ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"PLANIFICACIÓN DE LA IMPLEMENTACIÓN DE UN ESQUEMA DE SEGURIDAD BASADA EN LA NORMA ISO 27001:2013, PARA EL PROCESO DE ADMINISTRACIÓN DEL SISTEMA DE INFORMACIÓN GEOGRÁFICA EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN SAMBORONDÓN"

TRABAJO DE TITULACIÓN

Previo a la obtención del título de

MÁGISTER EN SEGURIDAD INFORMÁTICA APLICADA

VÍCTOR MANUEL SÁNCHEZ MERA

GUAYAQUIL – ECUADOR

AÑO: 2019

AGRADECIMIENTO

Agradezco a Dios por darme las fuerzas para seguir adelante en este proyecto de vida.

A mi padre Víctor Manuel, abuelo Julio y abuelo Víctor Hugo que juntos desde el cielo guían y acompañan cada paso que doy en la vida.

A mi madre Martha por su amor incondicional, por su fortaleza frente a las adversidades y por estar presente cada día de mi vida.

A mi tutor por su invaluable apoyo para la culminación de este proyecto.

DEDICATORIA

A Dios, a mis padres, a mi familia, tutor, amigos y todos quienes estuvieron conmigo apoyándome para siempre seguir adelante.

TRIBUNAL DE SUSTENTACIÓN

MSIG. LENÍN FREIRE COBO

DIRECTOR DE LA MSIA

MSIG. LENÍN FREIRE COBO

DIRECTOR DEL PROYECTO DE GRADUACIÓN

MSIG. RONNY SANTANA ESTRELLA

MIEMBRO DEL TRIBUNAL

DECLARACIÓN EXPRESA

"Declaro de forma expresa que todo el contenido de este trabajo de titulación es de mi completa autoría y responsabilidad, por lo que doy mi consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"

VÍCTOR MANUEL SÁNCHEZ MERA

RESUMEN

El presente trabajo consiste en establecer una planificación adecuada para implementar un esquema de seguridad informático basado en la norma ISO 270001:2013 dentro del proceso de administración del sistema de información geográfica del Gobierno Autónomo Descentralizado del cantón Samborondón, donde se identificarán las potenciales amenazas y riesgos con el propósito de contar con los elementos necesarios para la toma de decisiones con respecto a la administración de los mismos donde se encuentra expuesta la información.

Este documento se divide en cinco capítulos que están estructurados de la siguiente manera:

En el Capítulo 1, se describen las generalidades del GAD del cantón Samborondón, la problemática existente con respecto al proceso de administración del Sistema de Información Geográfica implementado. Se define el objetivo general, los objetivos específicos, de la misma manera se indica la metodología que se llevará a cabo para el proyecto.

En el Capítulo 2, se describe el marco teórico de la Norma ISO 27001 que permitirá seleccionar los objetivos de control y controles para poder contrarrestar amenazas que puedan llegar a afectar a la información teniendo como base la evaluación del riesgo y su tratamiento.

En el Capítulo 3, se presenta el levantamiento de contexto del GAD de Samborondón en el cual se presenta un breve diagnóstico político institucional, la estructura organizacional del GAD para posteriormente detallar el proceso de administración del sistema de información geográfica con el análisis de brecha respectivo.

En el Capítulo 4, se muestra el análisis de los riesgos del proceso de información geográfica el cual involucra la definición de los activos, las amenazas y vulnerabilidades de estos activos, valoración de los riesgos y el análisis respectivo.

En el Capítulo 5, se define la planificación de implementación del esquema de seguridad donde se encuentran las acciones a tomar para el tratamiento de los riesgos, la reformulación del impacto y sus consecuencias, definición de proyectos y la elaboración de las políticas de seguridad.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

ISO	Organización de Estándares Internacionales
BSI	British Standards Institution
SGSI	Sistema de Gestión de Seguridad de la Información
IEC	Comisión Electrotécnica Internacional
Anexo SL	Estándar que define la nueva estructura de Alto Nivel para todos los sistemas de gestión de las Normas ISO
RRHH	Recursos Humanos
MAGERIT:	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información elaborada por el Consejo Superior de Administración Electrónica de España
MARION:	Metodología de Análisis de Riesgos Informáticos Dirigida por Niveles.
MELISA:	Metodología Análisis de Riesgos Informáticos procedente del entorno militar francés.
CRAMM:	Metodología de Análisis de Riesgos desarrollado por el Centro de Informática y la Agencia Nacional de Telecomunicaciones del gobierno del Reino Unido
OCTAVE:	Metodología de Análisis de Riesgos desarrollada por la Universidad de Carnegie Mellon.
SEI	Instituto de Ingeniería de Software (Software Engineering Institute)
OSSTMM	Manual de Metodología Abierta de Testeo de Seguridad
ISECOM	Institute for Security and Open Methodologies
COOTAD	Código de Ordenamiento Territorial Autónomo Descentralizado

GAD	Gobierno Autónomo Descentralizado
IDE	Infraestructura de Datos Espaciales
SSL	Secure Sockets Layer, protocolo diseñado para transmitir información de ida y de manera segura hacia atrás
SSH	Secure Shell, protocolo de administración remota que permite a los usuarios controlar y modificar sus servidores remotos a través del internet.
HTTPS	Hypertext Transfer Protocol Secure (protocolo seguro de transferencia de hipertexto)
EPSG	European Petroleum Survey Group
SRID	Spatial Reference System Identifier (identificador de referencia espacial)
ENISA	Agencia de Seguridad de las Redes y de la Información de la Unión Europea
NIST	Instituto Nacional de Estándares y Tecnología
SANS	SysAdmin Audit, Networking and Security Institute
GIS	Sistema de Información Geográfica
IAAS	Infraestructura como servicio
UNE	Una Norma Española
TIC	Tecnologías de Información y Comunicación

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

El presente trabajo tiene como finalidad crear un esquema de seguridad de la información al proceso de administración del Sistema de Información Geográfica del Gobierno Autónomo Descentralizado del Cantón Samborondón, para lo cual se ha realizado un estudio para determinar las amenazas y vulnerabilidades, análisis y tratamiento de riesgos al proceso mencionado, siguiendo la norma ISO 27001:2013.

En la actualidad el tema de seguridad informática para las organizaciones e instituciones ya sean privadas o públicas evoluciona con gran rapidez en nuestro medio, siendo necesario verificar periódicamente la seguridad de los activos y así mismo tomar las medidas necesarias para asegurarlos de posibles ataques tanto internos como externos.

De esta manera, el activo más importante para todas las organizaciones es la información, por tal motivo existen procedimientos, normas y estándares internacionales que sirven como una hoja de ruta a seguir para implementar controles en cuanto a la seguridad de la información se refiere.

El esquema de seguridad de información se basa en la definición de políticas y procedimientos y de varios proyectos planteados que servirán para garantizar la integridad, confidencialidad y disponibilidad de la información proporcionada por el Gobierno Autónomo Descentralizado del cantón Samborondón.

CAPÍTULO 1

GENERALIDADES

1.1 Antecedentes

En la era digital que actualmente se desenvuelve el mundo, la información es uno de los activos más importantes de las empresas, organizaciones, instituciones del sector privado e instituciones gubernamentales, por ese motivo es necesario que sea protegida de riesgos en su entorno, tanto interno como externo. Se consideran riesgos internos según Álvaro Gómez en la

Enciclopedia de la Seguridad Informática en su 2da Edición a las propias amenazas dentro de la institución donde la información es administrada y riesgos externos son las amenazas externas por parte de cualquier recurso humano y/o tecnológico ajeno a la institución. [1]

Hoy en día los sistemas de información geográfica son usados con diferentes fines a nivel académico, comercial, personal o militar, se han integrado como una herramienta tecnológica dentro de las empresas, organizaciones, instituciones del sector privado e instituciones gubernamentales para la gestión y análisis de la información geográfica, procesamiento y visualización de mapas y sobre todo para la toma de decisiones.

1.2 Descripción del problema

Actualmente no existe un esquema de seguridad, al proceso de administración del sistema de información geográfica del Gobierno Autónomo Descentralizado del Cantón Samborondón. El proceso de administración se inicia desde el alojamiento físico, control de acceso, administración de datos y configuración de la aplicación, este proceso por su falta de seguridad corre el riesgo que la información sea extraída y alterada, no hay seguridad en su integridad, pueden alterar la configuración del equipo e instalar programas

para realizar conexiones remotas no permitidas. Se ha identificado que no se cuenta con un adecuado control y soporte en cuanto al nivel de seguridad de la información.

Además, el Municipio cuenta con medidas limitadas para gestionar la seguridad al interior de la institución por lo que es necesario la implementación de políticas, estrategias de concientización y divulgación de seguridad de la información y realizar la implementación de herramientas y procedimientos que garanticen la seguridad de la información, del proceso en mención.

Es un potencial problema porque al contar con un sistema de información geográfica para que los usuarios puedan acceder y descargar información, estos insumos deben estar disponibles y sus datos libres de modificaciones o alteraciones no autorizadas.

1.3 Objetivo General

Planificar la implementación de un esquema de seguridad basada en la norma ISO 27001:2013 que contenga las medidas de seguridad necesarias para el proceso de administración del Sistema de Información Geográfica en el Gobierno Autónomo Descentralizado del Cantón Samborondón.

1.4 Objetivos Específicos

- Definir el proceso de administración del sistema de información geográfica
- Recabar la información necesaria para analizar las posibles vulnerabilidades y amenazas existentes dentro del proceso de administración del sistema de información geográfica.
- Realizar el análisis de riesgos del proceso de administración del sistema de información geográfica.
- Diseñar un plan de tratamiento de riesgos del proceso de administración del sistema de información geográfica.
- Proponer un manual de políticas de seguridad informática para el proceso de administración del sistema de información geográfica basada en el estándar ISO 27001:2013

1.5 Metodología

La metodología para realizar el presente proyecto se compone en las siguientes fases:

- Estudio del Estándar/Norma
  - Estudio de la norma ISO 27001:2013
- Análisis del proceso de administración del sistema de información geográfica
  - Situación presente del proceso de administración, amenazas que podrían estar expuestos los activos, vulnerabilidades y riesgos basados en la valoración de las amenazas y activos.
- Diseño e implementación de políticas y procedimientos.
  - Selección de controles que ayuden a minimizar los riesgos, definición de políticas y procedimiento para asegurar la administración del activo.

