuación en caso de movimiento telúrico.	Movimiento Telúrico
No se cuenta con un plan de evacuación en caso de tsunami.	Tsunami

Tabla 19 – Vulnerabilidades Naturales.
Fuente: Los Autores

VULNERABILIDAD	FUENTE DE AMENAZA
No se encuentran instalados dispositivos apropiados para el exterminio y prevención de incendios.	Falla Eléctrica/Suspensión del servicio de energía eléctrica
No se tienen UPSs (Uninterruptible Power Supply) de energía eléctrica de respaldo.	
No existen controles suficientes para la seguridad física.	Condiciones de trabajo inadecuadas
No se posee sistemas de calefacción y de aire acondicionado.	

Tabla 20 – Vulnerabilidades Ambientales.
Fuente: Los Autores

VULNERABILIDAD	FUENTE DE AMENAZA
No existen controles suficientes para asegurar la integridad de los datos en la exportación de los mismos para su revisión.	Hacker, cracker
No existen suficientes controles para asegurar la validación y no alteración de los datos.	Personal y usuarios internos (deficiente capacitación, descontento, malicia, negligencia, error, deshonestidad, o empleados cesados, limpieza incorrecta, frustración)
No se protege adecuadamente la integridad de los datos.	

Tabla 21 – Vulnerabilidades Humanas.
Fuente: Los Autores

VULNERABILIDAD	FUENTE DE AMENAZA
No existe un plan de continuidad del negocio, que contemple este caso.	Falla del proveedor de Internet
Falta de revisión de los controles de seguridad del sistema.	Inoperatividad de controles existentes
No se puede resolver conflictos sin entrar directamente en la base de datos.	Vulnerabilidades o errores de software
No se actualiza periódicamente y/o revisa el software de detección y eliminación de virus.	Virus, bombas lógicas, caballo de Troya (código malicioso)

Tabla 22 – Vulnerabilidades Técnicas.
Fuente: Los Autores

VULNERABILIDAD	FUENTE DE AMENAZA
No se ha desarrollado, documentado e implementado un plan de contingencia.	Falta o insuficiencia de reglas
No existe un proceso formal de respuesta a incidentes de seguridad.	
No se realiza evaluaciones de riesgo periódicamente, ni se ha determinado un nivel aceptable de riesgo.	Falta o insuficiencia de Gestión de la Seguridad de TI, monitoreo insuficiente de las medidas de seguridad TI
No existe un plan de seguridad que gestione la Seguridad TI.	
No existen controles de acceso lógico en la red que restrinjan a los usuarios para funciones y transacciones autorizadas.	
Falta de revisión de los controles de seguridad del sistema y sistemas interconectados	

Tabla 23 – Vulnerabilidades Organizacionales.
Fuente: Los Autores

2.2 ANÁLISIS DE IMPACTO, PROBABILIDAD Y CONTROLES

Hasta el momento se han tratado las amenazas y vulnerabilidades que tiene el servicio de “Censos de Información Comercial”; a continuación se mostrarán los

controles implementados en el servicio, el impacto y la probabilidad de ocurrencia de las vulnerabilidades.

2.2.1 CONTROLES IMPLEMENTADOS

Los controles implementados se describen a continuación:

VULNERABILIDAD	FUENTE DE AMENAZA	CONTROLES IMPLEMENTADOS
No se cuenta con un plan de evacuación en caso de movimiento telúrico.	Movimiento Telúrico	No se ha implementado ningún control.
No se cuenta con un plan de evacuación en caso de tsunami.	Tsunami	No se ha implementado ningún control.

Tabla 24 – Controles Implementados para Vulnerabilidades Naturales.
Fuente: Los Autores

VULNERABILIDAD	FUENTE DE AMENAZA	CONTROLES IMPLEMENTADOS
No se encuentran instalados dispositivos apropiados para el exterminio y prevención de incendios.	Falla Eléctrica/Suspensión del servicio de energía eléctrica	No se ha implementado ningún control.
No se tiene UPSs (Uninterruptible Power Supply) de energía eléctrica de respaldo.		No se ha implementado ningún control.
No existen controles suficientes para la seguridad física.	Condiciones de trabajo inadecuadas	La empresa tiene una puerta para el ingreso al lugar donde se encuentran los equipos.

Tabla 25 – Controles Implementados para Vulnerabilidades Ambientales.
Fuente: Los Autores

VULNERABILIDAD	FUENTE DE AMENAZA	CONTROLES IMPLEMENTADOS
No existen controles suficientes para asegurar la integridad de los datos en la exportación de los mismos para su revisión.	Hacker, cracker	Se tiene implantado un firewall, pero las reglas de este no se encuentran documentadas.
No existen suficientes controles para asegurar la validación y no alteración de los datos.	Personal y usuarios internos (deficiente capacitación, descontento, malicia, negligencia, error, deshonestidad, o empleados cesados, limpieza incorrecta, frustración)	No se ha implementado ningún control.
No se protege adecuadamente la integridad de los datos.		Se tiene implantado un firewall, pero las reglas de este no se encuentran documentadas.

Tabla 26 – Controles Implementados para Vulnerabilidades Humanas.
Fuente: Los Autores

VULNERABILIDAD	FUENTE DE AMENAZA	CONTROLES IMPLEMENTADOS
No existe un plan de continuidad del negocio, que contemple este caso.	Falla del proveedor de Internet	No se ha implementado ningún control.
Falta de revisión de los controles de seguridad del sistema.	Inoperatividad de controles existentes	No se ha implementado ningún control.
No se puede resolver conflictos sin entrar directamente en la base de datos.	Vulnerabilidades o errores de software	No se ha implementado ningún

VULNERABILIDAD	FUENTE DE AMENAZA	CONTROLES IMPLEMENTADOS
		control.
No se actualiza periódicamente y/o revisa el software de detección y eliminación de virus.	Virus, bombas lógicas, caballo de Troya (código malicioso)	No se ha implementado ningún control.

Tabla 27 – Controles Implementados para Vulnerabilidades Técnicas.
Fuente: Los Autores

VULNERABILIDAD	FUENTE DE AMENAZA	CONTROLES IMPLEMENTADOS
No se ha desarrollado, documentado e implementado un plan de contingencia.	Falta o insuficiencia de reglas	No se ha implementado ningún control.
No existe un proceso formal de respuesta a incidentes de seguridad.		No se ha implementado ningún control.
No se realiza evaluaciones de riesgo periódicamente, ni se ha determinado un nivel aceptable de riesgo.	Falta o insuficiencia de Gestión de la Seguridad de TI, monitoreo insuficiente de las medidas de seguridad TI	No se ha implementado ningún control.
No existe un plan de seguridad que gestione la Seguridad TI.		No se ha implementado ningún control.
No existen controles de acceso lógico en la red que restrinjan a los usuarios para funciones y transacciones autorizadas.		No se ha implementado ningún control.
Falta de revisión de los controles de seguridad del sistema y sistemas interconectados		No se ha implementado ningún control.

Tabla 28 – Controles Implementados para Vulnerabilidades Organizacionales.
Fuente: Los Autores

2.2.2 PROBABILIDAD E IMPACTO

Para realizar la calificación del impacto y probabilidad de cada una de las vulnerabilidades mencionadas en el punto anterior, se debe definir una escala de probabilidad y de impacto, la misma que se describe a continuación:

ESCALA DE PROBABILIDAD	
PROBABILIDAD	**DESCRIPCIÓN**
Alto	La fuente de amenaza está altamente motivada y es lo suficientemente capaz y los controles para prevenir la vulnerabilidad son ineficientes.
Medio	La fuente de amenaza está motivada y es lo capaz pero los controles implementados pueden bloquear la explotación exitosa de la vulnerabilidad.
Bajo	La fuente de amenaza carece de motivación o capacidad, o los controles que han sido implementados para prevenir o impedir de manera significativa la explotación de la vulnerabilidad.

Tabla 29 – Escala de Probabilidad.
Fuente: NIST SP 800-30: Risk Management Guide for Information Technology Systems

ESCALA DE IMPACTO	
PROBABILIDAD	**IMPACTO**
Alto	La explotación exitosa de la vulnerabilidad implica: • Pérdida de los principales activos o recursos tangibles. • Violación significativa u obstaculización de la misión de la organización, la reputación o intereses. • Pérdidas humanas y heridos graves.

ESCALA DE IMPACTO	
PROBABILIDAD	**IMPACTO**
Medio	La explotación exitosa de la vulnerabilidad puede ocasionar: • Pérdida costosa de bienes o recursos tangibles. • Violación, daño o impedimento de la misión de la organización, la reputación o intereses. • Lesiones.
Bajo	La explotación exitosa de la vulnerabilidad puede ocasionar: • Pérdida de algunos activos o recursos tangibles. • Afectación notable a la misión de la organización, la reputación o intereses.

Tabla 30 – Escala de Impacto.
Fuente: NIST SP 800-30: Risk Management Guide for Information Technology Systems

VULNERABILIDAD	FUENTE DE AMENAZA	PROBABILIDAD	IMPACTO
No se cuenta con un plan de evacuación en caso de movimiento telúrico.	Movimiento Telúrico	Baja	Medio
No se cuenta con un plan de evacuación en caso de tsunami.	Tsunami	Media	Medio

Tabla 31 – Probabilidad e Impacto de Vulnerabilidades Ambientales.
Fuente: Los Autores

VULNERABILIDAD	FUENTE DE AMENAZA	PROBABILIDAD	IMPACTO
No se encuentran instalados dispositivos apropiados para el exterminio y prevención de incendios.	Falla Eléctrica/Sus-pensión del servicio de energía eléctrica	Baja	Medio
No se tiene UPSs (Uninterruptible Power Supply) de energía eléctrica de respaldo.		Baja	Medio
No existen controles suficientes para la seguridad física.	Condiciones de trabajo inadecuadas	Media	Medio

Tabla 32 – Probabilidad e Impacto de Vulnerabilidades Ambientales.
Fuente: Los Autores

VULNERABILIDAD	FUENTE DE AMENAZA	PROBABILIDAD	IMPACTO
No existen controles suficientes para asegurar la integridad de los datos en la exportación de los mismos para su revisión.	Hacker, cracker	Media	Medio
No existen suficientes controles para asegurar la validación y no alteración de los datos.	Personal y usuarios internos (deficiente capacitación, descontento, malicia, negligencia, error, deshonestidad, o empleados cesados, limpieza incorrecta, frustración)	Media	Bajo
No se protege adecuadamente la integridad de los datos.		Medio	Medio

Tabla 33 – Probabilidad e Impacto de Vulnerabilidades Humanas.
Fuente: Los Autores

VULNERABILIDAD	FUENTE DE AMENAZA	PROBABILIDAD	IMPACTO
No existe un plan de continuidad del negocio, que contemple este caso.	Falla del proveedor de Internet	Medio	Medio
Falta de revisión de los controles de seguridad del sistema.	Inoperatividad de controles existentes	Medio	Medio
No se puede resolver conflictos sin entrar directamente en la base de datos.	Vulnerabilidades o errores de software.	Medio	Medio
No se actualiza periódicamente y/o revisa el software de detección y eliminación de virus.	Virus, bombas lógicas, caballo de Troya (código malicioso)	Alta	Medio

Tabla 34 – Probabilidad e Impacto de Vulnerabilidades Técnicas.
Fuente: Los Autores

VULNERABILIDAD	FUENTE DE AMENAZA	PROBABILIDAD	IMPACTO
No se ha desarrollado, documentado e implementado un plan de contingencia.	Falta o insuficiencia de reglas	Alta	Medio
No existe un proceso formal de respuesta a incidentes de seguridad.		Alta	Medio
No se realiza evaluaciones de riesgo periódicamente, ni se ha determinado un nivel aceptable de riesgo.	Falta o insuficiencia de Gestión de la Seguridad de TI, monitoreo insuficiente de las medidas de seguridad TI	Alta	Medio
No existe un plan de seguridad que gestione la Seguridad TI.		Alta	Medio
No existen controles de acceso lógico en la red que restrinjan a los usuarios para funciones y transacciones autorizadas.		Media	Bajo
Falta de revisión de los controles de seguridad del sistema y sistemas interconectados		Media	Bajo

Tabla 35 – Probabilidad e Impacto de Vulnerabilidades Organizacionales.
Fuente: Los Autores

2.3 DETERMINACIÓN DEL RIESGO

Para poder calificar el riesgo de cada una de las vulnerabilidades mencionadas anteriormente, se debe definir una escala de valoración del riesgo, la cual se describe a continuación:

Valoración del Riesgo			
Probabilidad de Ocurrencia	Impacto		
	Bajo(10)	Medio(50)	Alto(100)
Alto(1.0)	Bajo(10)	Medio(50)	Alto(100)
Medio(0.5)	Bajo(5)	Bajo(25)	Medio(50)
Bajo(0.1)	Bajo(1)	Bajo(5)	Bajo(10)

Tabla 36 – Valoración del Riesgo.
Fuente: NIST SP 800-30: Risk Management Guide for Information Technology Systems.

ESCALA DEL RIESGO	
NIVEL DEL RIESGO	DESCRIPCIÓN DEL RIESGO Y ACCIONES NECESARIAS
Alto	Sí una observación o hallazgo se evalúa como de riesgo alto, existe una fuerte necesidad de medidas correctivas. Un sistema existente puede continuar operando, pero un plan de acción correctiva debe ser puesto en marcha el antes posible.
Medio	Sí una observación está clasificada como riesgo medio, las acciones correctivas son necesarias y un plan debe ser desarrollado para incorporar estas acciones dentro de un periodo de tiempo razonable.
Bajo	Sí una observación está clasificada como riesgo bajo, la autoridad aprobatoria designada para el sistema debe determinar si aún se requieren acciones correctivas o se decide aceptar el riesgo.