CAPÍTULO 2

MARCO TEÓRICO

2.1 Norma ISO 27001

Con la aparición de las Tecnologías de Información y Comunicación, la información se ha convertido en un activo de vital importancia para las organizaciones hasta el punto de necesitar asegurar adecuadamente la información y los sistemas que la procesan, de esta manera se hizo fundamental la necesidad de crear un sistema que metodológicamente y de forma documentada cumpla con los objetivos de seguridad planteados por la organización y permita el tratamiento adecuado de los riesgos a los que está expuesta.

En relación a lo mencionado aparece el conjunto de estándares ISO/IEC 27000, los mismos que proporcionan el marco para la gestión de la seguridad de la información de las organizaciones tanto públicas como privadas. A continuación se detallará un breve resumen de la creación y actualización de los estándares hasta la actualidad.

En el año de 1995 se publicó el “conjunto de buenas prácticas para la gestión de la seguridad de la información” un documento publicado por el gobierno del Reino Unido el mismo que se convirtió en un estándar denominado BS799 por el British Standards Institution (BSI). Entidad de normalización internacional creada en el año 1901.

La primera parte de éste estándar (BS799-1) corresponde a una guía de buenas prácticas, para la cual no se establece un esquema de certificación, en tanto que la segunda parte (BS799-2) publicada en 1998, establece los requisitos de un sistema de seguridad de la información (SGI) para ser certificable.

BS799-1 fue adoptada sin grandes cambios por ISO en el año 2000 como la norma ISO 17799 y en el año 2005 la Organización Internacional de Estandarización y la Comisión Electrónica Internacional y numerosas empresas certificadas en BS799-2 publicaron la norma ISO 27001 que es considerado un estándar internacional, debido a que hace referencia a un compendio de requisitos que exigen que los sistemas de seguridad de la información en la organización garanticen la mejora continua y la administración adecuada de la información. En este mismo año (2005) se revisó y actualizó la ISO 17799, la cual fue nombrada como 27002:2005 en el año 2007. [2]

En el año 2013 luego de ser revisada y reorganizada se publica la nueva versión de la ISO 27001 que tiene cambios significativos en su estructura, evaluación y tratamiento de riesgos.

Esta norma es certificable por auditores externos, contiene 114 controles presentados en 14 secciones. En su Anexo A, enumera en forma de

resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en la implementación de un SGSI; a pesar de que la implementación de los controles enumerados en el Anexo A no es obligatoria, la organización deberá argumentar la no aplicabilidad de los controles no implementados. [3]

En el año 2014 aparece la nueva versión de la ISO 27002, que se actualiza de acuerdo a los cambios de la norma ISO 27001:2013, es una guía de buenas prácticas en seguridad de la información, la cual no es certificable, describe tanto los objetivos de control como los controles recomendables para la organización. Contiene 133 controles presentados en 39 objetivos de control en 11 dominios. Actualmente incluye el teletrabajo.

Para la elaboración del presente proyecto se ha tomado como referencia el estándar ISO 27001:2013, el cual ha sido elaborado con la finalidad de proporcionar los requisitos para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información (SGSI) dentro de una organización.

Este estándar permite conservar la confidencialidad, integridad y disponibilidad de los datos y de la información, así como de los sistemas que la procesan, cumpliendo de esta manera con los principios de la seguridad de la información, así mismo permite evaluar los riesgos y la aplicación de controles necesarios para manejarlos adecuadamente. [4]

Tiene como objetivo principal lograr asumir, conocer, gestionar y minimizar de forma ordenada y documentada los riesgos derivados de la seguridad de la información, considerando que la información es un activo con un valor muy importante por lo cual debe estar protegido mediante un proceso sistemático y documentado conocido por toda la organización.

La ISO/IEC 27001:2013 está desarrollada en base al anexo SL de la ISO, el cual proporciona el formato y lineamientos bajo una misma estructura a cumplir por todos los documentos relacionados con los sistemas de gestión, lo que facilita la integración entre sistemas.

Incluye el Anexo A que corresponde al resumen de dominios y controles detallados en la norma ISO 27002:2014, los cuales se enlistan a continuación:

- Políticas de seguridad

- Organización de la seguridad de la información

- Seguridad de los RRHH

- Gestión de activos

- Control de acceso

- Criptografía

- Seguridad física y ambiental

- Operaciones de seguridad

- Seguridad de las comunicaciones

- Sistemas de adquisición, desarrollo y mantenimiento

- Relación con proveedores

- Gestión de incidentes

- Seguridad de la información para la continuidad del negocio

- Cumplimiento

2.2 Metodología de análisis y tratamiento de riesgos

El análisis y la gestión de riesgos forman parte de un método fundamental para determinar los riesgos de un sistema de información y en base a los resultados obtenidos se establecen las medidas adecuadas que me sirven de apoyo para controlar adecuadamente los riesgos.

El análisis de riesgos se concentra en investigar los diversos factores que contribuyen a la presencia de riesgos, implica que hay que evaluar el impacto que una acceso no permitido tendría sobre una organización, de la misma manera ayuda a determinar las vulnerabilidades frente a las amenazas latentes. El análisis de riesgos indica la magnitud de riesgos que está expuesta la organización.

Por otra parte la gestión de riesgos usa los resultados del análisis de riesgos para seleccionar las medidas de seguridad adecuadas para controlar los riesgos identificados.

Las principales metodologías para el análisis y gestión de riesgo de los sistemas de información se detallan a continuación:

MAGERIT: Metodología pública española creada en 1996 por el Ministerio de las Administraciones Públicas en colaboración con la empresa de tecnologías de la información Atos Origin, actualizada en su versión 3 en octubre del 2012 [5]

MARION: Metodología francesa creada en 1985, se actualiza por CLUSIF (Asociación de empresas aseguradoras francesas)

MELISA: Metodología procedente del entorno militar francés, creada en 1984

CRAMM: Iniciada en 1985, del CTA (Central Computer and Telecommunications Agency) se usa en la administración pública británica

OCTAVE: Del SEI (Software Engineering Institute) que vista desde el punto organizativo y técnico analiza los riesgos y propone un plan de mitigación.

OSSTMM (Manual de Metodología Abierta de Testeo de Seguridad): Del ISECOM (Institute for Security and Open Methodologies) propone evaluar la seguridad en redes con testeos de intrusión, mediante Hacking Ético.

Para la planificación de la implementación del esquema de seguridad basado en la norma ISO 27001:2013, para el proceso de administración del Sistema de Información Geográfico en el Gobierno Autónomo Descentralizado del

cantón Samborondón se tomará de referencia la metodología tradicional MAGERIT.

CAPÍTULO 3

LEVANTAMIENTO DE CONTEXTO DE LA ORGANIZACIÓN

3.1 Propósito y Objetivos Estratégicos

El Municipio es un Gobierno Autónomo Descentralizado regido por el Código de Ordenamiento Territorial Autónomo Descentralizado "COOTAD" (Art.238), cuya finalidad es el bien común, y dentro de este y en forma primordial la atención de las necesidades y servicios básicos del Cantón.

Cada municipio constituye una persona jurídica de derecho político con patrimonio propio y con capacidad para realizar los actos jurídicos

necesarios para el cumplimiento de sus fines, en forma y condiciones que determinan la Constitución y las Leyes respectivas.

MISIÓN DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN SAMBORONDÓN

Desarrollar liderazgo y los servicios municipales a fin de dotar al Cantón Samborondón de un Gobierno Local facilitados y gestor de procesos que promuevan el desarrollo de la comunidad de forma integral y sostenible, con una orientación permanente a la Calidad Total y en un Medio Ambiente que proporcione la más alta productividad, con un recurso humano comprometido, capacitado y motivado.[6]

VISIÓN DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN SAMBORONDÓN

Contar con una estructura municipal sólidamente organizada ejecutiva, ágil y de absoluta credibilidad. Con un equipo humano integrado del más alto nivel profesional, motivado, positivo en permanente actualización; innovador, ejerciendo liderazgo en el Cantón Samborondón con la más alta calidad y generando condiciones básicas de gobernabilidad. Se ha reducido significativamente los índices de pobreza, carencias de infraestructura y equipamientos, generando un ambiente más seguro y productivo, con protección a la ecología de la región. [6]

SISTEMA DE INFORMACIÓN INSTITUCIONAL

El sistema de información que lleva la entidad Municipal es regular, ya que la institución no cuenta con una plataforma informática dinámica que permita accesibilidad tanto para funcionarios como para usuarios. Desde el mes de agosto del 2014 se está trabajando en el Desarrollo de Software para el análisis, diseño, desarrollo e implementación de módulos, la cobertura, disponibilidad y servicios de los procesos, que servirán para que los trámites

ciudadanos se realicen de forma ágil. Sin embargo falta implementar un sistema integral para los trámites administrativos. [6]

SISTEMA CARTOGRÁFICO ACTUAL

El GAD Municipal de Samborondón tiene actualmente registrados 28.961 predios urbanos, en el año 2012 se realizó el levantamiento de 19.207 predios que corresponden a la Parroquia Satélite La Puntilla.

Se actualizó la cartografía predial con información geográfica georreferenciada, se cuenta con una imagen satelital de la parroquia La Puntilla tomada por el satélite GeoEye-1 a 60 cm de resolución por pixel tomada en el 2012, capas geográficas vectorizadas con el deslinde predial, área de edificación, manzanero y vial. [6]

Se tiene una aplicación de catastro desarrollada bajo la siguiente arquitectura:

- Plataforma de desarrollo: Java Enterprise Edition 7

- Frameworks de desarrollo: EJB 3.1, Spring, Hibernate, JSF 2.1, JDBC

- Lenguajes Java 7, XML, JSP, JSPX, XHTML, JavaScript

- IDE de desarrollo: Eclipse 3.6 (indigo), Netbeans 7.