Tabla 37 – Escala del Riesgo.
Fuente: NIST SP 800-30: Risk Management Guide for Information Technology Systems

Se establecen los riesgos existentes junto con su valoración, de acuerdo a la evaluación de la probabilidad y el análisis del impacto que cada riesgo presenta, como se muestra a continuación:

VULNERABILIDAD	FUENTE DE AMENAZA	PROBABILIDAD	IMPACTO	VALORACIÓN DEL RIESGO
No se cuenta con un plan de evacuación en caso de movimiento telúrico.	Movimiento Telúrico	Baja	Medio	Bajo
No se cuenta con un plan de evacuación en caso de tsunami.	Tsunami	Media	Medio	Medio

Tabla 38 – Valoración de Riesgos Naturales.
Fuente: Los Autores

VULNERABILIDAD	FUENTE DE AMENAZA	PROBABILIDAD	IMPACTO	VALORACIÓN DEL RIESGO
No se encuentran instalados dispositivos apropiados para el exterminio y prevención de incendios.	Falla Eléctrica/Sus-pensión del servicio de energía eléctrica	Baja	Medio	Bajo
No se tienen UPSs (Uninterruptible Power Supply) de energía eléctrica de respaldo.		Baja	Medio	Bajo
No existen controles suficientes para la seguridad física.	Condiciones de trabajo inadecuadas	Media	Medio	Medio

Tabla 39 – Valoración de Riesgos Ambientales.
Fuente: Los Autores

VULNERABILIDAD	FUENTE DE AMENAZA	PROBABILIDAD	IMPACTO	VALORACIÓN DEL RIESGO
No existen controles suficientes para asegurar la integridad de los datos en la exportación de los mismos para su revisión.	Hacker, cracker	Media	Medio	Medio
No existen suficientes controles para asegurar la validación y no alteración de los datos.	Personal y usuarios internos (deficiente capacitación, descontento, malicia, negligencia, error, deshonestidad, o empleados cesados, limpieza incorrecta, frustración)	Media	Bajo	Bajo
No se protege adecuadamente la integridad de los datos.		Medio	Medio	Medio

Tabla 40 – Valoración de Riesgos Humanos.
Fuente: Los Autores

VULNERABILIDAD	FUENTE DE AMENAZA	PROBABILIDAD	IMPACTO	VALORACIÓN DEL RIESGO
No existe un plan de continuidad del negocio, que contemple este caso.	Falla del proveedor de Internet	Medio	Medio	Medio
Falta de revisión de los controles de seguridad del sistema.	Inoperatividad de controles existentes	Medio	Medio	Medio
No se puede resolver conflictos sin entrar directamente en la base de datos.	Vulnerabilidades o errores de software	Media	Medio	Medio
No se actualiza periódicamente y/o revisa el software de detección y eliminación de	Virus, bombas lógicas, caballo de Troya	Alta	Medio	Medio

VULNERABILIDAD	FUENTE DE AMENAZA	PROBABILIDAD	IMPACTO	VALORACIÓN DEL RIESGO
virus.	(código malicioso)			

Tabla 41 – Valoración de Riesgos Técnicos.
Fuente: Los Autores

VULNERABILIDAD	FUENTE DE AMENAZA	PROBABILIDAD	IMPACTO	VALORACIÓN DEL RIESGO
No se ha desarrollado, documentado e implementado un plan de contingencia.	Falta o insuficiencia de reglas	Alta	Medio	Medio
No existe un proceso formal de respuesta a incidentes de seguridad.		Alta	Medio	Medio
No se realiza evaluaciones de riesgo periódicamente, ni se ha determinado un nivel aceptable de riesgo.	Falta o insuficiencia de Gestión de la Seguridad de TI, monitoreo insuficiente de las medidas de seguridad TI	Alta	Medio	Medio
No existe un plan de seguridad que gestione la Seguridad TI.		Alta	Medio	Medio
No existen controles de acceso lógico en la red que restrinjan a los usuarios para funciones y transacciones autorizadas.		Media	Bajo	Bajo
Falta de revisión de los controles de seguridad del sistema y sistemas interconectados		Media	Bajo	Bajo

Tabla 42 – Valoración de Riesgos Organizacionales.
Fuente: Los Autores

2.4 RECOMENDACIONES DE CONTROL

Una vez identificadas las vulnerabilidades y clasificadas de acuerdo a su naturaleza, se recomendarán los mejores controles para su gestión a continuación:

VULNERABILIDAD	FUENTE DE AMENAZA	CONTROLES A IMPLEMENTAR
No se cuenta con un plan de evacuación en caso de tsunami.	Tsunami	Definir las directrices necesarias para regular el desarrollo del plan de contingencia de acuerdo a los riesgos existentes.

Tabla 43 – Controles a Implementar para Vulnerabilidades Naturales.
Fuente: Los Autores

VULNERABILIDAD	FUENTE DE AMENAZA	CONTROLES A IMPLEMENTAR
No existen controles suficientes para la seguridad física.	Condiciones de trabajo inadecuadas	Analizar e implementar los controles adecuados para la seguridad física en la empresa de servicios

Tabla 44 – Controles a Implementar para Vulnerabilidades Ambientales.
Fuente: Los Autores

VULNERABILIDAD	FUENTE DE AMENAZA	CONTROLES A IMPLEMENTAR
No existen controles suficientes para asegurar la integridad de los datos en la exportación de los mismos para su revisión.	Hacker, cracker	Definir e implementar controles para la revisión de las reglas del firewall.

Tabla 45 – Controles a Implementar para Vulnerabilidades Humanas.
Fuente: Los Autores

VULNERABILIDAD	FUENTE DE AMENAZA	CONTROLES A IMPLEMENTAR
No existe un plan de continuidad del negocio que contemple la falta de servicio de Internet.	Falla del proveedor de Internet	Implementar directrices y controles para el desarrollo del plan de contingencia de acuerdo a los riesgos existentes.
Falta de revisión de los controles de seguridad del sistema.	Inoperatividad de controles existentes	Establecer un intervalo de tiempo para la revisión de los controles de seguridad
No se puede resolver conflictos sin entrar directamente en la base de datos.	Vulnerabilidades o errores de software	Establecer un intervalo de tiempo para la revisión de los controles de seguridad
No se actualiza periódicamente y/o revisa el software de detección y eliminación de virus.	Virus, bombas lógicas, caballo de Troya (código malicioso)	Desarrollar e implementar directrices y controles para la detección, prevención y tratamiento de software malicioso.

Tabla 46 – Controles a Implementar para Vulnerabilidades Técnicas.
Fuente: Los Autores

VULNERABILIDAD	FUENTE DE AMENAZA	CONTROLES A IMPLEMENTAR
No existe un proceso formal de respuesta a incidentes de seguridad.	Falta o insuficiencia de reglas	Documentar políticas de control de incidentes en la empresa de servicios.
No se realiza evaluaciones de riesgo periódicamente, ni se ha determinado un nivel aceptable de riesgo.	Falta o insuficiencia de Gestión de la Seguridad de TI, monitoreo insuficiente de las medidas de seguridad TI	Establecer políticas de continuidad del negocio en la empresa de servicios.
No existe un plan de seguridad que gestione la Seguridad TI.		Establecer la política de la seguridad de la información de la empresa de servicios.

Tabla 47 – Controles a Implementar para Vulnerabilidades Organizacionales.
Fuente: Los Autores

2.5 ANÁLISIS DE REQUERIMIENTOS DE SEGURIDAD

Se lo realiza de acuerdo a las normas básicas de seguridad que debe tener el servicio (Tabla 48); para realizar todo el análisis se consideran tres áreas:

- Administrativa
- Operacional
- Técnica

ÁREA DE SEGURIDAD	CRITERIOS DE SEGURIDAD
Seguridad Administrativa	• Asignación de responsabilidades • La continuidad de la ayuda • Capacidad de respuesta a incidentes • Revisión periódica de controles de seguridad • Investigaciones de liquidación de personal y de fondo • Evaluación de riesgos • La formación en seguridad y técnica • Separación de funciones • Sistema de autorización y reautorización • Plan de seguridad del sistema o de la aplicación
Seguridad Operacional	• El control de los contaminantes transportados por el aire (humo, polvo, productos químicos) • Controles para garantizar la calidad del suministro de energía eléctrica • El acceso y la eliminación de medios de Datos

ÁREA DE SEGURIDAD	CRITERIOS DE SEGURIDAD
	• Distribución de datos externa y el etiquetado • Protección de la instalación (por ejemplo, sala de informática, centro de datos, oficina) • Control de humedad • Control de la temperatura • Las estaciones de trabajo, portátiles y ordenadores personales independientes
Seguridad Técnica	• Comunicaciones (por ejemplo, acceso telefónico, de interconexión de sistemas, enrutadores) • Criptografía • Control de acceso discrecional • Identificación y autenticación • La detección de intrusiones • Reutilización de objetos • Sistema de auditoría

Tabla 48 – Criterios de Seguridad.
Fuente: NIST SP 800-30: Risk Management Guide for Information Technology Systems.

Los criterios de seguridad se han seleccionado de la ISO 27005, de acuerdo a las necesidades del servicio de "Censos de Información Comercial". En la columna observación se detallará el análisis realizado en la empresa de servicios "XYZ".

En las siguientes tablas se detallará cada uno de los requerimientos seleccionados.

REQUERIMIENTOS DE SEGURIDAD ADMINISTRATIVOS				
#	REQUERIMIENTOS	ÁREA DE APLICABILIDAD	OBSERVACIÓN	NIVEL DE CUMPLIMIENTO
1	Políticas de evaluación de la seguridad	Riesgos	No se ha desarrollado formalmente las políticas necesarias para evaluar la seguridad en el servicio.	BAJO
2	Procedimientos para realizar evaluaciones de seguridad	Riesgos	No se ha desarrollado formalmente los procedimientos necesarios para evaluar la seguridad en el servicio.	BAJO
3	Política de seguridad del personal.	Recursos Humanos	Existen políticas para asegurar al personal del servicio pero no están formalizadas.	ALTO
4	Procedimientos de monitoreo continuo de controles de seguridad de sistemas de información	Infraestructura y Riesgos	No se monitorea el funcionamiento de los controles de seguridad de información implementados.	BAJO
5	Registros de monitoreo del desempeño de sistemas de información	Infraestructura y Riesgos	No existen registros de monitoreo	BAJO
6	Informe de Monitoreo de Seguridad	Infraestructura y Riesgos	No se realizan informes de monitoreo de seguridad de información	BAJO
7	Procedimientos de evaluación de impacto a la Privacidad en Sistemas de Información	Riesgos	No se realizan evaluaciones periódicas de la privacidad de la información en los sistemas del servicio.	BAJO
8	Evaluación del Impacto a	Riesgos	No se evalúa el impacto a	BAJO

REQUERIMIENTOS DE SEGURIDAD ADMINISTRATIVOS				
#	REQUERIMIENTOS	ÁREA DE APLICABILIDAD	OBSERVACIÓN	NIVEL DE CUMPLIMIENTO
	la Privacidad		la privacidad de la información en el servicio.	
9	Políticas y Procedimientos de Evaluación del Riesgo de Seguridad de Información	Infraestructura y Riesgos	No se han formalizado políticas o procedimientos para evaluar el riesgo el riesgo de la seguridad de información en el servicio.	BAJO
10	Informe de Evaluación del Riesgo	Infraestructura y Riesgos	No se realizan informes de evaluación de riesgos.	BAJO
11	Registros de Actualizaciones de la Evaluación del Riesgo	Infraestructura y Riesgos	No existen registros de actualizaciones de evaluación de riesgos.	BAJO
12	Procedimientos relativos al escaneo de vulnerabilidades	Infraestructura y Riesgos	Se realizan búsquedas de vulnerabilidades que pueden afectar a la seguridad de información del negocio.	ALTO
13	Resultados del escaneo de vulnerabilidades	Infraestructura y Riesgos	Se analizan los resultados de búsquedas de vulnerabilidades para implementar controles en caso que sea necesario.	ALTO
14	Parche y registros de gestión de vulnerabilidades,	Infraestructura	Se toman las medidas necesarias en caso que se detecten vulnerabilidades que afecten al servicio.	ALTO
15	Contratos de Adquisición de Sistemas de Información o Servicios incluye SLA's	Infraestructura	No se ha firmado un SLA con el proveedor de Internet debido a que este no es crítico para el servicio.	MEDIO
16	Documentación de Sistemas de Información que incluya Guía del Administrador y Guía del Usuario	Infraestructura	Existen guías y manuales de usuario para el manejo seguro de los sistemas del servicio.	ALTO
17	Procedimientos relativos a restricciones de uso de software	Riesgos	Existen procedimientos para el uso de software en los sistemas del servicio, pero estos no están formalizados.	MEDIO
18	Documentación de Licencias de software (Inventario de licencias)	Infraestructura	Se cumple con la documentación de licencias para el uso de software en el servicio.	ALTO
19	Listado de Restricciones de Uso del Software	Infraestructura	Se han desarrollado y comunicado las restricciones sobre el uso de software, pero estas no están formalizadas.	MEDIO
20	Procedimientos relativos a software instalado por el usuario	Infraestructura	Se han desarrollado y comunicado las procedimientos sobre el uso de software, pero estos no están formalizados.	MEDIO
21	Registros de seguimiento de fallas de seguridad	Infraestructura	No existen registros de fallas de seguridad	BAJO

Tabla 49– Requerimientos Administrativos.
Fuente: Sistema de Gestión de Seguridad de la Información ISO/ IEC 27001 2013.

REQUERIMIENTOS DE SEGURIDAD OPERACIONALES				
#	REQUERIMIENTOS	ÁREA DE APLICABILIDAD	OBSERVACIÓN	NIVEL DE CUMPLIMIENTO
1	Políticas y Procedimientos de Concientización y Entrenamiento en seguridad al personal	Recursos Humanos	Existen políticas y procedimientos de capacitación de personal para el manejo seguro de	ALTO

REQUERIMIENTOS DE SEGURIDAD OPERACIONALES				
#	REQUERIMIENTOS	ÁREA DE APLICABILIDAD	OBSERVACIÓN	NIVEL DE CUMPLIMIENTO
			los servicios y sistemas en el servicio.	
2	Material de los programas de concientización en Seguridad	Recursos Humanos	Se cuenta con el material necesario para capacitar al personal en el uso de los sistemas y servicios.	ALTO
3	Procedimientos de configuración de Sistemas de Información	Infraestructura	Existen procedimientos formales para configurar los sistemas de información en el servicio.	ALTO
4	Procedimientos relativos a Inventario de los componentes del Sistema de Información	Infraestructura	El inventario no está formalizado.	MEDIO
5	Registros de Inventario de los componentes del Sistema de Información	Infraestructura	No existe un registro de inventarios	BAJO
6	Plan de Contingencia	Infraestructura y Riesgos	No se han desarrollado planes de contingencia.	BAJO
7	Documentos de la Planificación de TI	Gerencia de TI	La planificación existente para TI no está formalizada.	MEDIO
8	Pruebas del Plan de Contingencias	Infraestructura y Riesgos	No existe un plan de contingencia	BAJO
9	Resultados de Pruebas del Plan de Contingencias	Infraestructura y Riesgos	No existe un plan de contingencia	BAJO
10	Procedimientos relativos a Revisiones y Actualizaciones del Plan de Contingencia	Infraestructura y Riesgos	No existe un plan de contingencia	BAJO
11	Procedimientos relativos a Sitios de almacenamiento alterno	Infraestructura	No existe un plan de contingencia	BAJO
12	Definición de Sitio de Almacenamiento Alterno	Infraestructura	No existe un plan de contingencia	BAJO
13	Procedimientos relativos a Servicios de Telecomunicaciones Alterno	Infraestructura	No existe un plan de contingencia	BAJO
14	Procedimientos de recuperación y reconstitución de la Información	Infraestructura	Existen procedimientos no formalizados para recuperar información en caso que existan conflictos.	MEDIO
15	Políticas de Respaldos	Infraestructura	Existen políticas no formalizadas de respaldos de información	MEDIO
16	Bitácoras de Respaldos y Almacenamiento con firmas de responsabilidad	Infraestructura	No existen bitácoras de respaldos.	BAJO
17	Políticas y Procedimientos de Respuesta a Incidentes.	Infraestructura	No existen políticas o procedimientos de respuesta ante incidentes	BAJO
18	Registros de Auditoría de operaciones	Infraestructura	No existe un manejo formalizado de los logs de auditoría	MEDIO
19	Políticas y Procedimientos de Protección de los Medios (respaldos)	Infraestructura	No existen políticas o procedimientos de protección de respaldos	BAJO
20	Políticas de Protección física y ambiental	Infraestructura	Existen políticas no formalizadas de protección física y ambiental	MEDIO
21	Diagramas de las facilidades de comunicación y del cableado - Data Center	Infraestructura	No existen diagramas.	BAJO
22	Procedimientos relativos al	Infraestructura	Existen procedimientos de	MEDIO

REQUERIMIENTOS DE SEGURIDAD OPERACIONALES				
#	REQUERIMIENTOS	ÁREA DE APLICABILIDAD	OBSERVACIÓN	NIVEL DE CUMPLIMIENTO
	monitoreo de acceso físico		monitoreo a las instalaciones de procesamiento de información, pero no están formalizados.	
23	Logs o Registros del Acceso Físico, Logs o Registros de la alarma de intrusión y/o equipo de vigilancia	Infraestructura / Seguridad física	No existen logs de acceso físico. No existe un equipo de vigilancia.	BAJO
24	Logs o Registros de Control de Acceso a las Instalaciones	Seguridad Física	Existen registros del acceso del personal a las instalaciones.	ALTO
25	Documentación del suministro de energía alternativo	Infraestructura/Seguridad física	No se ha implementado un suministro de energía alternativo.	BAJO
26	Documentación de Dispositivos/Sistemas de detección y extinción de incendios	Seguridad Física	No existen equipos de control de incendios.	BAJO
27	Procedimientos relativos a la terminación de personal	Recursos Humanos, Infraestructura y Riesgos	Existen procedimientos para la terminación de personal, pero no están formalizados.	MEDIO
28	Mecanismos de Protección contra código malicioso	TI	Se han implementado sistemas de antivirus y antimalware, pero no se actualizan regularmente	MEDIO
29	Procedimientos relativos a Protección contra el Spam	TI	Se han implementado sistemas de antivirus y antimalware, pero no se actualizan regularmente.	MEDIO

Tabla 50– Requerimientos Operacionales.
Fuente: Sistema de Gestión de Seguridad de la Información ISO/ IEC 27001 2013.

REQUERIMIENTOS DE SEGURIDAD TÉCNICOS				
#	REQUERIMIENTOS	ÁREA DE APLICABILIDAD	OBSERVACIÓN	NIVEL DE CUMPLIMIENTO
1	Manual de Políticas y Procedimientos de Seguridad de Control de Acceso a: • Red • Sistemas de Información • Aplicaciones Críticas	Infraestructura, Riesgos	Existen políticas y procedimientos de control de acceso, pero no están formalizadas.	ALTO
2	Políticas de Administración de Contraseñas	Infraestructura y Riesgos	Las reglas de administración de claves no son suficientes para salvaguardar el acceso a los sistemas	BAJO
3	Lista de usuarios de red	Infraestructura	Debido a la arquitectura de red, el desarrollo de una lista de usuarios es opcional.	MEDIO
4	Lista de usuarios de sistemas de información y aplicaciones críticas	Riesgos	Existe una lista de usuarios, pero no se encuentra formalizada.	MEDIO
5	Documentación Técnica, usuario y diseño de: • Red • Sistemas de Información • Aplicaciones Críticas	Infraestructura	Existe toda la documentación técnica de: • Hardware • Software • Bases de Datos • Redes y Telecomunica-ciones	ALTO
6	Listado de cuentas activas	Infraestructura	El listado existente no	MEDIO

REQUERIMIENTOS DE SEGURIDAD TÉCNICOS				
#	**REQUERIMIENTOS**	**ÁREA DE APLICABILIDAD**	**OBSERVACIÓN**	**NIVEL DE CUMPLIMIENTO**
			está formalizado	
7	Manual de Configuración de: • Red • Sistemas de Información • Aplicaciones Críticas	Infraestructura	Existe toda la documentación técnica de: • Hardware • Software • Bases de Datos • Redes y Telecomunica-ciones	ALTO
8	Manual Orgánico Funcional de la Institución que indique Funciones y Responsabilidades de cada área	Gerencia	No existe un manual formalizado, pero el Líder junto al Gerente del Proyecto gestiónan las funciones y responsabilidades de las áreas involucradas en el desarrollo del servicio.	MEDIO
9	Segregación de Funciones por Área	Gerencia TI	La segregación de funciones no está formalizada.	MEDIO
10	Informe de Intentos de acceso fallidos	Riesgos	Los logs de auditoría de sistemas registran la información de los intentos de acceso a los mismos.	ALTO
11	Bitácoras de cambio en la configuración de: • Red • Sistemas de Información • Aplicaciones Críticas	Infraestructura	No existen estas bitácoras.	BAJO
12	Procedimiento de bloqueo de sesiones	Infraestructura y Riesgos	No se ha implementado el bloqueo de sesiones en el uso de sistemas	BAJO
13	Estándares de Documentación de Bases de Datos como: Modelo Entidad Relación Diccionario de Datos	Infraestructura	Se cuenta con toda la documentación técnica de la base de datos.	ALTO
14	Estándares de Respaldos de la Configuración de: • Red • Servidores • Bases de Datos • Sistemas de Información • Firewall • Active Directory • Aplicaciones Críticas • Sistemas de Información	Infraestructura	No se utilizan estándares de respaldos de configuración de: • Hardware • Software • Bases de Datos • Redes y Telecomunica-ciones	BAJO
15	Respaldo de la Configuración de: • Red • Servidores • Bases de Datos • Sistemas de Información • Firewall • Active Directory • Aplicaciones Críticas • Sistemas de Información	Infraestructura	No se realizan respaldos de configuraciones de: • Hardware • Software • Bases de Datos • Redes y Telecomunica-ciones	BAJO
16	Reportes e Informes de	Soporte, Infraestructura,	No se realizan reportes o	BAJO

REQUERIMIENTOS DE SEGURIDAD TÉCNICOS				
#	**REQUERIMIENTOS**	**ÁREA DE APLICABILIDAD**	**OBSERVACIÓN**	**NIVEL DE CUMPLIMIENTO**
	Auditoría de: • Accesos no permitidos a la red • Cuentas bloqueadas por intentos fallidos de Sistemas de Información, red, aplicaciones críticas, etc.	Riesgos	informes de auditoría de: • Hardware • Software • Bases de Datos • Redes y Telecomunica-ciones	
17	Informes de Auditoría de: • Transacciones sensibles en las aplicaciones críticas • Cambios en Base de Datos desde el Administrador de • Base de Datos • Acceso Remoto	Infraestructura	No se realizan reportes o informes de auditoría de: • Hardware • Software • Bases de Datos • Redes y Telecomunica-ciones	BAJO
18	Procedimiento para sincronización de relojes de los Sistemas de Información	Infraestructura	No existen procedimientos de sincronización de relojes.	BAJO
19	• Políticas de Correo Electrónico. • Políticas de Administración del Firewall (Configuración). • Políticas y procedimientos para no repudio de información.	Infraestructura, Soporte	Existen estas políticas y procedimientos pero no están formalizados	MEDIO

Tabla 51– Requerimientos Técnicos.
Fuente: Sistema de Gestión de Seguridad de la Información ISO/ IEC 27001 2013.

CAPÍTULO 3. IDENTIFICACIÓN Y EVALUACIÓN DE OBJETIVOS DE CONTROL ISO/IEC 27001

Para definir y gestionar formalmente un SGSI se debe considerar:

- Requerimientos legales y organizacionales
- Alcance y límites del SGSI
- Política del SGSI
- El enunciado de aplicabilidad de acuerdo a las actividades generales que lleva a cabo la empresa de servicios “XYZ” en el servicio de “Censos de Información Comercial”.

A continuación se detallarán cada uno de estos puntos.

3.1 REQUERIMIENTOS LEGALES Y ORGANIZACIONALES

El área administrativa de la empresa de servicios “XYZ” será la responsable de identificar todos los requerimientos legales que se deben cumplir para el desarrollo del servicio.

La empresa de servicios “XYZ” también deberá firmar un acuerdo de confidencialidad para proteger la información de los clientes de la Distribuidora de Energía.

3.1.1 IDENTIFICACIÓN DE REQUISITOS Y PARTES INTERESADAS

La empresa de servicios “XYZ” identificará a todos los individuos (personas u organizaciones) cuyas actividades puedan verse afectadas por el desarrollo del servicio, o por las medidas tomadas para salvaguardar su información. También identificará requisitos legales, normativos, contractuales o de otra índole que correspondan.

La empresa de servicios “XYZ” definirá un responsable para el monitoreo del cumplimiento de los requisitos individuales para proteger la información. También identificará las partes interesadas que deberán ser notificadas en caso que ocurran cambios que afecten al desarrollo del servicio, por ejemplo: adquisición de nueva tecnología para la obtención y procesamiento de datos, creación de nuevos roles de trabajo, creación de nuevos perfiles para el uso de sistemas de información, etc.

El “Área Administrativa” de la empresa de servicios “XYZ” deberá notificar al Líder de Proyecto si detecta algún nuevo requisito legal, normativo, contractual o de otra índole, que pueda ser importante para la gestión de la seguridad de información en el servicio.

Los requerimientos legales y organizacionales identificados se describen a continuación:

No.	REQUERIMIENTO LEGAL Y ORGANIZACIONAL	DOCUMENTO QUE IMPONE EL REQUERIMIENTO	RESPONSABLE DEL CUMPLIMIENTO
1	Cumplimiento obligatorio de las normas referidas a “Evaluación de Riesgos”, Política de la seguridad de la Información.	Normas de control interno de la empresa de servicios “XYZ”.	Gerente de la empresa de servicios “XYZ”.
2	Cumplimiento obligatorio de los “Art. 18.-Todas las personas, en forma individual o colectiva, tienen derecho a: ……. 2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información.”[6]	Constitución de la República del Ecuador	Gerente de la empresa de servicios “XYZ”.
3	Cumplimiento obligatorio, en especial de los capítulos “Finalidad, objeto y ámbito de aplicación” y “Principios generales del registro de	Ley del sistema nacional de registro de datos públicos	Gerente de la empresa de servicios “XYZ”.

[6] Fuente: Constitución de la República del Ecuador

No.	REQUERIMIENTO LEGAL Y ORGANIZACIONAL	DOCUMENTO QUE IMPONE EL REQUERIMIENTO	RESPONSABLE DEL CUMPLIMIENTO
	datos públicos"		
5	Acuerdos de Confidencialidad de los funcionarios de la empresa de servicios "XYZ"	Acuerdos de Confidencialidad firmados	Gerente de la empresa de servicios "XYZ".
6	Cumplimiento obligatorio de todo su contenido	Ley orgánica de transparencia y acceso a la información pública	Gerente de la empresa de servicios "XYZ".
7	Referencia de cumplimiento, de acuerdo a las necesidades de los procesos de obligaciones contractuales y sanciones	Código Civil	Gerente de la empresa de servicios "XYZ".
8	Cumplimiento obligatorio de todo su contenido	Ley de comercio electrónico, firmas electrónicas y mensajes de datos; y, su Reglamento	Gerente de la empresa de servicios "XYZ".
9	Cumplimiento obligatorio, en especial de los derechos de autor: Libro I, Título I, De los derechos de autor y derechos conexos	Ley de Propiedad Intelectual	Gerente de la empresa de servicios "XYZ".
10	Referencia de cumplimiento, de acuerdo a las necesidades de los procesos de obligaciones contractuales y sanciones	Código Penal	Gerente de la empresa de servicios "XYZ".
11	Referencia de cumplimiento, de acuerdo a las necesidades de los procesos de obligaciones contractuales y sanciones	Código de Procedimiento Civil y Penal	Gerente de la empresa de servicios "XYZ".
12	Cumplimiento recomendado, de acuerdo a los componentes y funciones del Sistema de Gestión de la Información del servicio de Censos de Información Comercial (SGSI).	ISO IEC 27001:2013	Gerente de la empresa de servicios "XYZ".

Tabla 52– Requerimientos Legales y Organizacionales.
Fuente: Sistema de Gestión de Seguridad de la Información ISO/ IEC 27001 2013.

3.2 ALCANCE Y LÍMITES DEL SGSI

Para obtener un SGSI efectivo para el servicio de "Censos de Información Comercial" se debe considerar, previo a su desarrollo, su alcance y límites en función del objetivo del servicio, que es recopilar información de Catastro de clientes de una Distribuidora de Energía.

La definición del alcance y límites del SGSI se realizará tomando en cuenta todos los procesos involucrados en el funcionamiento del servicio:

- Planificación de rutas, que consiste en el diseño de rutas, la asignación de las mismas al gestor de campo y finalmente la impresión de las rutas.
- Levantamiento de información comercial, conformado por la carga de los datos a las PocketPC, la recolección de información de datos y la descarga de datos censados en el respectivo repositorio de datos.
- Procesamiento de información, donde se realiza la validación de datos censados y la carga de datos mediante la base móvil.
- Afinamiento de información, que consta de la recolección y validación de datos censados, una carga auxiliar de datos de la base móvil según sea el caso, la verificación y validación de dichos datos, la generación de reportes con resultados y la resolución de conflictos con la información.

3.2.1 RECURSOS

Los recursos utilizados están comprendidos en los siguientes campos:

- Hardware.
- Software.
- Bases de Datos.
- Redes y Telecomunicaciones.
- Recursos Humanos.

Estos recursos están definidos en los puntos 1.4.5 *"RED"* y 1.4.6 *"ACTIVOS DE INFORMACIÓN", l*os cuales son utilizados en el desarrollo del servicio.

Otro recurso importante para el servicio es el de Internet, el cual es utilizado para consultar y, si es necesario, actualizar los datos de los clientes de la Distribuidora de Energía, de manera que la información utilizada sea confiable.

Finalmente, se considera también el cumplimiento de aspectos legales definido en el punto anterior.

3.3 POLÍTICA DEL SGSI

En la empresa de servicios “XYZ” se debe definir una política de SGSI de acuerdo a las reglas del negocio, cuya organización considerará los siguientes puntos:

- Marco de referencia para fundamentar los objetivos, una dirección general y las acciones que se relacionen con la seguridad de la información. Para el presente caso, el marco de referencia a utilizarse será la norma ISO/IEC 27001:2013.
- Requerimientos legales, comerciales y responsabilidades contractuales.
- Alineamiento con la gestión del riesgo estratégico de la empresa de servicios para establecer y brindar mantenimiento al SGSI.
- Criterios de evaluación el riesgo.
- Aprobación de la gerencia de la empresa de servicios.

Además, la política del SGSI debe estar alineada con el alcance y límites (punto 3.2 *“ALCANCE Y LÍMITES DEL SGSI”*) y la metodología de evaluación y tratamiento de riesgos (punto 2.1.2 “*IMPLEMENTACIÓN DE LA METODOLOGÍA SELECCIONADA”*).

Los responsables de monitorear el cumplimiento y efectividad de esta política son:

- El Gerente de Proyecto y el Líder de Proyecto:
    - Apoyarán la implementación y administración del SGSI, así como la comunicación y capacitación al resto del personal implicado en el desarrollo de dicho servicio.
    - Monitorearán el funcionamiento operativo del SGSI.
- El Gerente de Proyecto revisará anualmente el SGSI, o cuando se produzca algún cambio que afecte al servicio.
- Cuando ocurran cambios del tipo mencionado en el punto anterior, se debe comunicar y capacidad a los trabajadores implicados en el desarrollo del servicio.

- La responsabilidad de la seguridad de la información de los recursos utilizados en el desarrollo del servicio, será responsabilidad de propietarios previamente asignados.

La Política de Seguridad de la Información para la empresa de servicios “XYZ” está indicada en **“Anexo G - Política del Seguridad de Información”**.

3.4 ENUNCIADO DE APLICABILIDAD

El enunciado de aplicabilidad es un documento que describe los controles relevantes y aplicables al servicio de “Censos de Información Comercial”. Estos controles son el resultado de:

- Análisis del riesgo previo
- Requerimientos legales
- Obligaciones de la empresa para proteger la integridad, disponibilidad y confidencialidad de la información.

El enunciado de aplicabilidad contempla los siguientes puntos:

- Objetivos de control y motivo de selección.
- Objetivos de control que la empresa de servicios “XYZ” tiene implementados actualmente.
- Exclusión de controles con su respectiva justificación.
- Creación de controles exclusivos para salvaguardar la información en el servicio.