- Interfaz gráfica: Plantillas Facelets 1.1, css3, html5

- Servidores e Infraestructura de aplicaciones Apache TomEE 1.6

- Bases de Datos PostgresSQL 9.1

- Redes: Comunicación con sockets seguros SSL y protocolos HTTPS entre el cliente y el servidor

Las aplicaciones web son ejecutadas en cualquiera de los siguientes navegadores:

Internet Explorer 8 o superior, Firefox 4 o superior, Chrome 5 o superior, Safari 5.0 o superior.

SISTEMA DE ALMACENAMIENTO ACTUAL

La Municipalidad tiene el servicio de un data center de categoría tier IV que soporta toda la infraestructura de las aplicaciones web desarrolladas con herramientas de software libre y bajo una plataforma LINUX.

SISTEMA DE INFORMACIÓN GEOGRÁFICA

Existe un sistema de información geográfica web que permite la publicación de capas, búsqueda y visualización de información espacia, esta infraestructura de datos espaciales está desarrollada con herramientas de software libre en la siguiente arquitectura:

- Plataforma de desarrollo: Java Enterprise Edition 7

- Frameworks de desarrollo: EJB 3.1, Spring, Hibernate, JSF 2.1, JDBC.

- Lenguajes Java 7, XML, JSP, JSPX, XHTML, Javascrit

- IDE de desarrollo: Eclipse 3.6 (indigo), Netbeans 7

- Interfaz Gráfica: Plantillas Facelets 1.1, css3, html5.

- Servidores de Infraestructura de aplicaciones Apache TomEE 1.6

- Base de Datos PostgresSqL 9.1, PostGIS

- Servidor de mapas: Geoserver

- Api espacial: OpenLayers

Actualmente el Sistema de Información Geográfica del Gobierno Autónomo Descentralizado del Cantón Samborondón está instalado en un servidor con las siguientes características:

Tabla 1. Detalles técnicos servidor del Sistema de Información Geográfica

Servidor	Geoportal Externo
Tipo de Máquina	FISICO
OS	Linux
Versión	CentOS 6.8
Tipo de Procesador	Intel Core i7
Arquitectura/plataforma	X86_64
#CPU	32(2-16)
Memoria	8 GB

Cabe señalar que el servidor que aloja el Sistema de Información Geográfica del Gobierno Autónomo Descentralizado del cantón Samborondón [imagen 4] está ubicado en el centro de cómputo del edificio matriz (Municipio Samborondón) [imágenes 1 y 2], ésta área cuenta con las siguientes características:

- Dimensiones: Largo 2,50 m – Ancho 2,00 m – Alto 2,60 m

- Climatización: Sistema centralizado de aire acondicionado para todo el edificio

- Piso falso: NO

- Techo falso: SI

- Ventanas: NO

- Acceso segundario: NO

- Ubicación de servidor: Rack de 19 pulgadas

- Seguridad de acceso: Puerta de aluminio y vidrio con cerradura convencional

A continuación se muestran las imágenes del resultado de un levantamiento fotográfico del área en mención:

Figura 3.1 Vista exterior del centro de cómputo del GAD Samborondón

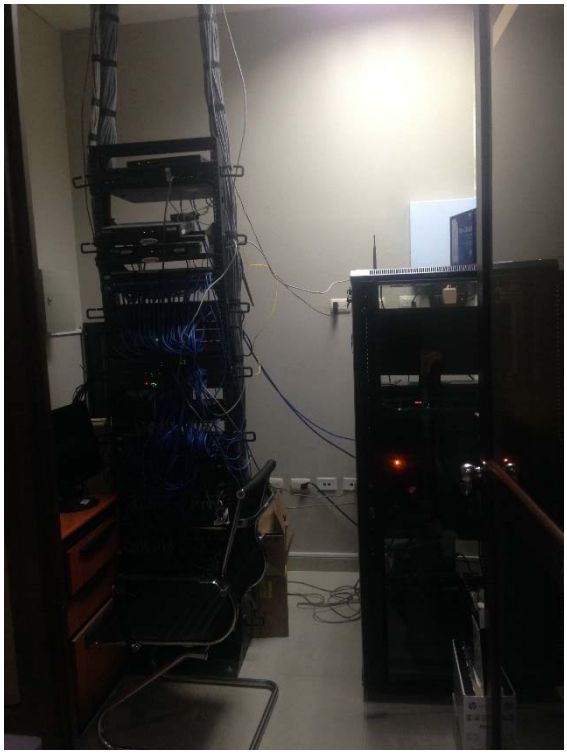

Figura 3.2 Vista interior del centro de cómputo del GAD Samborondón

Figura 3.3 Rack de 19” donde se encuentra ubicado físicamente el servidor GIS

Figura 3.4 Servidor GIS (derecha)

Figura 3.5 Sistema de climatización, iluminación y contra incendios

Figura 3.6 Cielo falso / rack de comunicaciones

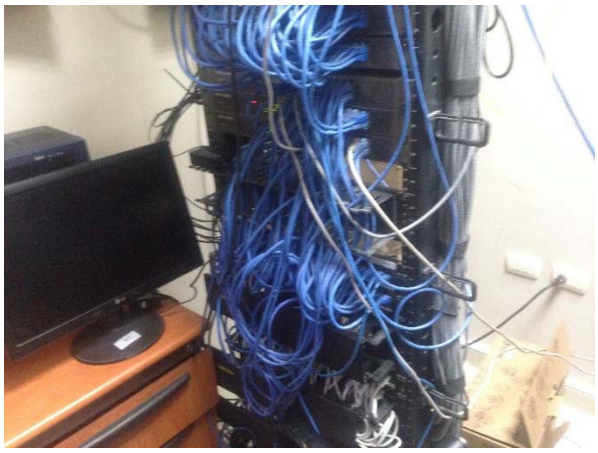

Figura 3.7 Rack de comunicaciones

3.2 Organigrama de la empresa

Organigrama Estructura del Gobierno Autónomo Descentralizado Municipal de Samborondón