El análisis de riesgos, la Política del SGSI y la norma ISO/IEC 27001:2013 indican los controles que necesitan ser implementados en el servicio, descritos a continuación:

ID	CONTROLES SEGÚN LA NORMA ISO/IEC 27001	APLICABILIDAD (SÍ/NO)	MOTIVOS PARA ELECCIÓN/ NO ELECCIÓN	OBJETIVOS DEL CONTROL	MÉTODO DE IMPLEMENTACIÓN
A5	**POLÍTICAS DE SEGURIDAD DE INFORMACIÓN**				
A5.1	**Dirección de Gestión de Seguridad de la Información**				
A5.1.1	Políticas de seguridad de información	SI	Garantizar la confidencialidad, integridad y disponibilidad de la información.	Apoyar a la empresa de servicios en el aseguramiento de información.	Política del Sistema de Gestión de la Seguridad de la Información.
A5.1.2	Revisión de políticas de seguridad de información				
A6	**ORGANIZACIÓN DE LA SEGURIDAD DE INFORMACIÓN**				
A6.1	**Organización Interna**				
A6.1.1	Roles y responsabilidades de seguridad de información	SI	Resguardar la seguridad de la información en el servicio.	Definir roles y responsabilidades para garantizar la seguridad de información.	Política de la Organización de la Seguridad de la Información.
A6.1.2	Segregación de deberes	SI	Evitar que la información clasificada como confidencial sea modificada.	Separar las funciones y áreas de responsabilidad con el fin de reducir las posibilidades de modificación no autorizada.	
A6.1.3	Contacto con autoridades	NO	Definir quién y cuándo deberían ser contactada las autoridades como Policía, 911, etc.	**N/A**	**N/A**
A6.1.4	Contacto con grupos de interés especial	SI	Conseguir el apoyo en la gestión de incidentes de seguridad por las autoridades correspondientes.	Mantener contacto con grupos de interés especializados u otras asociaciones profesionales de la seguridad de la información.	Política de la Organización de la Seguridad de la Información.
A6.1.5	Seguridad de información en la gestión de proyectos	SI	Garantizar la seguridad de información del servicio.	Gestionar las actividades de seguridad de información por las autoridades a cargo del servicio.	
A6.2	**Dispositivos Móviles y Teletrabajo**				
A6.2.1	Política de uso de dispositivos móviles	SI	Garantizar el uso adecuado de los dispositivos móviles en las actividades que del servicio.	Elaborar una política apropiada de seguridad para protegerse contra el uso el uso indebido de computación móvil.	Política de la Organización de la Seguridad de la Información.
A6.2.2	Teletrabajo	SI	Precautelar la Integridad de la información del servicio.	Implementar políticas para el teletrabajo.	
A7	**SEGURIDAD DE RECURSOS HUMANOS**				
A7.1	**Antes de Empleo**				
A7.1.1	Evaluación de aspirantes	NO	Esta función es parte del área de recursos humanos.	**N/A**	**N/A**
A7.1.2	Términos y condiciones de empleo	NO	Esta función es parte del área de recursos humanos.	**N/A**	**N/A**

ID	CONTROLES SEGÚN LA NORMA ISO/IEC 27001	APLICABILIDAD (SÍ/NO)	MOTIVOS PARA ELECCIÓN/ NO ELECCIÓN	OBJETIVOS DEL CONTROL	MÉTODO DE IMPLEMENTACIÓN
A7.2	**Durante el Empleo**				
A7.2.1	Responsabilidades de la Administración	SI	Garantizar que los empleados respeten las políticas establecidas en el servicio.	Asegurar que los trabajadores y contratistas y terceros cumplan las políticas de seguridad.	Política y Procedimiento de Seguridad de Recursos Humanos.
A7.2.2	Concienciación, educación y entrenamiento sobre la seguridad de la información	SI	Concientizar a los empleados y proveedores del servicio acerca de la seguridad de la información.	Capacitar adecuadamente a los empleados de la organización y contratistas acerca de la seguridad de la información.	
A7.2.3	Proceso disciplinario	SI	Evitar violaciones a las políticas de seguridad de la información del servicio.	Establecer sanciones a los trabajadores que no cumplan con las políticas de seguridad de información.	
A7.3	**Terminación y Cambio de Empleo**				
A7.3.1	Terminación o cambio de responsabilidades laborales	SI	Evitar la fuga de información por activos no devueltos o por accesos abiertos a ex empleados.	Asegurar la devolución de activos y retiro de los privilegios de acceso del trabajador o contratista.	Política y Procedimiento de Seguridad de Recursos Humanos.
A8	**GESTIÓN DE ACTIVOS**				
A8.1	**Responsabilidad de Activos**				
A8.1.1	Inventario de activos	SI	Proteger los activos de información del servicio.	Identificar todos los activos importantes del servicio.	Política y Procedimiento de Gestión de Activos.
A8.1.2	Propiedad de activos	SI	Establecer los responsables de la seguridad de la información de los activos del servicio.	Determinar las responsabilidades de los propietarios de cada activo de información.	
A8.1.3	Uso aceptable de activos	SI	Garantizar el uso adecuado de los activos de información del servicio.	Identificar y documentar las regulaciones de información y sus activos asociados.	
A8.1.4	Categorías de activos	SI	Establecer la importancia y criticidad de cada uno de los activos de información.	Categorizar los activos de acuerdo a su criticidad.	
A8.2	**Clasificación de Información**				
A8.2.1	Clasificación de la información	SI	Garantizar la confidencialidad de la información del servicio.	Clasificar la información de acuerdo a su criticidad y sensibilidad.	Política y Procedimiento de Gestión de Activos.
A8.2.2	Etiquetado de información	SI	Evitar pérdida de activos de información.	Etiquetar la información de acuerdo a su clasificación y criticidad.	
A8.2.3	Manejo de activos	NO	Esta función no es parte del servicio.	**N/A**	**N/A**

ID	CONTROLES SEGÚN LA NORMA ISO/IEC 27001	APLICABILIDAD (SÍ/NO)	MOTIVOS PARA ELECCIÓN/ NO ELECCIÓN	OBJETIVOS DEL CONTROL	MÉTODO DE IMPLEMENTACIÓN
A8.3	**Manejo del Soporte**				
A8.3.1	Gestión de soportes extraíbles	SI	Evitar la fuga de información en soportes extraíbles.	Gestionar los soportes extraíbles.	Política y Procedimiento de Gestión de Activos.
A8.3.2	Eliminación de medios de comunicación	SI	Evitar la fuga de información en soportes extraíbles antes a su desecho.	Eliminar los soportes extraíbles de forma segura.	
A8.3.3	Transferencia de medios físicos	SI	Evitar el uso indebido o divulgación de información confidencial durante el transporte de los medios físicos.	Proteger los medios físicos en el momento de ser transportados al exterior de las oficinas de procesamiento.	
A9	**CONTROL DE ACCESO**				
A9.1	**Requerimientos del Negocio de Control de Acceso**				
A9.1.1	Política de control de acceso	SI	Garantizar el acceso autorizado a la información.	Desarrollar políticas de control de acceso basadas en los requerimientos de seguridad del servicio.	Política y Procedimiento de Control de Acceso.
A9.1.2	Acceso a redes y servicios de red	SI	Precautelar la seguridad, confidencialidad y disponibilidad de la red.	Identificar las características de seguridad, nivel de servicio y requisitos de los servicios de red.	
A9.2	**Gestión de Acceso de Usuario**				
A9.2.1	Registro de usuarios y bajas	SI	El registro de usuarios no es parte del servicio.	**N/A**	**N/A**
A9.2.2	Administración de acceso de usuarios	SI		**N/A**	**N/A**
A9.2.3	Gestión de derechos de acceso privilegiados	NO		**N/A**	**N/A**
A9.2.4	Gestión de la información de autenticación secreta de usuarios	NO		**N/A**	**N/A**
A9.2.5	Revisión de derechos de acceso de usuario	NO		**N/A**	**N/A**
A9.2.6	Eliminación o ajuste de derechos de acceso	NO		**N/A**	**N/A**
A9.3	**Responsabilidades del Usuario**				
A9.3.1	Uso de información secreta de autenticación (Uso de claves)	SI	Garantizar el acceso autorizado a los sistemas de información	Establecer una guía para que el usuario seleccione y realice el mantenimiento de contraseñas seguras.	Política y Procedimiento de Control de Acceso.
A9.4	**Control del Sistema y Acceso a Aplicaciones**				
A9.4.1	Restricción de acceso a información	NO	No es parte del servicio.	**N/A**	**N/A**

ID	CONTROLES SEGÚN LA NORMA ISO/IEC 27001	APLICABILIDAD (SÍ/NO)	MOTIVOS PARA ELECCIÓN/ NO ELECCIÓN	OBJETIVOS DEL CONTROL	MÉTODO DE IMPLEMENTACIÓN
A9.4.2	Procedimientos de inicio de sesión seguro	NO		N/A	N/A
A9.4.3	Sistema de gestión de contraseñas	NO		N/A	N/A
A9.4.4	El uso de los programas de servicios públicos privilegiados	NO		N/A	N/A
A9.4.5	Control de acceso a código s fuente	NO		N/A	N/A
A10	**CRIPTOGRAFÍA**				
A10.1	**Controles Criptográficos**				
A10.1.1	Política sobre el uso de controles criptográficos	SI	Garantizar la integridad de la información al servicio.	Establecer políticas sobre el uso de controles criptográficos para la protección de información.	Política de Criptografía.
A10.1.2	Gestión de claves	SI	Evitar el acceso no autorizado al servicio.	Establecer la gestión de claves en el uso de las técnicas de encriptación.	
A11	**SEGURIDAD FÍSICA Y AMBIENTAL**				
A11.1	**Áreas Seguras**				
A11.1.1	Perímetro de seguridad física	SI	Impedir el acceso físico no autorizado a las instalaciones de procesamiento de información del servicio.	Implementar un perímetro de seguridad para proteger el área de procesamiento de información.	Política de Seguridad Física y Ambiental.
A11.1.2	Controles de entrada físicas	SI		Asegurar que los controles de seguridad estén en un lugar permitido solo para el personal autorizado.	
A11.1.3	Asegurar oficinas, salas e instalaciones	SI		Asegurar que las oficinas que procesan información estén bajo llave.	
A11.1.4	La protección contra amenazas externas y ambientales	SI		Diseñar políticas para la protección física contra los daños causados por incendio, inundación, terremoto, explosión, disturbios civiles y otras formas de desastres naturales o provocados por el hombre.	
A11.1.5	Trabajo en zonas seguras	SI	Evitar la pérdida de información por accesos no autorizados en áreas seguras.	Diseñar las protecciones físicas y directrices para trabajar en áreas seguras.	
A11.1.6	Zonas de entrega y carga	NO	No es parte del servicio.	N/A	N/A
A11.2	**Equipo**				

ID	CONTROLES SEGÚN LA NORMA ISO/IEC 27001	APLICABILIDAD (SÍ/NO)	MOTIVOS PARA ELECCIÓN/ NO ELECCIÓN	OBJETIVOS DEL CONTROL	MÉTODO DE IMPLEMENTACIÓN
A11.2.1	Ubicación y protección del equipo	SI	Impedir la pérdida o robo de los activos de información al interior del área "Procesamiento de Información" del servicio.	Proteger y reducir los riesgos de las amenazas ambientales y de los accesos no autorizados al área de "Procesamiento de Información".	Política de Seguridad Física y Ambiental.
A11.2.2	Apoyo a los servicios públicos	SI	Garantizar que los equipos del área "Procesamiento de Información" funcionen correctamente ante cualquier eventualidad.	Proteger los equipos de fallas de energía.	
A11.2.3	Seguridad del cableado	SI	Garantizar el funcionamiento correcto de las redes de "Procesamiento de Información".	Proteger el cableado de la intercepción o daño de cables de telecomunicaciones, servicio de transporte de datos o información.	
A11.2.4	Mantenimiento de equipo	SI	Impedir interrupciones en el servicio por falta de mantenimiento de los equipos.	Asegurar la disponibilidad continua e integridad del equipo.	
A11.2.5	Eliminación de los activos	NO	Esta función es parte del área de sistemas.	**N/A**	**N/A**
A11.2.6	Seguridad de equipo y activos fuera de las instalaciones	SI	Se debe mantener la seguridad de los equipos fuera de las instalaciones del servicio.	Precautelar la integridad de la información de los equipos cuando se encuentren fuera de las instalaciones del servicio.	Política y Procedimiento de Seguridad Física y Ambiental.
A11.2.7	Eliminación segura o reutilización de equipos	SI	No aplica al servicio.	**N/A**	**N/A**
A11.2.8	Equipos desatendidos de usuario	NO	No aplica al servicio.	**N/A**	**N/A**
A11.2.9	Política de escritorio y pantalla limpia	SI	Impedir el acceso no autorizado a información.	Asegurar los documentos y equipos utilizados en el servicio.	Política de Seguridad Física y Ambiental.
A12	**OPERACIONES DE SEGURIDAD**				
A12.1	**Procedimientos y Responsabilidades Operacionales**				
A12.1.1	Procedimientos operativos documentados	NO	Los procedimientos dependen de la empresa de servicio eléctrico.	**N/A**	**N/A**
A12.1.2	Gestión de cambio	NO	No es parte del servicio.	**N/A**	**N/A**
A12.1.3	Gestión de capacidad	NO	No es parte del servicio de Censos de Información Comercial.	**N/A**	**N/A**
A12.1.4	Separación de entornos operativos de desarrollo y prueba	NO	No aplica al servicio.	**N/A**	**N/A**

ID	CONTROLES SEGÚN LA NORMA ISO/IEC 27001	APLICABILIDAD (SÍ/NO)	MOTIVOS PARA ELECCIÓN/ NO ELECCIÓN	OBJETIVOS DEL CONTROL	MÉTODO DE IMPLEMENTACIÓN
A12.2	**Protección Contra el Malware**				
A12.2.1	Controles contra el malware	SI	Resguardar la integridad de los activos de información.	Desarrollar políticas para la protección, detección y recuperación contra malware.	Política y Procedimiento de Operaciones de Seguridad.
A12.3	**Backup**				
A12.3.1	Copia de seguridad de la información	SI	Proteger la integridad y disponibilidad de la información.	Crear y probar regularmente los respaldos de información de acuerdo a las políticas.	Política y Procedimiento de Operaciones de Seguridad.
A12.4	**Registro y Supervisión**				
A12.4.1	Registro de eventos	SI	Identificar los eventos que ocurren en el servicio.	Registrar los eventos del servicio de "Censos de Información Comercial" para su posterior análisis y sus respectivas acciones de mitigación.	Política y Procedimiento de Operaciones de Seguridad.
A12.4.2	Protección de información de registro	SI	Impedir la eliminación de los logs por personal no autorizado.	Proteger los logs de auditoría contra manipulación y accesos no autorizados.	
A12.4.3	Registros de administrador y operador	SI	Impedir el uso no autorizado de los sistemas de procesamiento de información.	Registrar las actividades del administrador y operador del sistema y revisarlas con regularidad.	
A12.4.4	Sincronización de la hora	SI	Usar la sincronización estándar del tiempo.	Sincronizar el sistema de "Censos de información Comercial" con una fuente precisa de tiempo.	
A12.5	**Control de Software Operativo**				
A12.5.1	Instalación de software en sistemas operativos	SI	Evitar la instalación de software sin licencia en los sistemas operativo.	Controlar la instalación de software en los sistemas operativos.	Política de Operaciones de Seguridad.
A12.6	**Gestión de Vulnerabilidades Técnicas**				
A12.6.1	Gestión de vulnerabilidades técnicas	SI	Identificar vulnerabilidades y mitigar cada una de ellas antes de que sean explotadas.	Obtener y utilizar la Información técnica de las vulnerabilidades y poder mitigar las mismas.	Política de Operaciones de Seguridad.
A12.6.2	Restricciones de instalación de software	SI	Evitar la instalación de programas que impidan el funcionamiento de normal de las aplicaciones del servicio.	Limitar la modificación de los paquetes de software sólo a cambios necesarios.	
A12.7	**Consideraciones de Auditoría de Sistemas de Información**				
A12.7.1	Controles de auditoría de sistemas de información	SI	Identificar las actividades que se realizan en cada	Activar los logs de auditoria de las aplicaciones y	Política de Operaciones de Seguridad.