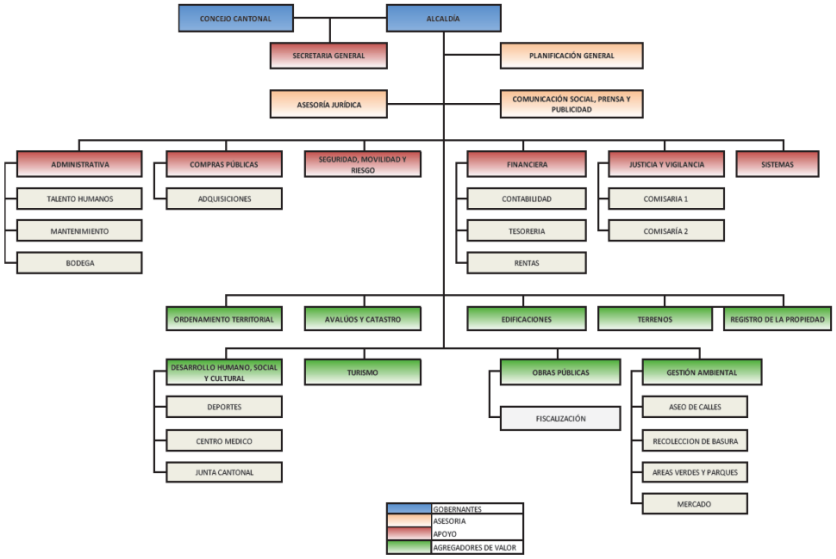

Figura 3.8 Organigrama Estructura del GAD Municipal del cantón Samborondón

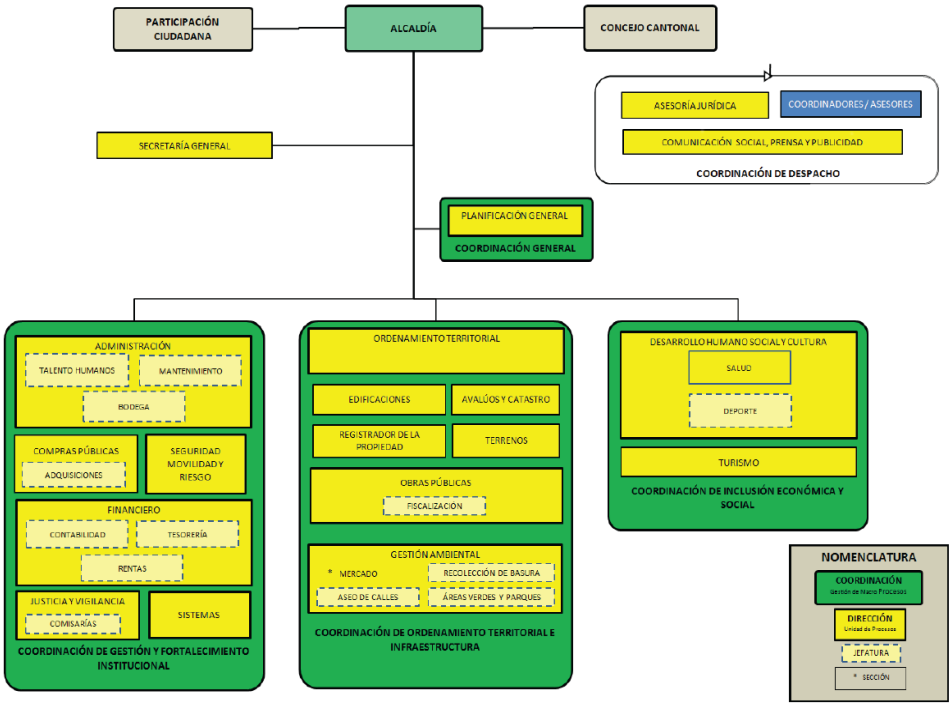

Figura 3.9 Organigrama por procesos del GAD Municipal del cantón Samborondón

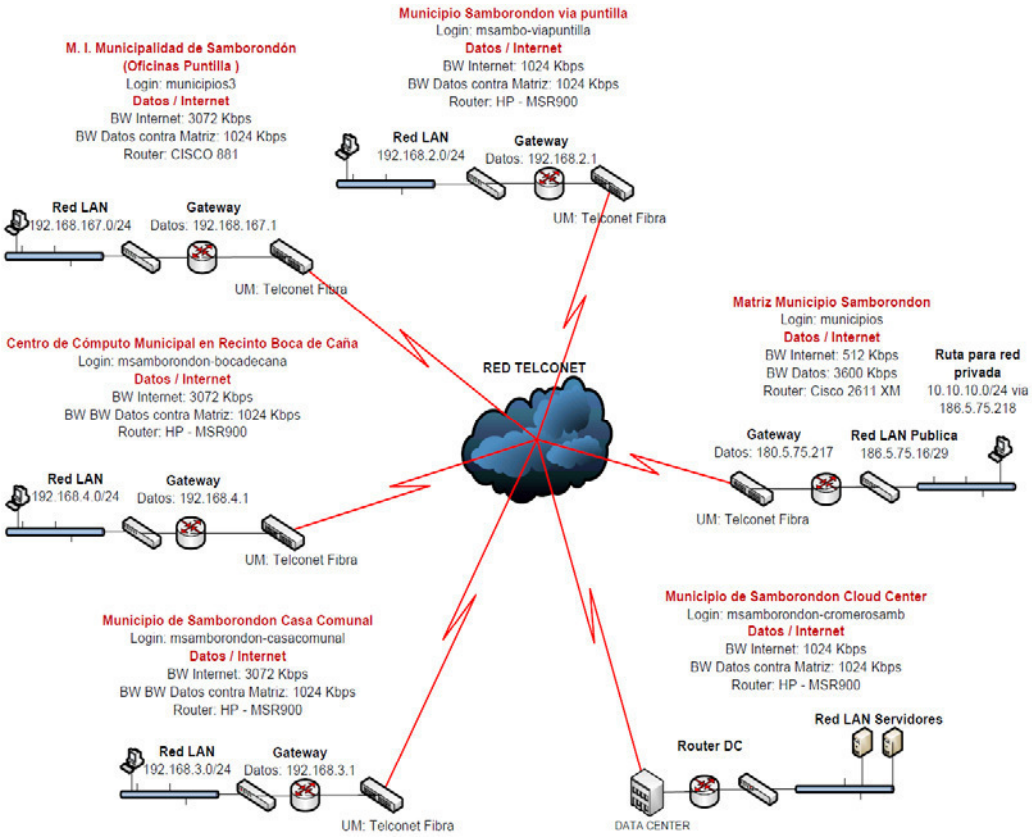

Figura 3.10 Diagrama de conexiones GAD Municipal del cantón Samborondón

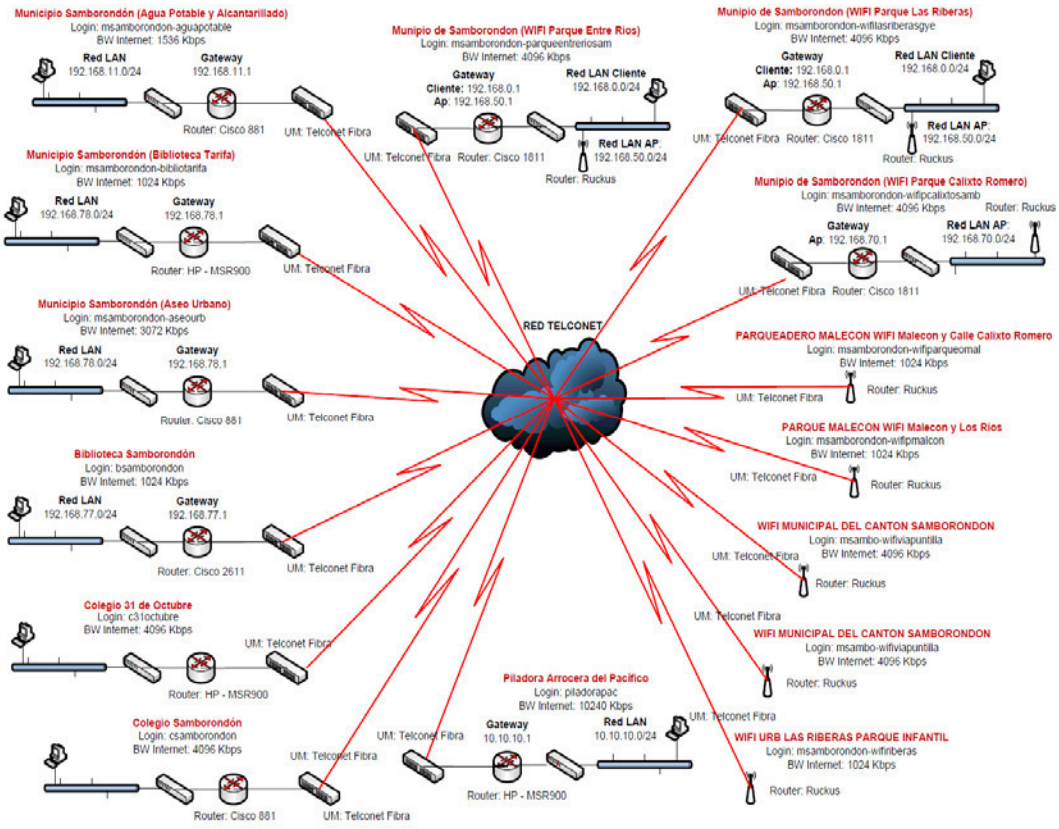

Figura 3.11 Diagrama de conexiones (servicios proveedor) GAD Municipal del cantón Samborondón

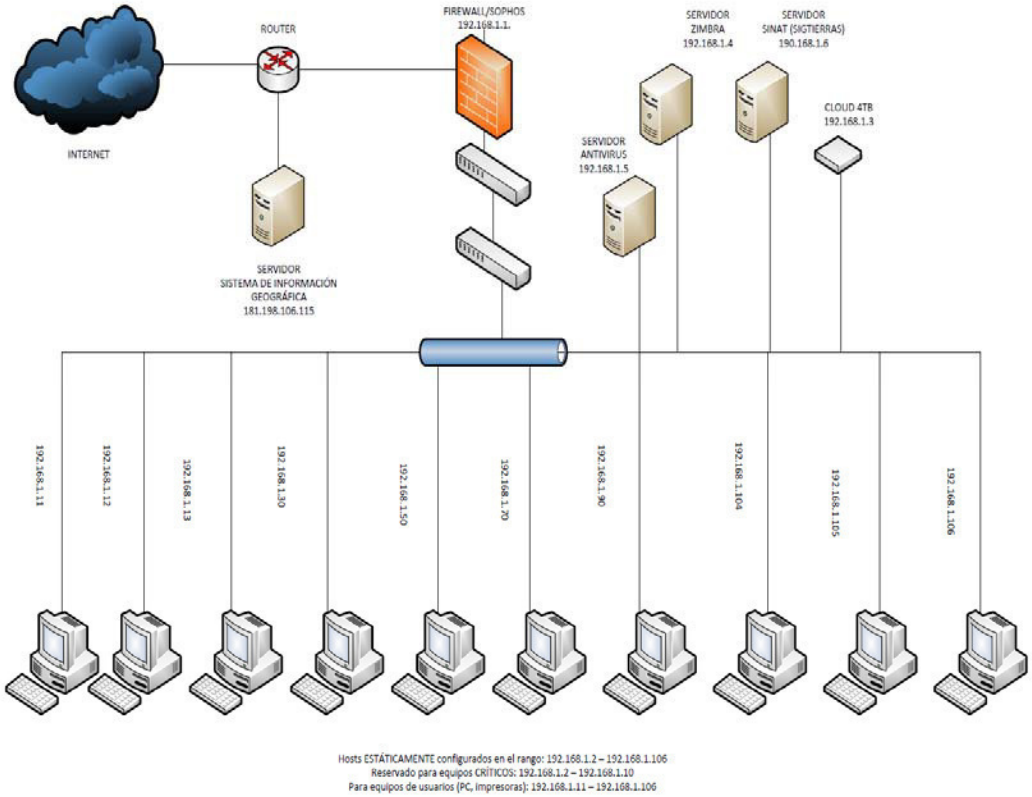

Figura 3.12 Diagrama de red oficina matriz GAD municipal del cantón Samborondón

3.3 Mapa de proceso

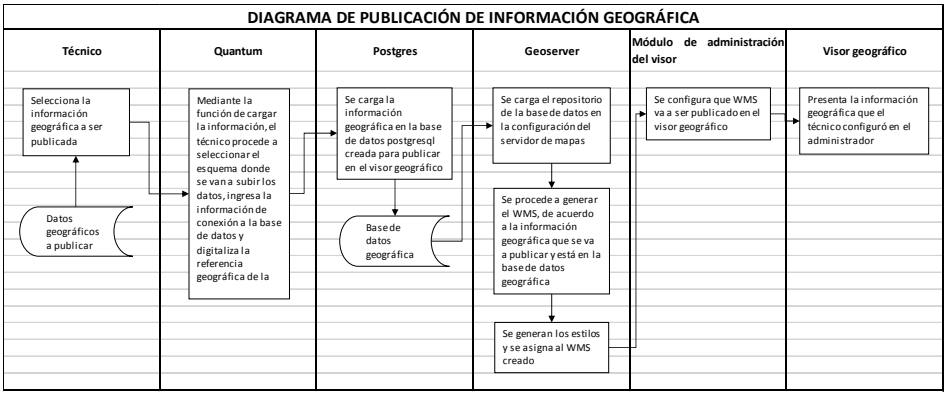

Figura 3.13 Mapa de proceso de publicación de información geográfica

3.4 Proceso de Administración del Sistema de Información Geográfica

1.- Verificar el acceso al servidor mediante las credenciales asignadas, para este caso se usa cualquier herramienta que permita conexión SSH

```
login as: root
root@181.198.106.115's password:
Last login: Fri Aug  3 17:34:43 2018 from mail.samborondon.gob.ec
```

Figura 3.14 Verificación de acceso mediante consola

2.- Mediante la herramienta Quantum GIS (código libre) se accede al menú Database -> Spit -> Import Shapefiles to Postgresql

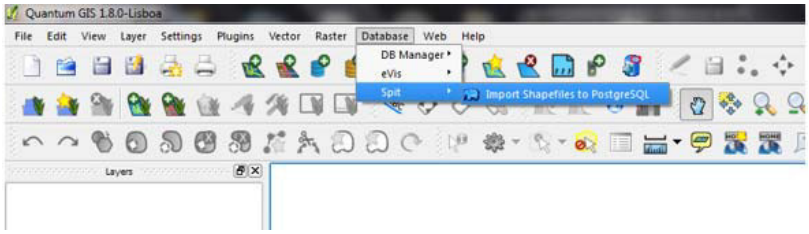

Figura 3.15 Proceso de importación de capas a la base de datos postgresql

3.- Crear conexión a la base de datos postgresql presionando el botón New en la sección PostgreSQL connections:

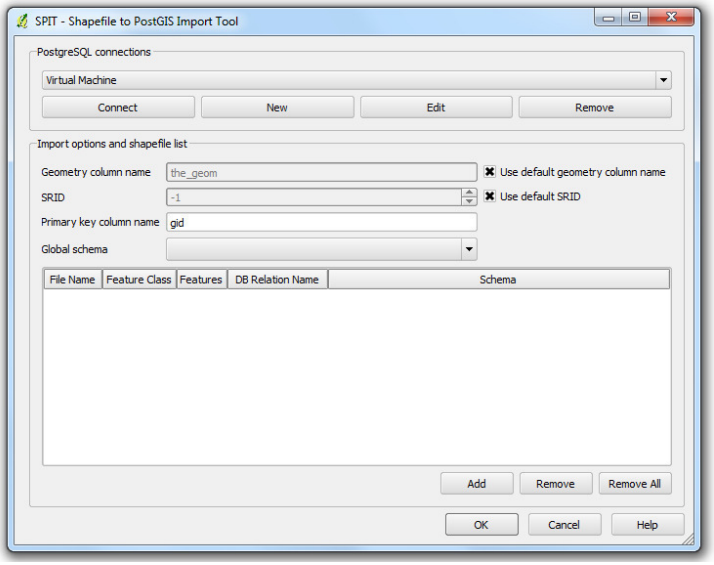

Figura 3.16 Creación de conexión a la base de datos postgresql

4.- Se abrirá la ventana de conexión a la base de datos, donde se definen las siguientes opciones:

Name: Nombre para identificar la conexión

Host: La dirección IP del servidor de base de datos

Port: El puerto configurado para la base de datos (por defecto 5432)

Username: El usuario de la base de datos

Password: La contraseña del usuario de la base de datos

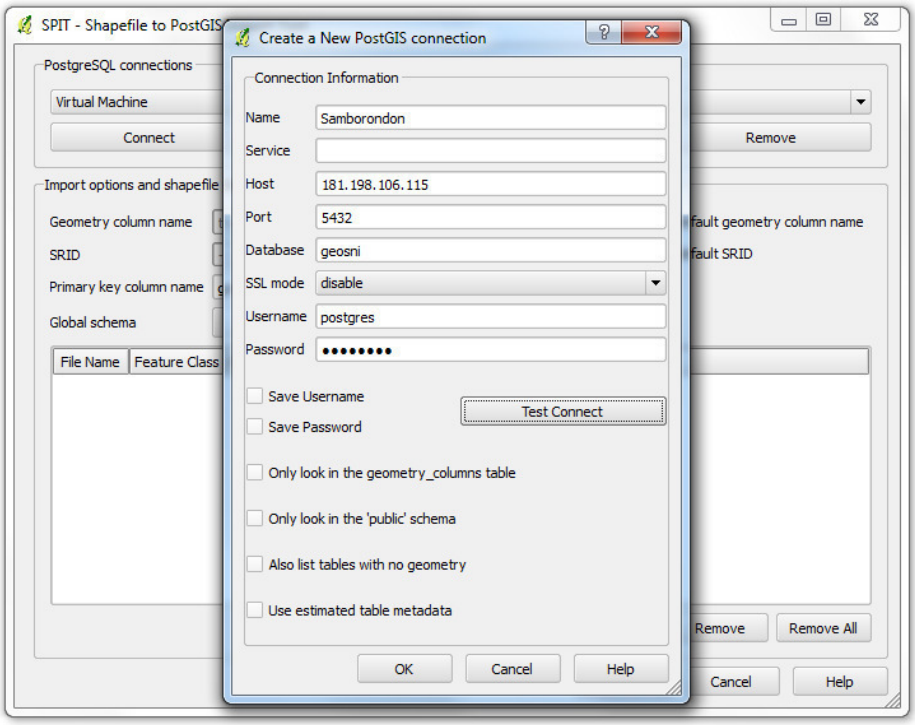

Figura 3.17 Definición de parámetros de conexión a la base de datos

Luego de dar click en Test Connect deberá aparecer un mensaje que confirma que es posible la conexión a la base de datos.

Figura 3.18 Verificación de conexión

5.- Antes de subir el shapefile se deberá verificar que el sistema de coordenadas corresponda a EPSG:32717 (Sistema de proyección de coordenadas para Ecuador UTM zona 17S)

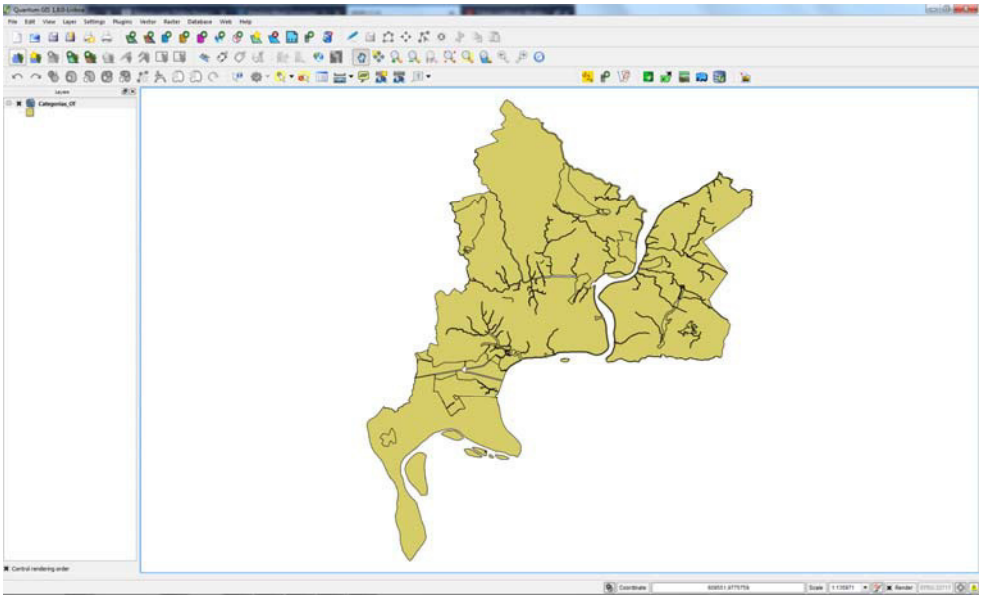

Figura 3.19 Comprobación del sistema de coordenadas de la capa a cargar mediante herramienta QuantumGIS

6.- Una vez verificada se escoge la conexión creada y se presiona el botón Connect, donde dice SRID se ingresa el código de proyecto a usarse, que es el correspondiente al shapefile (32717). Se presiona el botón Add para

escoger el shapefile a importar, luego se elige el archivo a importar desde el disco y se presiona open.

En DB Relation Name se escribe el nombre de la tabla en que se escribirán los datos (minísculas y sin espacio) y en Schema se selecciona el esquema donde se desea crear la tabla.

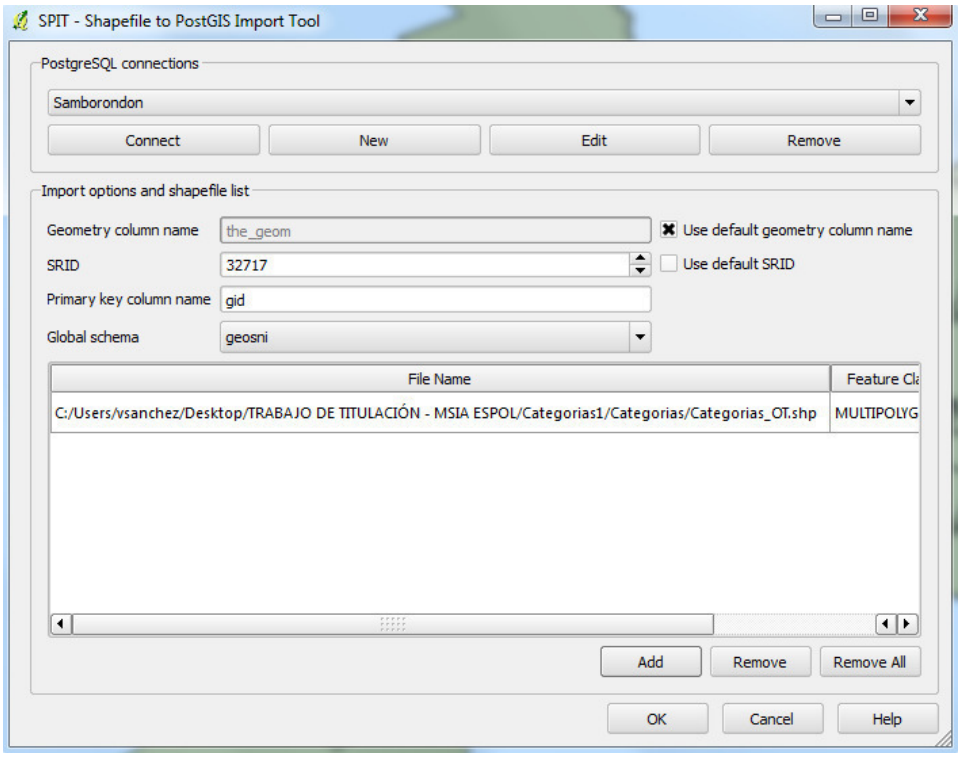

Figura 3.20 Selección de capa a cargar a la base de datos y definición de parámetros respectivos

Se presiona Ok y se iniciará la carga de datos geográficos a postgresql hasta su totalidad. Se puede repetir este proceso las veces necesarias, también pueden cargarse múltiples shapefiles a la vez.