ID	CONTROLES SEGÚN LA NORMA ISO/IEC 27001	APLICABILIDAD (SÍ/NO)	MOTIVOS PARA ELECCIÓN/ NO ELECCIÓN	OBJETIVOS DEL CONTROL	MÉTODO DE IMPLEMENTACIÓN
			uno de los sistemas de información.	sistemas operativos.	
A13	**SEGURIDAD DE LAS COMUNICACIONES**				
A13.1	**Gestión de la Seguridad de Red**				
A13.1.1	Controles de red	SI	Asegurar la disponibilidad y confidencialidad de las redes de comunicación del servicio.	Gestionar y controlar adecuadamente la red para protegerla de amenazas y mantener la seguridad de los sistemas y aplicaciones.	Política de Seguridad de las Comunicaciones.
A13.1.2	Seguridad de los servicios de red	SI		Administrar los servicios de red de forma segura, determinar un monitoreo periódico de los mismos y aplicar auditorías a estos servicios.	
A13.1.3	La segregación en las redes	NO	Las áreas están segregadas correctamente.	**N/A**	**N/A**
A13.2	**Transferencia de Información**				
A13.2.1	Políticas y procedimientos de transferencia de información	SI	Evitar la divulgación de información del servicio.	Asegurar el intercambio de información con la Distribuidora de Energía.	Política de Seguridad de las Comunicaciones.
A13.2.2	Acuerdos sobre la transferencia de información	SI		Establecer acuerdos de intercambio de información.	
A13.2.3	Mensajería electrónica	SI	Proteger la información del servicio transmitida mediante mensajería electrónica.	Establecer reglas y perfiles de uso de servicio de mensajería electrónica.	
A13.2.4	Acuerdos de confidencialidad o de no divulgación	SI	Garantizar la integridad, confidencialidad y autenticidad de la información del servicio.	Revisar periódicamente los acuerdos de confidencialidad o no divulgación para proteger la información.	
A14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**				
A14.1	**Los Requisitos de Seguridad de Sistemas de Información**				
A14.1.1	Análisis y especificación de requisitos de seguridad de información	NO	El servicio no comprende la adquisición, desarrollo o mantenimiento de desarrollo de software.	**N/A**	**N/A**
A14.1.2	Aseguramiento de servicios de aplicaciones en redes públicas	NO		**N/A**	**N/A**
A14.1.3	Protección de transacciones en servicios de aplicación	NO		**N/A**	**N/A**

ID	CONTROLES SEGÚN LA NORMA ISO/IEC 27001	APLICABILIDAD (SÍ/NO)	MOTIVOS PARA ELECCIÓN/ NO ELECCIÓN	OBJETIVOS DEL CONTROL	MÉTODO DE IMPLEMENTACIÓN
A14.2	**Seguridad en los Procesos de Desarrollo y Soporte**				
A14.2.1	Política de desarrollo seguro	NO	El servicio no comprende la adquisición, desarrollo o mantenimiento de desarrollo de software.	**N/A**	**N/A**
A14.2.2	Procedimientos de control de cambio de sistema	NO		**N/A**	**N/A**
A14.2.3	Revisión técnica de solicitudes después de cambios en la plataforma operativa	NO		**N/A**	**N/A**
A14.2.4	Las restricciones a cambios en los paquetes de software	NO		**N/A**	**N/A**
A14.2.5	Principios de ingeniería de sistemas seguros	NO		**N/A**	**N/A**
A14.2.6	Aseguramiento del entorno de desarrollo	NO		**N/A**	**N/A**
A14.2.7	Desarrollo externo	NO		**N/A**	**N/A**
A14.2.8	Pruebas de seguridad sistema	NO		**N/A**	**N/A**
A14.2.9	Pruebas de aceptación del sistema	NO		**N/A**	**N/A**
A14.3	**Datos de Prueba**				
A14.3.1	Protección de datos de prueba	NO	El servicio no comprende la adquisición, desarrollo o mantenimiento de desarrollo de software.	**N/A**	**N/A**
A15	**RELACIONES CON PROVEEDORES**				
A15.1	**Seguridad de Información en la Relación con Proveedores**				
A15.1.1	Política de seguridad de información para relaciones con proveedores	SI	Asegurar la confidencialidad e integridad de la información.	Establecer acuerdos de servicio con el proveedor.	Política de Relaciones con los Proveedores.
A15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	SI	Asegurar la confidencialidad e integridad de la información.		
A15.1.3	Cadena de suministro de las TIC	NO	No forma parte del desarrollo del servicio.	**N/A**	**N/A**
A15.2	**Gestión de la Prestación de Servicios de Proveedores**				
A15.2.1	Seguimiento y revisión de los servicios de proveedores	NO	Esta función no está comprendida en el desarrollo del servicio.	**N/A**	**N/A**
A15.2.2	Gestión de cambios en los servicios de proveedores	NO		**N/A**	**N/A**
A16	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE INFORMACIÓN**				

ID	CONTROLES SEGÚN LA NORMA ISO/IEC 27001	APLICABILIDAD (SÍ/NO)	MOTIVOS PARA ELECCIÓN/ NO ELECCIÓN	OBJETIVOS DEL CONTROL	MÉTODO DE IMPLEMENTACIÓN
A16.1	**Gestión de Incidencias y Mejoras de Seguridad de Información**				
A16.1.1	Responsabilidades y procedimientos	SI	Establecer cuáles son las personas y como deben actuar ante un incidente de seguridad de la información.	Establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida y efectiva en caso de un incidente de seguridad.	Política y Procedimiento de Gestión de Incidentes De Seguridad de Información.
A16.1.2	Comunicación de los incidentes de seguridad de información	SI	Comunicar sobre cualquier evento que se tenga sospecha de que sea un incidente de seguridad de la información.	Implementar un procedimiento formal para la comunicación de incidentes de seguridad.	
A16.1.3	Informes sobre debilidades de seguridad de información	NO	El área de sistemas es la encargada de llevar a cabo estas actividades.	**N/A**	**N/A**
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	NO		**N/A**	**N/A**
A16.1.5	Respuesta a incidentes de seguridad de la información	SI	Reaccionar de manera oportuna y adecuada ante los incidentes de seguridad de información.	Establecer un procedimiento de respuesta a incidentes de seguridad.	Política y Procedimiento de Gestión de Incidentes De Seguridad de Información.
A16.1.6	Aprendizaje de incidentes de seguridad de información	SI	Determinar a qué incidentes de seguridad de la información es más susceptible el servicio.	Identificar y calificar los diferentes tipos, regularidad de ocurrencia y costos de incidentes de seguridad.	
A16.1.7	Recolección de pruebas	SI	Almacenar las pruebas que involucran cada uno de los incidentes de seguridad para su respectivo análisis.	Recopilar y conservar las diferentes pruebas de los incidentes de la seguridad de información.	
A17	**ASPECTOS DE SEGURIDAD DE INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO**				
A17.1	**Continuidad de Seguridad de Información**				
A17.1.1	Planificación de la continuidad de la seguridad de información	SI	Incluir en el desarrollo del plan de continuidad de seguridad de información.	Direccionar los requerimientos de seguridad de información para desarrollar y mantener la continuidad del negocio.	Política de Aspectos de Seguridad de Información de la Gestión de Continuidad del Negocio.
A17.1.2	Implementación de la continuidad de seguridad de información	SI	Asegurar el funcionamiento correcto del plan de continuidad del negocio.	Asegurar la disponibilidad de la información en el tiempo requerido después de una interrupción o falla de los procesos del servicio.	
A17.1.3	Verificar, revisar y evaluar la continuidad de	SI		Probar y verificar que los planes de continuidad del	

ID	CONTROLES SEGÚN LA NORMA ISO/IEC 27001	APLICABILIDAD (SÍ/NO)	MOTIVOS PARA ELECCIÓN/ NO ELECCIÓN	OBJETIVOS DEL CONTROL	MÉTODO DE IMPLEMENTACIÓN
	seguridad de información			negocio para su correcto funcionamiento.	
A17.2	**Redundancia**				
A17.2.1	Disponibilidad de instalaciones de procesamiento de información	SI	Asegurar el funcionamiento continuo del procesamiento de la información.	Gestionar la disponibilidad de las instalaciones de procesamiento de información del servicio.	Política de Aspectos de Seguridad de Información de la Gestión de Continuidad del Negocio.
A18	**CUMPLIMIENTO**				
A18.1	**Cumplimiento de Requisitos Legales y Contractuales**				
A18.1.1	Identificación de la legislación aplicable y requisitos contractuales	SI	Identificar la legislación aplicable al servicio.	Documentar los estatutos legales, regulaciones y requerimientos del servicio.	Política de Cumplimiento.
A18.1.2	Derechos de propiedad intelectual	SI	Se aplica en el uso de licencias de software utilizado en el desarrollo del servicio.	Establecer las reglas en cuanto al uso de software licenciado.	Política y Procedimiento de Cumplimiento.
A18.1.3	Protección de registros	SI	Garantizar la confidencialidad e integridad de la información obtenida en el servicio.	Proteger los registros organizacionales de ser destruidos o falsificados en base a los estatutos, contratos y requerimientos del negocio.	Política de Cumplimiento.
A18.1.4	Privacidad y protección de datos personales	SI	Garantizar la confidencialidad de la información otorgada por parte de la Distribuidora de Energía.	Garantizar la protección y privacidad de los datos de acuerdo a la legislación del país vigente.	
A18.1.5	Reglamento de controles criptográficos	SI	Garantizar el uso adecuado de los controles criptográficos necesarios para la protección de información.	Desarrollar las políticas necesarias para gestionar los controles criptográficos.	Política de Criptografía.
A18.2	**Revisiones de Seguridad de Información**				
A18.2.1	Revisión independiente de seguridad de la información	NO	El área encargada de esta función es Administración.	**N/A**	**N/A**
A18.2.2	Cumplimiento de las políticas y estándares de seguridad	NO		**N/A**	**N/A**
A18.2.3	Revisión del cumplimiento técnico	NO		**N/A**	**N/A**

Tabla 53 – Declaración de Aplicabilidad.
Fuente: Sistema de Gestión de Seguridad de la Información ISO/ IEC 27001 2013.

3.5 PLAN DE ACCIÓN CON RECOMENDACIONES PARA LA IMPLANTACIÓN DE UN SGSI EN LA EMPRESA

El Plan de Acción para la Implementación del SGSI se definirá a partir de la documentación y considerando el Enunciado de Aplicabilidad en función de:

- Requerimientos Legales y Organizacionales.
- Alcance y Límites del SGSI.
- Política del SGSI.

Para que el SGSI sea diseñado de acuerdo a la norma ISO/IEC 27001:2013, se acoplará con los dominios, controles y sub controles existentes en dicha norma, considerando además el análisis de amenazas y vulnerabilidades para determinar el riesgo, de manera que se definan claramente que políticas y procedimientos serán necesarios para mantener un alto nivel de seguridad de información en el servicio.

El resultado de este análisis indica que será necesario considerar políticas y procedimientos para los dominios de la ISO/IEC 27001:2013 descritos a continuación:

No.	DOMINIO	POLÍTICA	PROCEDIMIENTO	IMPACTO PARA LA SEGURIDAD DE INFORMACIÓN DEL SERVICIO
5	Políticas de Seguridad de Información	X		ALTO
6	Organización de la Seguridad de Información	X		ALTO
7	Seguridad de Recursos Humanos	X	X	ALTO

No.	DOMINIO	POLÍTICA	PROCEDIMIENTO	IMPACTO PARA LA SEGURIDAD DE INFORMACIÓN DEL SERVICIO
8	Gestión de Activos	X	X	ALTO
9	Control de Acceso	X	X	ALTO
10	Criptografía	X		MEDIO
11	Seguridad Física y Ambiental	X	X	MEDIO
12	Operaciones de Seguridad	X	X	ALTO
13	Seguridad de las Comunicaciones	X		MEDIO
15	Relaciones con Proveedores	X		ALTO
16	Gestión de Incidentes de Seguridad de Información	X	X	ALTO
17	Aspectos de Seguridad de Información de la Gestión de Continuidad del Negocio	X		MEDIO
18	Cumplimiento	X	X	MEDIO

Tabla 54 – Plan de Implementación del SGSI en el Servicio.
Fuente: Sistema de Gestión de Seguridad de la Información ISO/ IEC 27001 2013.

La columna "*IMPACTO PARA LA SEGURIDAD DE LA INFORMACIÓN DEL SERVICIO"* indica el nivel de consecuencias que pueden afectar a la seguridad de la información si no se cumplen las políticas y procedimientos necesarios.

CAPÍTULO 4: IMPLEMENTACIÓN DEL SGSI DEL SERVICIO DE LEVANTAMIENTO CATASTRAL AUTOMATIZADO

En los capítulos anteriores se han identificado:

- Riesgos, amenazas y vulnerabilidades que pueden afectar a la seguridad de la información en el servicio.
- Requerimientos que deben ser cumplidos para mantener un nivel aceptable y salvaguardar dicha información.
- La metodología de tratamiento de riesgos.
- El plan de implementación del SGSI.

En el presente capítulo, se establecerán formalmente políticas y procedimientos que deben cumplir todos los activos y partes involucradas en el desarrollo del servicio para que el SGSI funcione de forma adecuada.

4.1 SELECCIÓN DE CONTROLES A IMPLEMENTAR

Los controles a implementar en el servicio se describen en a continuación:

No.	DOMINIO	SUBDOMINIO	CONTROLES	POLÍTICA	PROCEDIMIENTO
5	POLÍTICAS DE SEGURIDAD DE INFORMACIÓN	Dirección de Gestión de Seguridad de Información	Políticas de Seguridad de Información (SI)	X	
			Revisión de Políticas de SI		
6	ORGANIZACIÓN DE LA SEGURIDAD DE INFORMACIÓN	Organización Interna	Roles y Responsabilidades de SI	X	
			Segregación de Deberes		
			Contacto con Grupos de Interés Especial		
			Seguridad de Información en la Gestión de Proyectos		
		Dispositivos Móviles y	Política de Uso de Dispositivos		

No.	DOMINIO	SUBDOMINIO	CONTROLES	POLÍTICA	PROCEDIMIENTO
		Teletrabajo	Móviles		
			Teletrabajo		
7	SEGURIDAD DE RECURSOS HUMANOS	Durante el Empleo	Responsabilidades de la Administración	X	X
			Concienciación, Educación y entrenamiento sobre SI		
			Proceso Disciplinario		
		Terminación y Cambio de Empleo	Terminación o cambio de responsabilidades laborales		
8	GESTIÓN DE ACTIVOS	Responsabilidad de Activos	Inventario de Activos	X	X
			Propiedad de Activos		
			Uso Aceptable de Activos		
			Categorías de Activos		
		Clasificación de Información	Clasificación de Información		
			Etiquetado de Información		
		Manejo del Soporte	Gestión de Soportes Extraíbles		
			Eliminación de medios de comunicación		
			Transferencia de Medios Físicos		
9	CONTROL DE ACCESO	Requerimientos del Negocio de Control de Acceso	Política de Controle de Acceso	X	X
			Acceso a Redes y Servicios de Red		
		Responsabilidades del Usuario	Uso de Claves		
10	CRIPTOGRAFÍA	Controles Criptográficos	Política sobre el Uso de Controles Criptográficos	X	
			Gestión de Claves		
11	SEGURIDAD FÍSICA Y AMBIENTAL	Áreas Seguras	Perímetro de Seguridad Física	X	X
			Controles de Entrada Física		
			Asegurar Oficinas, Salas e Instalaciones		
			Protección contra Amenazas Externas y Ambientales		
			Trabajo en Zonas Seguras		
		Equipo	Ubicación y Protección de Equipo		
			Apoyo a servicios Públicos		
			Seguridad del Cableado		
			Mantenimiento de equipos		

No.	DOMINIO	SUBDOMINIO	CONTROLES	POLÍTICA	PROCEDIMIENTO
			Seguridad de equipos y activos fuera de las instalaciones		
			Política de Escritorio y Pantalla Limpios		
12	OPERACIONES DE SEGURIDAD	Protección contra Malware	Controles contra malware	X	X
		Backup	Copias de seguridad de Información		
		Registro y Supervisión	Registro de Eventos		
			Protección de Información de Registro		
			Registros de Administrador y Operador		
			Sincronización de la Hora		
		Control de Software Operativo	Instalación de Software en SO		
		Gestión de Vulnerabilidades Técnicas	Gestión de Vulnerabilidades Técnicas		
			Restricciones de Instalación de Software		
		Consideraciones de Auditoría en Sistemas de Información	Controles de Auditoría de Sistemas de Información		
13	SEGURIDAD DE LAS COMUNICACIONES	Gestión de la Seguridad de Red	Controles de Red	X	
			Seguridad de los Servicios de Red		
		Transferencia de Información	Políticas y Procedimientos de Transferencia de Información		
			Acuerdos de Transferencia de Información		
			Mensajería Electrónica		
			Acuerdos de Confidencialidad o de No Divulgación		
15	RELACIONES CON PROVEEDORES	Seguridad de Información en la Relación con Proveedores	Política de SI para Relaciones con Proveedores	X	
			Abordaje de la SI en Acuerdos con Proveedores		
16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE INFORMACIÓN	Gestión de Incidentes y Mejoras de Seguridad de Información	Responsabilidades y Procedimientos	X	X
			Comunicación de Incidentes de SI		
			Respuesta a Incidentes de SI		
			Aprendizaje de Incidentes de SI		
			Recolección de Pruebas		
17	ASPECTOS DE SEGURIDAD DE INFORMACIÓN DE	Continuidad de Seguridad de Información	Planificación de la Continuidad de SI	X	
			Implementación de		

No.	DOMINIO	SUBDOMINIO	CONTROLES	POLÍTICA	PROCEDIMIENTO
	LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO		la Continuidad de SI		
			Verificación, Revisión y Evaluación de la Continuidad de SI		
		Redundancia	Disponibilidad de Instalaciones de Procesamiento de Información		
18	CUMPLIMIENTO	Cumplimiento de Requisitos Legales y Contractuales	Identificación de Legislación Aplicable y Requisitos Contractuales	X	X
			Derechos de Propiedad Intelectual		
			Protección de Registros		
			Privacidad y Protección de Datos Personales		
			Reglamento de Controles Criptográficos		

Tabla 55 – Controles a Implementar en el Servicio.
Fuente: Sistema de Gestión de Seguridad de la Información ISO/ IEC 27001 2013.

4.2 ELABORACIÓN DE POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD

A continuación se describirá en que consiste cada uno de los controles a implementar, descritos en el punto anterior:

4.2.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta política tiene por objetivo proporcionar las reglas y lineamientos básicos para la gestión de la seguridad de información, se aplica a todo el alcance del SGSI y sus usuarios son todos los trabajadores del servicio.

En la actualidad el activo más importante de las organizaciones es la información, por este motivo se está en la obligación de precautelar su confidencialidad, integridad y disponibilidad, para mantener la confiabilidad y reputación frente a sus clientes.

Las organizaciones están expuestas a distintos ataques para realizar fraudes o sabotaje, de acuerdo a como ha ido evolucionando la tecnología, se han ido perfeccionando estos mecanismos, entre los más conocidos se tienen: los ataques de denegación de servicio, virus informáticos y malware, etc. Adicionalmente se debe tomar en consideración el riesgo de eventos de seguridad que existirían en caso de desastres naturales.

La Política de la Seguridad de la Información provee reglas generales de seguridad, para regular las actividades del servicio de "Censos de Información Comercial", de esta manera se mantenga un nivel adecuado de seguridad de los activos de información; esta política debe ser cumplida por el personal interno como terceros.

Los principales responsables para monitorear el cumplimiento de estas políticas son:

- Gerente de Proyecto.
- Líder de Proyecto.

Para mayor información revisar el "**Anexo G - Política de Seguridad de la Información"**.

4.2.2 POLÍTICA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Esta política tiene por objetivo proporcionar los lineamientos necesarios para la utilización de los activos y recursos de procesamiento de información en el servicio, se aplica a todo el alcance del SGSI y sus usuarios son todos los trabajadores de la empresa de servicios "XYZ". Los principales responsables para monitorear el cumplimiento de estas políticas son:

- Gerente de Proyecto.

- Líder de Proyecto.
- Supervisor de Procesamiento de Información.
- Supervisor de Campo.

Para mayor información revisar el **"Anexo H - Política de Organización de la Seguridad de la Información"**.

4.2.3 POLÍTICA DE SEGURIDAD DE RECURSOS HUMANOS

Estas políticas tienen por objetivo definir las responsabilidades y reglas para para mantener un alto grado de confidencialidad, integridad y disponibilidad de la información, mediante el control de los recursos humanos involucrados en el servicio; se aplican a todo el alcance del SGSI y sus usuarios son todos los trabajadores de la empresa de servicios "XYZ". Los principales responsables para monitorear el cumplimiento de estas políticas son:

- Gerente de Proyecto.
- Líder de Proyecto.
- Supervisor de Procesamiento de Información.
- Supervisor de Campo.

Para mayor información revisar el **"Anexo I - Política de Seguridad de Recursos Humanos"**.

4.2.3.1 Procedimiento de Seguridad de Recursos Humanos

Los procedimientos detallados en este control han sido creados para protejer la información utilizada en el servicio, en lo referente al desarrollo de las actividades de los trabajadores involucrados en su desarrollo. Los encargados de ejecutar el procedimiento son:

- Gerente de Proyecto

- Líder de Proyecto

Para mayor información revisar el **"Anexo J - Procedimiento de Seguridad de Recursos Humanos"**.

4.2.4 POLÍTICA DE GESTIÓN DE ACTIVOS

Esta política tiene por objetivo garantizar la protección de la información mediante reglas básicas de manejo de activos, se aplica a todo el alcance del SGSI y sus usuarios son todos los trabajadores de la empresa de servicios "XYZ". Los principales responsables para monitorear el cumplimiento de estas políticas son:

- Líder de Proyecto.
- Supervisor de Procesamiento de Información.
- Supervisor de Campo.

Para mayor información revisar el **"Anexo K - Política de Gestión de Activos"**.

4.2.4.1 Procedimiento de Gestión de Activos

Estos procedimientos han sido creados para alcanzar un alto nivel de seguridad de la información utilizada por los activos del servicio, de manera que no se presenten problemas al momento de trabajar con la misma. Se han designado a los siguientes roles como los responsables de su cumplimiento:

- Líder de Proyecto.
- Supervisor de Campo.
- Supervisor de Procesamiento Información.
- Personal de Campo y Oficina.

Para mayor información revisar el **"Anexo L - Procedimiento de Gestión de Activos"**.

4.2.5 POLÍTICA DE CONTROL DE ACCESO

Esta política tiene por objetivo proporcionar reglas para el acceso a los diferentes sistemas, equipos, instalaciones e información, de acuerdo a la seguridad de la información y necesidades del negocio. Se aplica a todo el alcance del SGSI y sus usuarios son todos los trabajadores del servicio. Los principales responsables para monitorear su cumplimiento son:

- Gerente de Proyecto.
- Líder de Proyecto.
- Supervisor de Procesamiento de Información.
- Supervisor de Campo.
- Área de Sistemas (funciona de forma independiente al servicio).
- Área de Recursos Humanos (funciona de forma independiente al servicio).

Para mayor información revisar el **"Anexo M - Política de Control de Acceso"**.

4.2.5.1 Procedimiento de Control de Acceso

El objetivo de estos procedimientos es mantener un nivel confiable de integridad, confidencialidad y disponibilidad de los activos de información, en el desarrollo de las actividades del servicio a través del control de acceso a recursos. Se han designado a los siguientes roles como los responsables de su ejecución:

- Líder de Proyecto.
- Supervisor de Procesamiento de Información.
- Área de Sistemas (funciona de forma independiente al servicio).
- Personal de Campo y Oficina.

Para mayor información revisar el **"Anexo N - Procedimiento de Control de Acceso"**.

4.2.6 POLÍTICA DE CRIPTOGRAFÍA

Esta política tiene por objetivo proporcionar reglas para el uso de controles y claves criptográficas, se aplica a todo el alcance del SGSI y sus usuarios son todos los trabajadores del servicio. Los responsables de monitorear su cumplimiento son:

- Gerente de Proyecto.
- Líder de Proyecto.

Para mayor información revisar el **"Anexo O - Política de Criptografía"**.

4.2.7 POLÍTICA DE SEGURIDAD FÍSICA Y AMBIENTAL

Esta política tiene por objetivo proporcionar las reglas para la seguridad física y ambiental en el servicio, se aplica a todo el alcance del SGSI y sus usuarios son todos los trabajadores del mismo. Los responsables del monitoreo y mantenimiento de estas políticas son:

- Líder de Proyecto.
- Supervisor de Campo.
- Supervisor de Procesamiento de Información.
- Gestores de Campo.
- Dibujante.
- Asistentes de Información.

Para mayor información revisar el "**Anexo P - Política de Seguridad Física y Ambiental"**.

4.2.7.1 Procedimiento de Seguridad Física y Ambiental

El objetivo de estos procedimientos es establecer un alto nivel de integridad, confidencialidad y disponibilidad de los activos de información en el desarrollo de

las actividades del servicio, controlando la seguridad física y ambiental. Se han designado a los siguientes roles como los responsables de su cumplimiento:

- Líder de Proyecto.
- Supervisor de Campo.

Para mayor información revisar el **"Anexo Q - Procedimiento de Seguridad Física y Ambiental"**.

4.2.8 POLÍTICA DE OPERACIONES DE SEGURIDAD

Esta política tiene por objetivo garantizar el funcionamiento adecuado de los activos y sistemas de procesamiento de información para su mantenimiento seguro, se aplica a todo el alcance del SGSI y sus usuarios son todos los trabajadores del servicio. Los responsables de monitorear el cumplimiento y resultados de la aplicación de estas políticas son:

- Líder de Proyecto.
- Supervisor de Procesamiento de Información.

Para mayor información revisar el **"Anexo R - Política de Operaciones de Seguridad"**.

4.2.8.1 Procedimiento de Operaciones de Seguridad

El objetivo de estos procedimientos es direccionar el trabajo responsable de los activos involucrados en el desarrollo del servicio, de manera que se proteja la integridad, disponibilidad y confidencialidad de la información. Se han designado a los siguientes roles como los responsables de su cumplimiento:

- Líder de Proyecto.
- Supervisor de Procesamiento de Información.

- Área de Sistemas (independiente al desarrollo del servicio).
- Personal de Campo y Oficina.

Para mayor información revisar el **"Anexo S - Procedimiento de Operaciones de Seguridad"**.

4.2.9 POLÍTICA DE SEGURIDAD DE LAS COMUNICACIONES

Esta política tiene por objetivo precautelar la seguridad de la información y el software cuando son utilizados o intercambiados, se aplica a todo el alcance del SGSI y sus usuarios son todos los trabajadores del servicio. Los principales responsables de monitorear el cumplimiento y efectividad de estas políticas son:

- Gerente de Proyecto.
- Líder de Proyecto.

Para mayor información revisar el "**Anexo T - Política de Seguridad de las Comunicaciones"**.

4.2.10 POLÍTICA DE RELACIONES CON PROVEEDORES

Esta política tiene por objetivo proporcionar las reglas básicas para la relación con los proveedores, con un enfoque para asegurar la información del servicio. Se aplica a todo el alcance del SGSI y sus usuarios son las personas responsables de las relaciones con los proveedores de servicios. Los principales responsables de monitorear el cumplimiento y efectividad de estas políticas son:

- Gerente de Proyecto.
- Líder de Proyecto.

Para mayor información revisar el "**Anexo U - Política de Relaciones con Proveedores"**.

4.2.11 POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE INFORMACIÓN

El objetivo de esta política es establecer los controles necesarios para gestionar los incidentes que afecten a la seguridad de la información, para minimizar los daños y evitar pérdidas o deficiencias en el tratamiento de la misma. Se han designado a los siguientes roles como los responsables de monitorear el cumplimiento de dichos procedimientos:

- Líder de Proyecto.
- Área de Sistemas (independiente al servicio).

Para mayor información revisar el **"Anexo V - Polìtica de Incidentes de Seguridad"**.

4.2.11.1 Procedimiento de Gestión de Incidentes de Seguridad de Información

Este procedimiento tiene por objetivo garantizar la detección, reacción y respuesta ante incidentes de seguridad de información, se aplica a todo el alcance del SGSI y sus usuarios son todos los trabajadores del servicio. El principal responsable de ejecutarlo es el Líder de Proyecto.

Para mayor información revisar el **"Anexo W - Procedimiento de Incidentes de Seguridad"**.

4.2.12 POLÍTICA DE CONTINUIDAD DEL NEGOCIO

Esta política tiene por objetivo proporcionar las reglas básicas para gestión de la continuidad del negocio, se aplica a todo el alcance del SGSI y sus usuarios son todos los trabajadores del servicio, como también todos los proveedores de servicios relacionados con el manejo de información. Los responsables de estas políticas son:

- Gerente de Proyecto.
- Líder de Proyecto.

Para mayor información revisar el "**Anexo X - Política de Continuidad del Negocio"**.

4.2.13 POLÍTICA DE CUMPLIMIENTO

Esta política tiene por objetivo proporcionar las reglas básicas para la identificación de los requisitos legales de acuerdo a las normas vigentes para el servicio, se aplica a todo el alcance del SGSI. Los responsables de monitorear su cumplimiento y efectividad son:

- Gerente de Proyecto.
- Líder de Proyecto.

Para mayor información revisar el **"Anexo Y - Política de Cumplimiento"**.

4.2.13.1 Procedimiento de Cumplimiento

El objetivo de estos procedimientos es precautelar la seguridad de la información y evitar futuras sanciones por entes reguladores por incumplimiento de normas legales, organizacionales o de cualquier otra índole en el servicio. El Líder de Proyecto es el principal responsable de su ejecución.

Para mayor información revisar el **"Anexo Z - Procedimiento de Cumplimiento"**.

4.3 IMPLANTACIÓN DE CONTROLES PARA EL SGSI

La Tabla 56 nos indica el procedimiento de implantación de la norma ISO/IEC 27001:2013 en el servicio de Censos de Información Comercial, tomando en cuenta las siguientes consideraciones:

La información de la columna *PORCENTAJE DE CUMPLIMIENTO DE CONTROLES (%)* indica si existen reglas formalizadas para el cumplimiento de los controles de seguridad de información mencionados en la columna *CONTROLES SEGÚN NORMA ISO/IEC 27001*, y el nivel de efectividad de las mismas. Esta columna ha sido completada en función de la experiencia laboral del área administrativa sobre el servicio, es decir, el Gerente de Proyecto y el Líder de Proyecto, además de la revisión realizada por los autores del presente proyecto de titulación a cada uno de los procesos que conforman el servicio.
La columna *RESPONSABLES* indica al personal que forma parte del desarrollo del servicio, que se hará cargo de supervisar el cumplimiento y monitorear el funcionamiento de las medidas tomadas para cumplir con los controles necesarios.