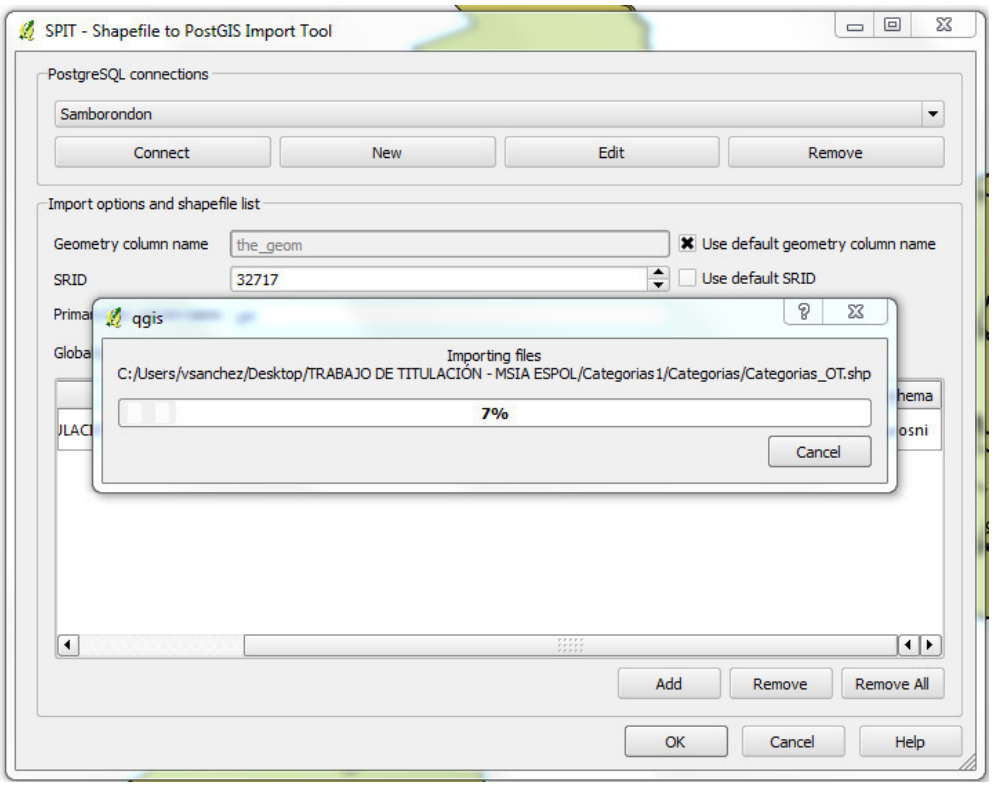

Figura 3.21 Importación de archivos a la base de datos postgresql

7.- Mediante la herramienta pgAdmin III (código libre) se verifica que se han cargado exitosamente los registros en la base de datos

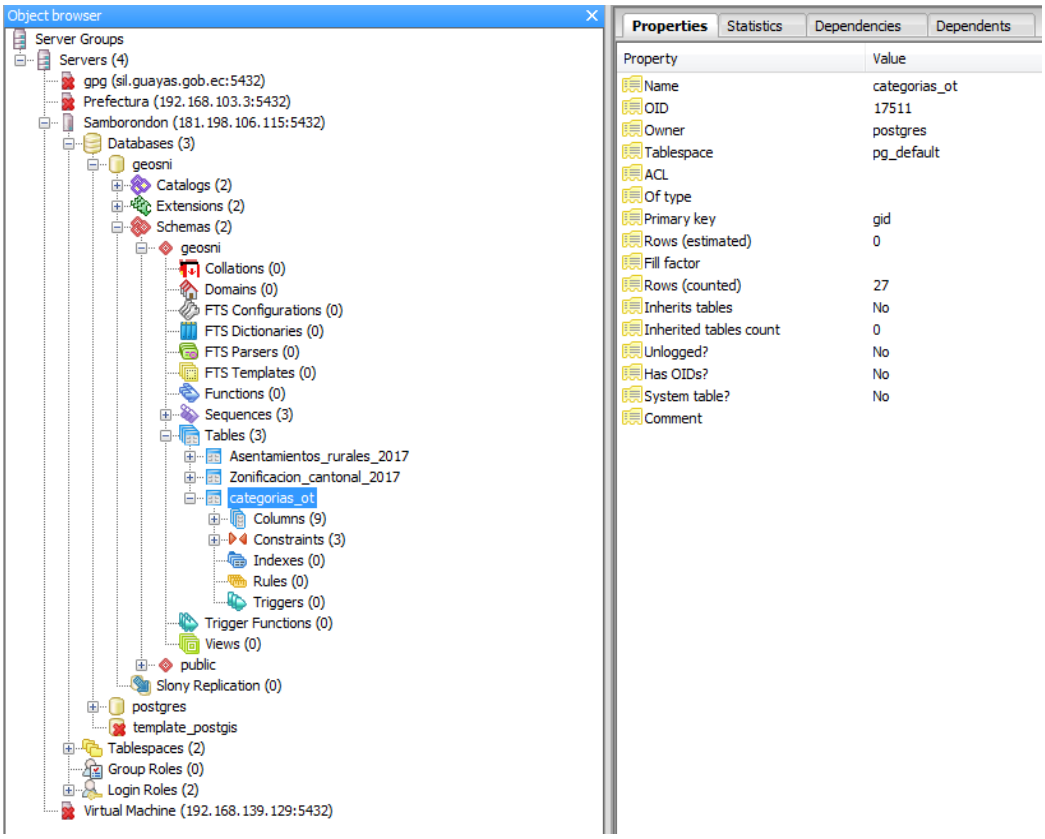

Figura 3.22 Comprobación de la existencia del archivo cargado en la base de datos mediante herramienta pgAdmin III

8.- Se ingresa a la administración del geoserver con las credenciales asignadas, la dirección de acceso es: http://181.198.106.115:8080/geoserver

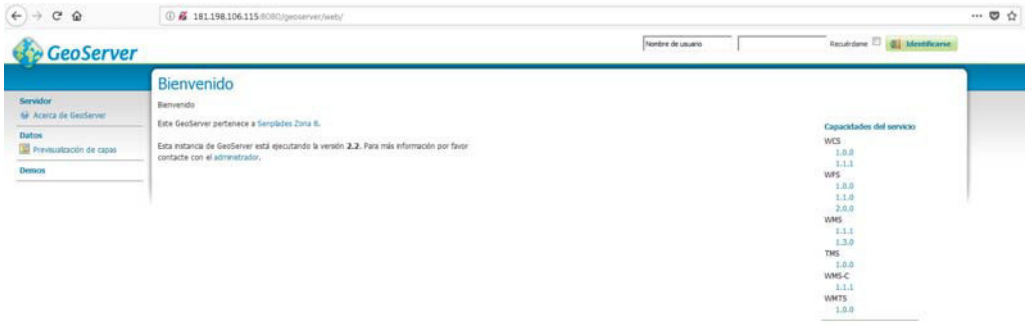

Figura 3.23 Acceso al geoserver del SIG del GAD Samborondón

9.- Se agrega la capa cargada al postgresql, ingresando a la sección Capas, presionando Agregar nuevo recurso

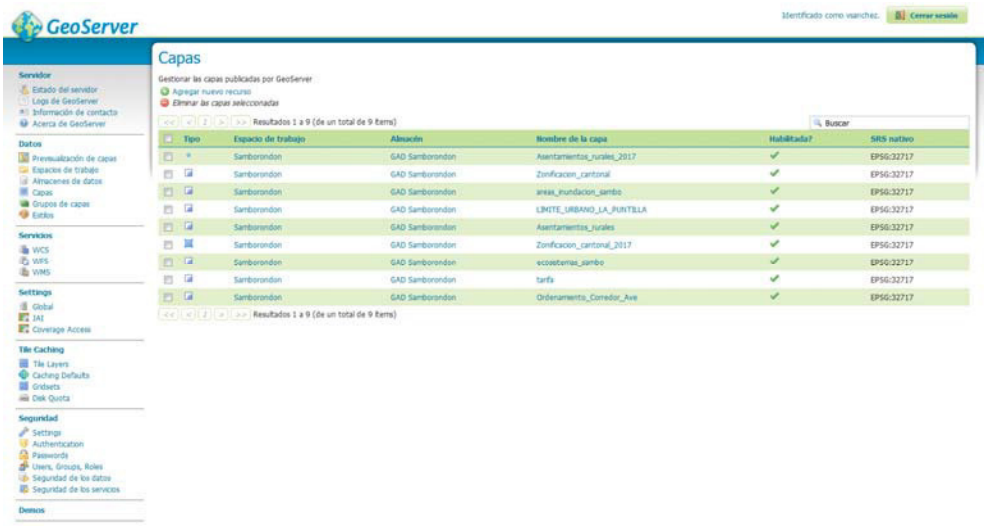

Figura 3.24 Gestión de las capas, se agrega al geoserver el nuevo recurso disponible en la base de datos postgresql

10.- En el campo Agregar capa de se selecciona la conexión que se realizó y se presiona el botón de Publicar la capa que se desea publicar.