Finalmente, en la columna *MÉTODO DE IMPLEMENTACIÓN* se describe las medidas seleccionadas para que la información del servicio sea protegida de los riesgos identificados anteriormente, mediante el cumplimiento de los controles de la ISO 27001:2013:

ID	Controles según Norma ISO/IEC 27001	Porcentaje de Cumplimiento de Controles (%)	Responsables	Método de Implementación	Fecha Límite de Implementación
A5	**Políticas de Seguridad de Información**				
A5.1	**Dirección de la Gestión de la Seguridad de Información**				
A5.1.1	Políticas de seguridad de información	Menos de 10%	Gerente de Proyecto. Líder de Proyecto.	Se implementará formalmente (por primera vez) políticas para cumplir con los controles mencionados.	29/02/16
A5.1.2	Revisión de políticas de seguridad de información	Menos de 10%			
A6	**Organización de la Seguridad de Información**				
A6.1	**Organización Interna**				

ID	Controles según Norma ISO/IEC 27001	Porcentaje de Cumplimiento de Controles (%)	Responsables	Método de Implementación	Fecha Límite de Implementación
A6.1.1	Roles y responsabilidades de seguridad de información	15%	Gerente de Proyecto. Líder de Proyecto. Supervisor de Procesamiento de Datos. Supervisor de Campo.	Se implementarán políticas para: • Definir y formalizar roles y responsabilidades. • Formalizar la segregación de deberes. • Tratados profesionales con grupos especializados en seguridad de información. Gestionar la seguridad de Información (SI) en proyectos relacionados al servicio.	29/02/16
A6.1.2	Segregación de deberes	80%			
A6.1.4	Contacto con grupos de interés especial	Menos de 10%			
A6.1.5	Seguridad de información en la gestión de proyectos	Menos de 10%			
A6.2	**Dispositivos Móviles y Teletrabajo**				
A6.2.1	Política de uso de dispositivos móviles	80%	Gerente de Proyecto. Líder de Proyecto. Supervisor de Procesamiento de Datos. Supervisor de Campo.	Existen reglas definidas para el uso de dispositivos móviles pero no están formalizadas. El control sobre el uso de teletrabajo es mínimo, por ello se definirán formalmente reglas para su uso.	23/12/15
A6.2.2	Teletrabajo	20%			
A7	**Seguridad de Recursos Humanos**				
A7.1	**Durante el Empleo**				
A7.2.1	Responsabilidades de la Administración	60%	Gerente de Proyecto. Líder de Proyecto. Supervisor de Procesamiento de Datos. Supervisor de Campo.	Las normas utilizadas para el cumplimiento de los controles presentes son insuficientes, por tal razón se han formalizado políticas para: • Responsabilidades de Administración. • Capacitación de personal.	23/12/15
A7.2.2	Concienciación, educación y entrenamiento sobre la seguridad de la información	30%			
A7.2.3	Proceso disciplinario	80%			
A7.3	**Terminación y Cambio de Empleo**				
A7.3.1	Terminación o cambio de responsabilidades laborales	80%	Gerente de Proyecto. Líder de Proyecto.	Existen normas y reglas para la terminación y cambio de responsabilidades laborales, las cuales serán formalizadas en políticas.	31/07/2015
A8	**Gestión de Activos**				
A8.1	**Responsabilidad de Activos**				
A8.1.1	Inventario de activos	20%	Líder de Proyecto. Supervisor de Campo. Supervisor de Procesamiento de Datos.	No existe un documento formal de inventario de activo ni responsabilidades de los mismos. Se formalizará un documento con políticas para: • Inventariar activos. Responsabilidades sobre los activos.	23/12/15
A8.1.2	Propiedad de activos	80%			
A8.1.3	Uso aceptable de activos	80%			
A8.1.4	Categorías de activos	20%			
A8.2	**Clasificación de Información**				
A8.2.1	Clasificación de la información	80%	Líder de Proyecto.	Existen normas y reglas claras para clasificar y categorizar la información	31/07/2015
A8.2.2	Etiquetado de	60%			

ID	Controles según Norma ISO/IEC 27001	Porcentaje de Cumplimiento de Controles (%)	Responsables	Método de Implementación	Fecha Límite de Implementación
	información		Supervisor de Procesamiento de Datos.	utilizada en el desarrollo del servicio, las cuales serán formalizadas en una Política de Clasificación de Información.	
A8.3	**Manejo de Soporte**				
A8.3.1	Gestión de soportes extraíbles	80%	Líder de Proyecto. Supervisor de Campo. Supervisor de Procesamiento de Datos.	Existen reglas que necesitan ser formalizadas para: • Gestión de soportes extraíbles. • Transferencia de medios físicos. Además se creará un documento formal que controle y direccione la eliminación de medios de comunicación.	31/07/2015
A8.3.2	Eliminación de medios de comunicación	Menos de 10%			
A8.3.3	Transferencia de medios físicos	80%			
A9	**Control de Acceso**				
A9.1	**Requerimientos del Negocio de Control de Acceso**				
A9.1.1	Política de control de acceso	60%	Gerente de Proyecto. Líder de Proyecto. Supervisor de Procesamiento de Datos. Supervisor de Campo.	Existen normas para gestionar el control de acceso pero no son suficientes para cumplir el control correspondiente y no están formalizadas; por otro lado, los controles implementados para el uso de la red son mínimos. Por esta razón se han creado y formalizado políticas para cumplir con estos controles.	23/12/15
A9.1.2	Acceso a redes y servicios de red	20%			
A9.3	**Responsabilidades de Usuario**				
A9.3.1	Uso de información secreta de autenticación (Uso de claves)	Menos de 10%	Gerente de Proyecto. Líder de Proyecto.	Se crearán normas para cumplir responsablemente con el uso de contraseñas.	29/02/16
A10	**Criptografía**				
A10.1	**Controles Criptográficos**				
A10.1.1	Política sobre el uso de controles criptográficos	Menos de 10%	Gerente de Proyecto. Líder de Proyecto.	Se crearán políticas para el uso y gestión de la criptografía en el desarrollo del servicio.	29/02/16
A10.1.2	Gestión de claves criptográficas	Menos de 10%			
A11	**Seguridad Física y Ambiental**				
A11.1	**Áreas Seguras**				
A11.1.1	Perímetro de seguridad física	Menos de 10%	Gerente de Proyecto. Líder de Proyecto. Supervisor de Procesamiento de Datos. Supervisor de Campo. Gestores de Campo. Dibujantes. Asistentes de Información.	Los controles existentes para gestionar la seguridad física y ambiental son mínimos, por lo que se crearán reglas para gestionar: • El perímetro de seguridad física en oficinas, incluidas vías de entrada y salida. • Aseguramiento de información en relación a amenazas de la sociedad del medio ambiente.	29/02/16
A11.1.2	Controles de entrada físicas	Menos de 10%			
A11.1.3	Asegurar oficinas, salas e instalaciones	20%			
A11.1.4	Protección contra amenazas externas y ambientales	Menos de 10%			
A11.1.5	Trabajo en zonas seguras	Menos de 10%			

ID	Controles según Norma ISO/IEC 27001	Porcentaje de Cumplimiento de Controles (%)	Responsables	Método de Implementación	Fecha Límite de Implementación
A11.2	**Equipo**				
A11.2.1	Ubicación y protección del equipo	60%	Gerente de Proyecto. Líder de Proyecto.	Existen normas para el uso seguro de equipos, pero no son suficientes para cumplir con los presentes controles, por lo que se crearán y formalizarán políticas para: • Gestionar la ubicación y el acceso a servicios de equipos cableado. • Dar mantenimiento adecuado y periódico a los equipos. • Formalizar reglas de escritorio y pantalla limpia.	23/12/15
A11.2.2	Apoyo a los servicios públicos	40%			
A11.2.3	Seguridad del cableado	20%			
A11.2.4	Mantenimiento de equipo	60%			
A11.2.6	Seguridad de equipo y activos fuera de las instalaciones	60%			
A11.2.9	Política de escritorio y pantalla limpia	80%			
A12	**Operaciones de Seguridad**				
A12.2	**Protección contra Malware**				
A12.2.1	Controles contra el malware	80%	Líder de Proyecto. Supervisor de Procesamiento de Datos.	Se necesita formalizar las reglas existentes para gestionar la amenaza de códigos maliciosos.	31/07/2015
A12.3	**Backup**				
A12.3.1	Copia de seguridad de la información	80%	Líder de Proyecto. Supervisor de Procesamiento de Datos.	Se necesita formalizar las reglas existentes para gestionar la creación y manejo de backups.	31/07/2015
A12.4	**Registro y Supervisión**				
A12.4.1	Registro de eventos	10%	Líder de Proyecto. Supervisor de Procesamiento de Datos.	Prácticamente no se han definido normas y reglas para gestionar logs (registros) necesarios para realizar auditorías en caso que ocurran eventos de seguridad de información. Por esta razón, se crearán políticas para: • Gestión de logs. • Sincronización de la hora.	29/02/16
A12.4.2	Protección de información de registro	10%			
A12.4.3	Registros de administrador y operador	10%			
A12.4.4	Sincronización de la hora	Menos de 10%			
A12.5	**Control de Software Operativo**				
A12.5.1	Instalación de software en sistemas operativos	80%	Líder de Proyecto. Supervisor de Procesamiento de Datos.	Se formalizarán los controles existentes para la instalación de software en SO.	31/07/2015
A12.6	**Gestión de Vulnerabilidades Técnicas**				
A12.6.1	Gestión de vulnerabilidades técnicas	60%	Líder de Proyecto. Supervisor de Procesamiento de Datos.	Se incluirán y formalizarán normas y reglas para administrar y tratar de forma efectiva vulnerabilidades técnicas que pueden afectar a la seguridad de información.	31/07/2015
A12.6.2	Restricciones de instalación de software	80%			
Consideraciones de Auditoría de Sistemas de Información					
A12.7.1	Controles de auditoría de sistemas de información	10%	Líder de Proyecto.	Se crearán formalmente políticas para gestionar	29/02/16

ID	Controles según Norma ISO/IEC 27001	Porcentaje de Cumplimiento de Controles (%)	Responsables	Método de Implementación	Fecha Límite de Implementación
			Supervisor de Procesamiento de Datos.	controles de auditoría de sistemas de información.	
A13	**Seguridad de las Comunicaciones**				
A13.1	**Gestión de Seguridad de Red**				
A13.1.1	Controles de red	20%	Gerente de Proyecto. Líder de Proyecto.	Las reglas existentes no son suficientes para gestionar la seguridad en la red, por lo tanto, se crearán nuevas reglas para: • Gestión para la implementación y administración de controles de red y sus servicios.	29/02/16
A13.1.2	Seguridad de los servicios de red	20%			
A13.2	**Transferencia de Información**				
A13.2.1	Políticas y procedimientos de transferencia de información	80%	Gerente de Proyecto. Líder de Proyecto.	Se formalizarán los controles existentes para: • Gestión de transferencia de información. • Gestión de mensajería electrónica. Además se actualizarán y crearán controles para el manejo de acuerdos de confidencialidad.	31/07/2015
A13.2.2	Acuerdos sobre la transferencia de información	80%			
A13.2.3	Mensajería electrónica	80%			
A13.2.4	Acuerdos de confidencialidad o de no divulgación	20%			
A15	**Relaciones con Proveedores**				
A15.1	**Seguridad de Información en Relaciones con Proveedores**				
A15.1.1	Política de seguridad de información para relaciones con proveedores	Menos de 10%	Líder de Proyecto.	Se crearán controles para gestionar y afianzar la seguridad de información en las relaciones y acuerdos existentes o por iniciar con los proveedores de servicios.	29/02/16
A15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	Menos de 10%			
A16	**Gestión de Incidentes de Seguridad de Información**				
A16.1	**Gestión de Incidentes y Mejoras de Seguridad de Información**				
A16.1.1	Responsabilidades y procedimientos	60%	Líder de Proyecto.	Se actualizarán y crearán nuevos procedimientos para: • Asignar responsabilidades y crear procedimientos en el caso que ocurran incidentes de seguridad de información. • Comunicar la ocurrencia de incidentes de seguridad de información a los responsables correspondientes. Además se crearán procedimientos para: • Recolectar información útil para el aprendizaje de incidentes en caso que ocurran nuevamente en un	29/02/16
A16.1.2	Comunicación de los incidentes de seguridad de información	60%			
A16.1.5	Respuesta a incidentes de seguridad de la información	20%			
A16.1.6	Aprendizaje de incidentes de seguridad de información	Menos de 10%			
A16.1.7	Recolección de pruebas	Menos de 10%			

ID	Controles según Norma ISO/IEC 27001	Porcentaje de Cumplimiento de Controles (%)	Responsables	Método de Implementación	Fecha Límite de Implementación
				futuro. • Recolección de pruebas de la ocurrencia de incidentes de seguridad de información.	
A17	**Aspectos de Seguridad de Información de la Gestión de Continuidad del Negocio**				
A17.1	**Continuidad de Seguridad de Información**				
A17.1.1	Planificación de la continuidad de la seguridad de información	20%	Gerente de Proyecto. Líder de Proyecto.	Se crearán políticas para planificar la continuidad de la seguridad de información.	23/12/15
A17.1.2	Implementación de la continuidad de seguridad de información	60%		Se actualizarán y crearán políticas para implementar la continuidad de la seguridad de información y métodos para su respectiva revisión y evaluación.	
A17.1.3	Verificar, revisar y evaluar la continuidad de seguridad de información	60%			
A17.2	**Redundancia**				
A17.2.1	Disponibilidad de instalaciones de procesamiento de información	Menos de 10%	Gerente de Proyecto. Líder de Proyecto.	Se implementarán políticas para revisar e investigar acerca de los requerimientos necesarios de las instalaciones de procesamiento de información.	29/02/16
A18	**Cumplimiento**				
A18.1	**Cumplimiento de Requisitos Legales y Contractuales**				
A18.1.1	Identificación de la legislación aplicable y requisitos contractuales	Menos de 10%	Gerente de Proyecto. Líder de Proyecto.	Se implementarán políticas para la identificación y control de cumplimiento de: • La legislación aplicable. • Derechos de Propiedad Intelectual. • Protección de registros. • Privacidad de datos personales. • Uso de controles criptográficos.	29/02/16
A18.1.2	Derechos de propiedad intelectual	Menos de 10%			
A18.1.3	Protección de registros	Menos de 10%			
A18.1.4	Privacidad y protección de datos personales	10%			
A18.1.5	Reglamento de controles criptográficos	Menos de 10%			

Tabla 56 – Tabla de Seguimiento de Implementación de Controles en el Servicio.
Fuente: Sistema de Gestión de Seguridad de la Información ISO/ IEC 27001 2013.

CAPÍTULO 5: CONCLUSIONES Y RECOMENDACIONES

A partir del diseño e implementación de un SGSI para el servicio de “Censos de Información Comercial” se puede concluir y recomendar:

5.1 CONCLUSIONES

- El servicio de “Censos de Información Comercial” tiene políticas y procedimientos de seguridad de información que no se encuentran formalizados e implementados en su totalidad, lo cual generan vulnerabilidades que pueden ser aprovechadas para la obtención de información por personas no autorizadas.

- Las políticas y procedimientos pueden variar de acuerdo a la Distribuidora de Energía y la provincia donde se brinde el servicio “Censos de Información Comercial”.

- Las vulnerabilidades encontradas en el presente proyecto son válidas y similares a las que se van obtener en el región Costa, ya que en la región Sierra estarían inmersos otros tipos de desastres naturales que son más probables por su ubicación geográfica.

- Es importante la identificación de los activos críticos de la información, para priorizar los riesgos que están ligados a cada uno de ellos.

- La seguridad de la información es muy importante ya que si no se presta atención a ella existiría fuga de información sensible, que podría ocasionar consecuencias como pérdida del prestigio de la institución y litigios para la empresa de servicios ”XYZ”.

- La ISO/IEC 27001:2013 tiene un enfoque más ordenado con respecto a versión del 2005, tiene nuevos controles que amplían la visión de la seguridad de la información, haciendo que esta nueva versión sea más entendible y de fácil aplicación.

- El tamaño y complejidad del servicio de “Censos de Información Comercial” influirá directamente en la complejidad del SGSI, debido a que afecta al alcance y límites que éste tendrá y a su tiempo de implementación. El factor fundamental para que se desarrolle e implemente de forma efectiva el SGSI es el apoyo de la dirección administrativa a cargo del proceso, ya que sería imposible trabajar si ésta área no aporta su conocimiento y experiencia acerca del servicio.

- La protección que ofrece un SGSI creado bajo la norma ISO/IEC 27001:2013 a la información del servicio de “Censos de Información Comercial”, no afecta al desarrollo habitual de sus procesos (Planificación de Rutas, Levantamiento de Información, Procesamiento de Información y Afinamiento de Información). El manejo y optimización de estos procesos puede realizarse utilizando otras normas y marcos de trabajo, por ejemplo: COBIT, BPM, etc., sin temor a que su implementación afecte el desempeño al SGSI.

- Se debe prestar especial atención al activo “Recursos Humanos” involucrado en el servicio de “Censos de Información Comercial” al momento de desarrollar el SGSI, debido a que tiene una relación directa con el resto de activos (Hardware, Software, Bases de Datos, Redes y Telecomunicaciones, Aspectos Legales y Servicio de Internet), por lo tanto, su importancia y afectación para la seguridad de información es muy amplia.