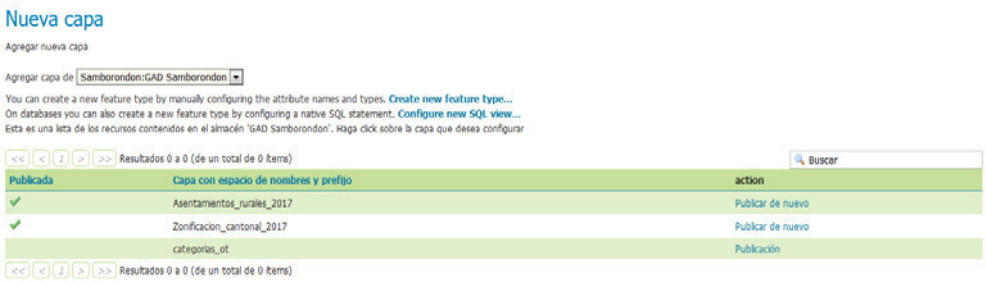

Figura 3.25 Publicación de la capa en el geoserver

11.- Se verifica la publicación de la información geográfica en el visor ingresando la URL correspondiente http://181.198.106.115/portal/

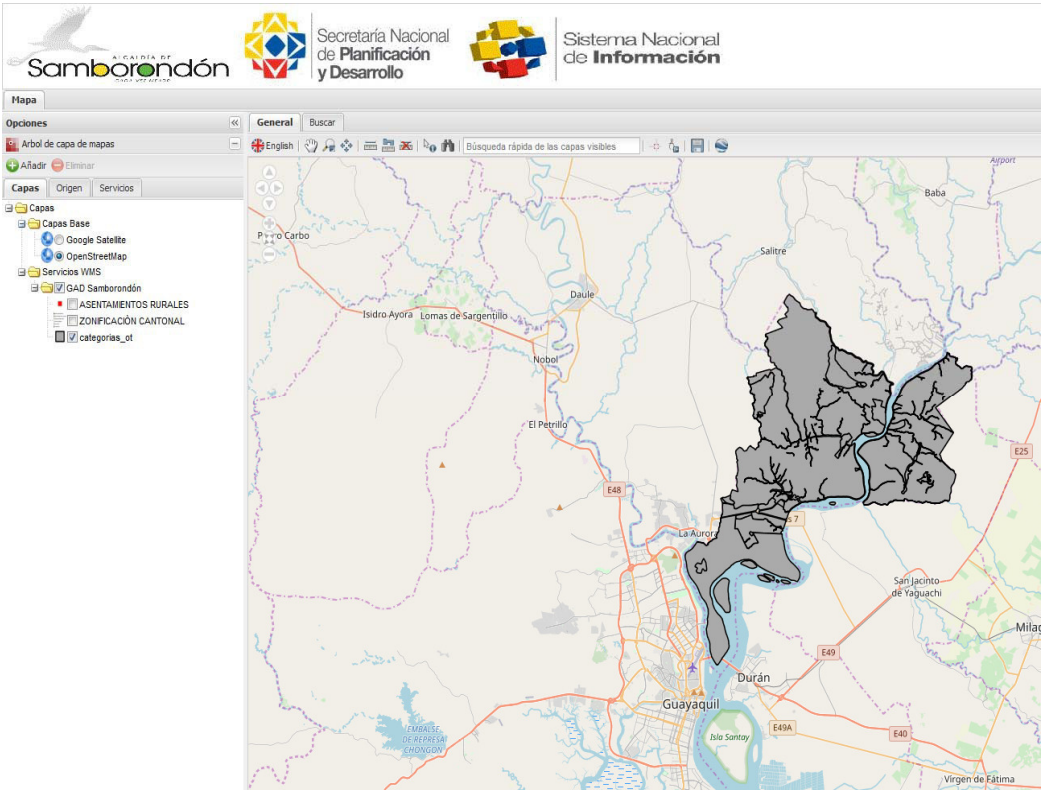

Figura 3.26 Verificación de la capa publicada en el visor geográfico del GAD Samborondón

3.5 Análisis de brecha

La adecuada realización de un análisis de brecha enfocado a la seguridad de la administración del sistema de información geográfica nos permite tener un diagnóstico de las prácticas de seguridad de la información con las que el GAD en base a las mejores prácticas en la industria.

“El análisis de brechas es una herramienta de análisis para comparar el estado y desempeño real de una organización, estado o situación en un momento dado, respecto a uno o más puntos de referencia seleccionados de orden local, regional, nacional y/o internacional.” [7]

Dentro de las prácticas recomendadas para realizar el análisis de brecha están:

- ISO/IEC 270002:2013

- PCI v3

- ENISA Article 13ª

- DDIS Information Security Manual

Entre las prácticas citadas se destaca a la ISO 27002 como la más aplicada para América Latina. [8]

CONTROLES DE SEGURIDAD

Los controles de seguridad son un conjunto de recomendaciones y buenas prácticas basados en estándares internacionales para la seguridad de la información como la SANS, NIST CF, PCI 3.0 e ISO 270002:2013, utilizadas para la defensa cibernética de las empresas. Éstos controles nos ofrecen soluciones para detener los ataques invasivos, tienen como principal beneficio priorizar y enfocar un número menor de acciones con altos resultados que permiten evaluar el nivel de madurez de la seguridad de la información.

SANS

El Instituto SANS (SysAdmin Audit, Networking and Security Institute) creado en el año de 1989 y con sede en Maryland – USA, es una institución que agrupa a más de 165 mil profesionales de la seguridad informática que cooperan en la educación e investigación referente a temas de seguridad y auditoría informática.

LA NORMA ISO 27002 COMO COMPLEMENTO PARA LA ISO 27001

Al escuchar hablar de seguridad de información inmediatamente se tiene como referencia la norma 27001. Ya que esta norma es muy importante dentro del sector debido a que toma como base todos los riesgos a los que se enfrenta la organización y tiene como objetivo principal establecer, implantar, mantener y mejorar de forma continua la seguridad de la información de la organización. [9] Dentro de este marco la norma ISO 270002 establece un catálogo de buenas prácticas que determina una serie de objetivos de control y controles que se integran dentro de todos los requisitos de la norma ISO 27001 en relación con el tratamiento de los riesgos.

Para realizar la evaluación del estado actual de seguridad del Sistema de Información Geográfico del GAD Municipal de Samborondón, se realizó un análisis de brechas “GAP” tanto para las cláusulas de la norma ISO/IEC 27001:2013, como para los dominios del Anexo A de la norma ISO/IEC 27002:2013 con la ayuda de una herramienta en Excel, de acuerdo con los datos entregados en entrevista realizada la funcionaria responsable del área de Tecnologías de Información y Comunicación del GAD en la cual se preguntó acerca de la seguridad de la información relacionada a la gestión de activos, seguridad física, control de acceso (lógico y físico), contratación

de personal de tecnologías, licenciamiento de software, funciones y características de los servidores físicos y virtuales, software y sistemas de información alojados en los servidores, etc.

A continuación se detallan los resultados generales obtenidos:

Tabla 2. Estado de cumplimiento de controles (cláusula y Anexo A) establecidos en la ISO/IEC 27002:2013

Código de Estado	Significado
D	El requisito está documentado e implementado
DD	El requisito está implementado pero debe ser documentado para asegurar su uso .
RD	El requisito no cumple con el estándar y debe ser rediseñado para cumplir con el estándar.
PNI	El requisito o proceso no existe / no está implementado. (no está documentado ni implementado)

Tabla 3. Cláusulas (4 – 10) ISO 27001

Cláusulas ISO 27001		
Obj. de Control	**Control**	**Estado de Cumplimiento**
4	**Contexto de la Organización**	
4.1	**Conocimiento de la organización y su contexto**	
4.1	La organización deberá determinar los asuntos internos y externos que sean relevantes para su propósito y que afectan su capacidad para lograr el o los resultados esperados de su sistema de gestión de la organización.	D
4.2	**Conocimiento de las necesidades y expectativas de las partes interesadas**	
4.2	La Organización deberá determinar:	
4.2 (a)	Las partes interesadas que sean relevantes para el sistema de gestión de la seguridad de la información;	PNI
4.2 (b)	Los requisitos de estas partes interesadas con respecto a la seguridad de la información	PNI
4.3	**Determinación del alcance del sistema de seguridad de la información**	
4.3	La organización deberá determinar los límites y la aplicabilidad del sistema de seguridad de la información para establecer su alcance.	PNI
4.3	Al determinar este alcance, la organización deberá considerar:	
4.3 (a)	Los asuntos internos y externos mencionados en 4.1	PNI
4.3 (b)	Los requisitos mencionados en el 4.2	PNI
4.3 (c)	Las interfaces y dependencias entre las actividades desempeñadas por la organización, y aquellas que desarrollan otras organizaciones	PNI
4.4	**Sistema de Gestión de la Seguridad de la Información**	
4.4	La organización deberá establecer, implementar, mantener y mejorar de manera continua el sistema de seguridad de la información, de acuerdo a los requisitos de la Norma Internacional	PNI
5	**Liderazgo**	
5.1	**Liderazgo y compromiso**	
5.1	La Alta Dirección deberá demostrar liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información mediante las siguientes acciones:	
5.1 (a)	Garantizando el establecimiento de la política y objetivos de la seguridad de la información y que estos sean compatibles con la dirección estratégica de la organización	PNI
5.1 (b)	Garantizando la integración de los requisitos del sistema de gestión de la información dentro de los procesos de la organización	PNI
5.1 (c)	Garantizando la disponibilidad de los recursos necesarios para el sistema de gestión de la seguridad de la información	PNI
5.1 (d)	Comunicando la importancia de una gestión efectiva de seguridad de la información y de adecuarse a los requisitos del sistema de gestión de la seguridad de la información	PNI
5.1 (e)	Garantizando que el sistema de seguridad de la información logre sus resultados esperados	PNI