- La baja, adquisición o actualización de activos de información puede afectar directamente al funcionamiento del SGSI, ya que según el

funcionamiento de estos, los procesos que comprende el servicio de "Censos de Información Comercial" pueden ser actualizados, eliminados o incluso se puede crear nuevos; incluso estos factores pueden ocasionar que se afecta al alcance del SGSI para que se acople a la nueva realidad del negocio.

- El hecho que los procesos del servicio de "Censos de Información Comercial" (Planificación de Rutas, Levantamiento de Información, Procesamiento de Información y Afinamiento de Información) sean desarrollados por un equipo de trabajo relativamente pequeño (23 personas), puede afectar a la calidad de los resultados obtenidos y a la seguridad de la información, dependiendo de los siguientes factores:

    - Experiencia del trabajador en el uso de la tecnología según su rol.
    - Experiencia laboral del trabajador.
    - Nivel académico.
    - Nivel de compromiso del trabajador con el servicio y la empresa de servicios "XYZ".

- El hecho que el sistema de "Censos de Información Comercial" y la base de datos han sido creados a la medida de las necesidades del servicio, minimiza la cantidad de riesgos, amenazas y vulnerabilidades que pueden afectar la seguridad de información del servicio, debido a su exclusividad de uso y administración; sin embargo, esto no significa que no corran riesgos o amenazas, ni posean vulnerabilidades, por lo que se hace necesario la formalización de políticas.

5.2 RECOMENDACIONES

- Se recomienda realizar un reconocimiento completo y minucioso de todos los factores (naturales, sociales, legales, etc..) que influyen en el desarrollo

del servicio de “Censos de Información Comercial”, de manera que el SGSI no omita ningún detalle ni sea incoherente o contradictorio con la realidad.

- Se recomienda asignar privilegios para el manejo de activos de información en función de las actividades prácticas comprobadas de los trabajadores del servicio de “Censos de Información Comercial”, de manera que no se exceda en asignaciones de responsabilidades a uno o pocos roles, y se evite la dependencia de uno o pocos trabajadores para controlar el buen uso de activos.

- Se recomienda alinear la planificación de la implementación de los controles del SGSI con el presupuesto anual de la empresa, para no afectar a otros proyectos o realizar esfuerzos innecesarios.

- Se recomienda hacer análisis costo-beneficio periodicos (para este proyecto, el período adecuado sería 2 meses), para revisar el funcionamiento y resultados obtenidos de la implementación del SGSI en el servicio de “Censos de Información Comercial”. Si tales resultados no son satisfactorios, se analizará la posibilidad de actualizar los controles implementados para salvaguardar la seguridad de información.

- Se recomienda formalizar y difundir normas, reglas y procedimientos de seguridad de información, a todos los trabajadores involucrados en el desarrollo del servicio, para que se comprometan a actuar de forma adecuada y salvaguardar la información de cualquier riesgo que pueda comprometer su integridad, disponibilidad y confidencialidad.

- En los procesos “Procesamiento de Información” y “Afinamiento de Información”, se recomienda automatizar la resolución de conflictos, para no tener que realizarla de manera manual en la base de datos, ya que esto representa un riesgo y al ser explotado podría afectar el servicio de “Censos de Información Comercial”.

- Una vez identificados los controles para la implementación del SGSI, se recomienda que sean concordantes a las necesidades del servicio, a las vulnerabilidades encontradas y a la realidad socioeconómica de la empresa de servicios “XYZ”.

- Se recomienda identificar de forma completa los activos y procesos críticos de la empresa de servicios “XYZ” involucrados en el servicio de “Censos de Información Comercial”, para que la metodología de evaluación de riesgos escogida abarque completamente estos aspectos.

- Al diseñar el SGSI, se recomienda que sea creado de manera que, en caso que ocurran actualizaciones o cambios en el desarrollo el servicio, sea actualizable, compatible y de utilidad para salvaguardar la información sin importar las condiciones de trabajo.

BIBLIOGRAFÍA

[1] William Raúl Ayala Vargas, "Solución Móvil para Facturación y Recaudación en un Ambiente Distribuido," Escuela Politécnica Nacional, Quito, Proyecto de Titulación CD-3129, 2010.

[2] Glenda Soraya Tixi Cali, "Desarrollo de un plan de continuidad del negocio de TI para el ISP "Megadatos S.A." de la ciudad de Quito," Escuela Politécnica Nacional, Quito, Proyecto de Titulación CD-5283, 2013.

[3] Jonathan Patricio Carrillo Sánchez, "Guía de Análisis de Gestión de Riesgos en la Adquisición e Implantación de Equipamiento y Servicios de Tecnologías de Información y Comunicaciones para Proyectos de Alcance Nacional," Escuela Politécnica Nacional, Quito, Proyecto de Titulación CD-4557, 2012.

[4] Richard Eduardo Posso Guerrero, "Desarrollo de políticas de seguridad informática e implementación de tres dominios en base a la norma 27002 para el área de Hardware en la Empresa Uniplex Systems S.A.," Escuela Politécnica Nacional, Quito, Proyecto de Titulación 2009.

[5] Flor María Alvarez Zurita and Pamela Anabel García Guzman, "Implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001, para la intranet de la Corporación Metropolitana de Salud," Escuela Politécnica Nacional, Quito, Proyecto de Titulación CD-1077, 2007.

[6] Sandra Tamara Parreño Pontón and Gabriela Lorena Suntaxi Oña, "Auditoría de la seguridad de la información de la Empresa Transportes Noroccidental," Escuela Politécnica Nacional, Quito, Proyecto de Titulación CD-3005, 2010.

[7] ISO 27000.ES EL PORTAL DE ISO 27001 EN ESPAÑOL. [Online]. HYPERLINK "http://www.iso27000.es/sgsi.html" http://www.iso27000.es/sgsi.html

[8] Álvaro Gómez Vieites, *Enciclopedia de la Seguridad Informática*, Segunda ed. España: RA-MA EDITORIAL, 2011.

[9] International Standard Organization. (2013) ISO/IEC 27001:2013. [Online]. HYPERLINK "http://www.iso.org/iso/catalogue_detail?csnumber=54534" http://www.iso.org/iso/catalogue_detail?csnumber=54534

[10] Gary Stoneburner, Alice Goguen, and Alexis Feringa. (2002, Julio) National Institute of Standards and Technology (NIST). [Online]. HYPERLINK "http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf" http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[11] The CERT Division | SEI | CMU. The CERT Division | SEI | CMU. [Online]. HYPERLINK "http://www.cert.org/resilience/products-services/octave/" http://www.cert.org/resilience/products-services/octave/

ANEXOS

Los anexos están incluidos en detalle en formato digital adjunto.

ANEXO A - Diagrama de Implementación SGSI

Consultar: ***"Anexo A - Diagrama de Implementación SGSI.vsd"***.

ANEXO B - Caracterización de los dispositivos computacionales de trabajo utilizados en el desarrollo del servicio de "Censos de Información Comercial"

Modelo	Características
D-Link DES-1008D	• Conmutador Nivel 2 • 8 puertos 10/100Mbps • Soporte full-dúplex y half-dúplex para cada puerto • Puerto de interconexión MDI para expansiones sencillas • Autocorrección de la inversión de polaridad rx • Gama completa de LEDs de diagnosis • De pequeñas dimensiones, ligero • FCC Clase A, Marca de la CE, VCCI Clase A, C-Tick, BSMI Clase A • UL, CSA

Tabla 1 - Características Técnicas del Switch[7].
Fuente: Empresa de servicios "XYZ"

Características		Descripción
Tecnología de Impresión		Tecnología de inyección de tinta MicroPiezo de 4 colores (CMYK).
Resolución de Impresión		Hasta 5760 x 1440 dpi de resolución optimizada en varios tipos de papel.
Velocidad de Impresión	Máxima	Negro 27 ppm y Color 15 ppm.
	Normal	Negro 3,0 ISO ppm y Color 1,6 ISO ppm
Capacidad de Papel	Bandeja de entrada para papel	100 hojas / 10 sobres
	Bandeja de salida	50 hojas
Tipo de Escáner		Cama plana con sensor de líneas CIS de color
Área de Digitalización		Máxima 21,6 x 29,7 cm (8,5" x 11,7")
Resolución de Escáner	Óptica	600 dpi
	Hardware	600 x 1200 dpi
	Interpolada	9600 x 9600 dpi
Interface y Conectividad		SB 2.0 (Compatible con USB 1.1)

Tabla 2 - Características Técnicas de la Impresora8.
Fuente: Empresa de servicios "XYZ"

[7]Fuente http://www.dlink.com/es/es/home-solutions/connect/switches/des-1008d-8-port-10-100mbps-desktop-switch

[8]Fuente http://global.latin.epson.com/data/pais/GL/archivos/C11CB42201_PDFFile.pdf

ARQUITECTURA DEL SISTEMA	DESCRIPCIÓN
Procesador	416 MHz MTK.
Sistema operativo	Microsoft Windows Mobile 6.5 Professional.
Memoria	256 MB RAM.
Memoria Flash	Memoria FLASH integrada de 512 MB. Admite ampliaciones de memoria Micro SD opcionales.
Pantalla	2,8″, QVGA transmisiva.
Teclado	Teclado numérico de 29 teclas con teclas IMD.
Panel táctil	Resistivo de 4 hilos.
Audio	Altavoz, receptor HAC, micrófono, vibrador.
Puertos E/S	Base USB/RS232 para cable USB de carga y comunicación.
Comunicación	Cliente de alta velocidad USB 2.0.
Entorno de desarrollo	Honeywell SDK para Microsoft Windows Mobile 6.5 Professional y Visual Studio 2008.
Software de aplicaciones	Honeywell Power Tools and Demos; Microsoft SDK; Remote Master Mind for Mobility.
Software de terceros	Software de desarrollo rápido de aplicaciones ITScriptNet con aplicaciones Ready To Go.
Ampliación de almacenamiento	Ranura para tarjetas de memoria Micro SDHC accesible para el usuario. Consulte la guía de precios actuales para las opciones de tarjetas cualificadas disponibles.
Cámara	LED con enfoque automático y flash de 3 megapíxeles.
Batería	Iones de litio, 5,7 vatios/hora.
Horas estimadas de funcionamiento	Perfil de lectura alto/WLAN: 8 horas; perfil WWAN y GPS: 8 horas; tiempo de conversación GSM: 6 horas.
Tiempo estimado de carga	Menos de 6 horas.
Lector/escáner	Motor de lectura 1D de Honeywell.
Funciones de decodificación	Lee simbologías 1D estándar.
Garantía	1 año de garantía de fábrica.
CONECTIVIDAD INALÁMBRICA	**DESCRIPCIÓN**
GPS	GPS asistido (AGPS) integrado.
WLAN	Compatibilidad con WAPI 802.11 b/g.
Seguridad de WLAN	WEP, WPA, WPA-PSK, WPA2, WPA2-PSK.
WPAN	Bluetooth V2.1 con EDR.
WWAN	Voz y datos GSM/GPRS/EDGE.

Tabla 3 - Características Técnicas de PDAs9.
Fuente: Empresa de servicios "XYZ"

CARACTERÍSTICAS	DESCRIPCIÓN
General	Trabajo continuo por alrededor de 12 horas en el modo Bluetooth Trabajo continuo durante más de 15hr w / o Bluetooth El registro de trazado circular sin fin Max. grabables 131.072 puntos con números de pistas ilimitadas Punto de inicio de sesión del usuario que se puede añadir por el uso de la función Push-To-Log Los usuarios pueden dividir pistas en diferentes secciones Trabajar de forma independiente de la batería si se alimenta por el puerto USB Advertencia de Batery-lo Tamaño compacto, diseño a prueba de agua Programación del ciclo en los modos de ahorro de energía.
GPS	Motor de GPS u-blox Sensibilidad-158dBm, 16CH 8192 rápida corrector búsqueda bin Precisión: 2,5 m CEP autónomo, S / A apagado) Tiempo al primer arreglo; 34s (arranque en frío) Sensibilidad de la adquisición: -142dBm

[9] Modificado de dolphin-6000.pdf

CARACTERÍSTICAS	DESCRIPCIÓN
	Seguimiento de sensibilidad; -158dBm Soporte SBAS
Especificaciones Bluetooth	Ver Bluetooth. 1.2 Potencia de salida: CLASE 2 (alrededor de 10 metros) Servicio: SPP Esclavo

Tabla 4- Características Técnicas del GPS.10
Fuente: Empresa de servicios "XYZ"

ANEXO C - Entrevista de Vulnerabilidades Ambientales y Humanas

Consultar ***"Anexo C - Entrevista de Vulnerabilidades Ambientales y Humanas.docx"***.

ANEXO D - Entrevista de Vulnerabilidades Naturales

Consultar ***"Anexo D - Entrevista de Vulnerabilidades Naturales.docx"***.

ANEXO E - Entrevista de Vulnerabilidades Organizacionales

Consultar ***"Anexo E - Entrevista de Vulnerabilidades Organizacionales.docx".***

ANEXO F - Entrevista de Vulnerabilidades Técnicas

Consultar ***"Anexo F - Entrevista de Vulnerabilidades Técnicas.docx".***

ANEXO G - Política de Seguridad de la Información

Consultar ***"Anexo G - Política de Seguridad de la Información.docx".***

[10] Fuente: http://www.wintec.com.tw/en/Products/gps/wbt_201.html

ANEXO H - Política de Organización de Seguridad de la Información

Consultar ***"Anexo H - Política de Organización de la Seguridad de Información.docx".***

ANEXO I - Política de Seguridad de Recursos Humanos.

Consultar ***"Anexo I - Política de Seguridad de Recursos Humanos.docx".***

ANEXO J - Procedimiento de Seguridad de Recursos Humanos.

Consultar ***"Anexo J - Procedimiento de Seguridad de Recursos Humanos.docx".***

ANEXO K - Política de Gestión de Activos

Consultar ***"Anexo K - Política de Gestión de Activos.docx".***

ANEXO L - Procedimiento de Gestión de Activos

Consultar ***"Anexo L - Procedimiento de Gestión de Activos.docx".***

ANEXO M - Política de Control de Acceso

Consultar ***"Anexo M - Política de Control de Acceso.docx".***

ANEXO N - Procedimiento de Control de Acceso

Consultar ***"Anexo N - Procedimiento de Control de Acceso.docx".***

ANEXO O - Política de Criptografía

Consultar el documento ***"Anexo O - Política de Criptografía.docx".***

ANEXO P - Política de Seguridad Física y Ambiental

Consultar ***"Anexo P - Política de Seguridad Física y Ambiental.docx".***

ANEXO Q - Procedimiento de Seguridad Física y Ambiental

Consultar ***"Anexo Q - Procedimiento de Seguridad Física y Ambiental.docx".***

ANEXO R - Política de Operaciones de Seguridad

Consultar ***"Anexo R - Política de Operaciones de Seguridad.docx".***

ANEXO S - Procedimiento de Operaciones de Seguridad

Consultar ***"Anexo S - Procedimiento de Operaciones de Seguridad.docx".***

ANEXO T - Política de Seguridad de las Comunicaciones

Consultar ***"Anexo T - Política de Seguridad de las Comunicaciones.docx".***

ANEXO U - Política de Relaciones con Proveedores

Consultar ***"Anexo U - Política de Relaciones con Proveedores.docx".***

ANEXO V - Política de Gestión de Incidentes de Seguridad de Información

Consultar ***"Anexo V - Política de Gestión de Incidentes de Seguridad de Información.docx".***

ANEXO W - Procedimiento de Gestión de Incidentes de Seguridad de Información

Consultar **"*Anexo W - Procedimiento de Gestión de Incidentes de Seguridad de Información.docx".***

ANEXO X - Política de Continuidad del Negocio

Consultar ***"Anexo X - Política de Continuidad del Negocio.docx".***

ANEXO Y - Política de Cumplimiento

Consultar ***"Anexo Y - Política de Cumplimiento.docx".***

ANEXO Z - Procedimiento de Cumplimiento

Consultar ***"Anexo Z - Procedimiento de Cumplimiento.docx".***