Continuación Tabla 3

5.1 (f)	Dirigiendo y dando soporte a las personas para que contribuyan con la efectividad del sistema de gestión de la seguridad de la información	PNI
5.1 (g)	Promoviendo la mejora continua	PNI
5.1 (h)	Apoyando las funciones de la gerencia que permitan demostrar su liderazgo siempre que corresponda a sus áreas de responsabilidad	PNI
5.2	**Política**	
5.2	La Alta Dirección deberá establecer una política de seguridad de la información que:	
5.2 (a)	Sea adecuada al propósito de la organización	PNI
5.2 (b)	Incluya los objetivos de seguridad de la información (ver 6.2) o proporcione un esquema para la determinación de los objetivos de la seguridad de la información	PNI
5.2 (c)	Incluya el compromiso de satisfacer los requisitos aplicables relacionados a la seguridad de la información	PNI
5.2 (d)	Incluya el compromiso de mejora continua del sistema de gestión de la seguridad de la información	PNI
5.2	La política de seguridad de la información deberá:	
5.2 (e)	Estar disponible como información documentada	PNI
5.2 (f)	Ser comunicada dentro de la organización	PNI
5.2 (g)	Estar disponible para las partes interesadas, de la manera que estimen adecuada	PNI
5.3	**Funciones, responsabilidades y autoridad de la organización**	
5.3	La Alta Gerencia deberá garantizar que se asigne y comunique las responsabilidades y autoridad para los roles relacionados con la seguridad de la información.	D
5.3	La Alta Dirección deberá asignar la responsabilidad y autoridad para:	
5.3 (a)	Garantizar que el sistema de gestión de seguridad de la información se adapte a los requisitos de esta Norma Internacional	PNI
5.3 (b)	Informar acerca del desempeño del sistema de gestión de seguridad de la información a la Alta Gerencia	PNI
6	**Planificación**	
6.1	**Acciones para enfrentar los riesgos y las oportunidades**	
6.1.1	**General**	
6.1.1	Al planificar el sistema de gestión de la seguridad de la información, la organización deberá considerar los temas referidos al punto 4.1 y a los requisitos mencionados en el punto 4.2, y determinar los riesgos y oportunidades que deben orientarse a:	
6.1.1 (a)	Garantizar que el sistema de gestión de seguridad de la información logre los resultados esperados	PNI
6.1.1 (b)	Evitar o reducir efectos indeseados	DD
6.1.1 (c)	Lograr la mejora continua	PNI

Continuación Tabla 3

6.1.1	La organización deberá planificar:	
6.1.1 (d)	Las acciones destinadas a manejar estos riesgos y oportunidades	PNI
6.1.1 (e)	Cómo	PNI
6.1.1 (e1)	Integrar e implementar las acciones dentro de los procesos del sistema de gestión de seguridad de la información	PNI
6.1.1 (e2)	Evaluar la efectividad de estas acciones	PNI
6.1.2	**Evaluación de los riesgos de seguridad de la información**	
6.1.2	La organización deberá definir y aplicar el proceso de evaluación de los riesgos de seguridad de la información que permita:	
6.1.2 (a)	establecer y mantener los criterios de los riesgos de seguridad de la información que incluyan:	
6.1.2 (a1)	Los criterios de aceptación del riesgo	PNI
6.1.2 (a2)	Los criterios para el desempeño de las evaluaciones de los riesgos de la seguridad de la información	PNI
6.1.2 (b)	Garantizar que la repetición de la evaluación repetitiva de los riesgos de la seguridad de la información arroje resultados válidos, consistentes y comparativos	PNI
6.1.2 (c)	Identificar los riesgos de seguridad de la información:	PNI
6.1.2 (c1)	Aplicando el proceso de evaluación de los riesgos de seguridad de la información para identificar los riesgos asociados a la pérdida de la confidencialidad, integridad y disponibilidad de la información dentro del alcance del sistema de gestión de seguridad de la información	PNI
6.1.2 (c2)	Identificando a los originadores de los riesgos	PNI
6.1.2 (d)	Analizar los riesgos de seguridad de la información:	PNI
6.1.2 (d1)	Evaluando las consecuencias potenciales que se producirían si los riesgos identificados en el punto 6.1.2 c) 1) llegarán a materializarse	PNI
6.1.2 (d2)	Evaluando la probabilidad realista de la ocurrencia de los riesgos identificados en el punto 6.1.2 c) 1)	PNI
6.1.2 (d3)	Determinando los niveles de riesgo	PNI
6.1.2 (e)	Evaluar los riesgos de la seguridad de la información:	PNI
6.1.2 (e1)	Comparando los resultados del análisis de riesgos con los criterios de riesgos establecidos en el punto 6.1.2 a)	PNI
6.1.2 (e2)	Priorizando los riesgos analizados para el tratamiento de los riesgos.	PNI
6.1.2	La organización deberá conservar la información documentada acerca del proceso de evaluación de la seguridad de la información.	PNI
6.1.3	**Tratamiento de los riesgos de la seguridad de la Información**	
6.1.3	La organización deberá definir y aplicar el proceso de tratamiento de los riesgos de la seguridad de la información con la finalidad de:	
6.1.3 (a)	Seleccionar las opciones de tratamiento de los riesgos de seguridad de la información, tomando en cuenta los resultados de la evaluación de los riesgos	PNI

Continuación Tabla 3

6.1.3 (b)	Determinar todos los controles que son necesarios para implementar la opción u opciones seleccionadas para el tratamiento de la seguridad de la información	PNI
6.1.3 (c)	Comparar los controles determinados en el punto 6.1.3 b), que anteriormente fueron determinados en el Anexo A, y verificar que no se haya omitido ningún control que sea de utilidad	PNI
6.1.3 (d)	Elaborar una Declaración de Aplicabilidad que contiene los controles necesarios (ver punto 6.1.3 b) y c)) y la argumentación de las inclusiones, si se aplicaran o no, y la argumentación de las exclusiones del control del Anexo A	PNI
6.1.3 (e)	Formular el tratamiento de los riesgos de seguridad de la información	PNI
6.1.3 (f)	Hacer que los poseedores del riesgos aprueben el plan de del tratamiento de riesgos de la seguridad de la información y acepten los riesgos residuales de la seguridad de la información.	PNI
6.1.3	La organización deberá conservar la información documentada acerca del proceso de tratamiento de los riesgos de la seguridad de la información	PNI
6.2	**Objetivos de Seguridad de la Información y la planificación para alcanzarlos**	
6.2	La organización deberá establecer los objetivos de seguridad de la información en relación a las funciones y niveles	PNI
6.2	Los objetivos de seguridad de la información deberán:	
6.2 (a)	Ser consistentes con la política de seguridad de la información	PNI
6.2 (b)	Ser medibles (si es aplicable)	PNI
6.2 (c)	Tomar en cuenta los requisitos de la seguridad de la información y los resultados de la evaluación de riesgos y del tratamiento de riesgos	PNI
6.2 (d)	Ser comunicados	PNI
6.2 (e)	Actualizarse, si así lo requiriera	PNI
6.2	La organización deberá conservar la información documentada sobre los objetivos de la seguridad de la información.	PNI
6.2	Al planificar cómo alcanzar sus objetivos de seguridad de la información, la organización deberá determinar:	
6.2 (f)	Qué deberá hacer	PNI
6.2 (g)	Qué recursos necesitará	PNI
6.2 (h)	Quién será el responsable	PNI
6.2 (i)	Cuándo será alcanzado dicho objetivo	PNI
6.2 (j)	Cómo medirá los resultados	PNI
7	**Apoyo / Soporte**	
7.1	**Recursos**	
7.1	La organización deberá determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la información.	D
7.2	**Competencia**	

Continuación Tabla 3

7.2	La organización:	
7.2 (a)	Determinará la competencia necesaria de la o las personas que harán el trabajo bajo su control, el mismo que afectará el desempeño de su seguridad de la información	D
7.2 (b)	Garantizará que estas personas tengan una competencia en base a una educación, entrenamiento y experiencia adecuados	D
7.2 (c)	Si fuera el caso, llevar a cabo acciones que permitan adquirir las competencias necesarias y evaluar la efectividad de las acciones tomadas	D
7.2 (d)	Conservar una adecuada documentación de la información como evidencia de la competencia	DD
7.3	**Concientización**	
7.3	Las personas que hacen el trabajo bajo en control de la organización deberán ser conscientes de:	
7.3 (a)	La política de seguridad de la información	D
7.3 (b)	Su contribución a la efectividad del sistema de gestión de la seguridad de la información, incluyendo los beneficios de la mejora en el desempeño de la seguridad de la información	D
7.3 (c)	Las implicancias de la no conformidad con los requisitos del sistema de gestión de la seguridad de la información	PNI
7.4	**Comunicación**	
7.4	La organización determinará la necesidad de las comunicaciones internas y externas con respecto al sistema de gestión de seguridad de la información incluyendo:	
7.4 (a)	Qué se debe comunicar	PNI
7.4 (b)	Cuándo se debe comunicar	PNI
7.4 (c)	Con quién se debe comunicar	PNI
7.4 (d)	Quién debe comunicar	PNI
7.4 (e)	El proceso por el cual se debe hacer efectiva la comunicación	PNI
7.5	**Documentación de la información**	
7.5.1	**General**	
7.5.1	El sistema de gestión de la información incluirá:	
7.5.1 (a)	la documentación de la información requerida por la Norma Internacional	PNI
7.5.1 (b)	La documentación de la información determinada por la organización como necesaria para la efectividad del sistema de gestión de la seguridad de la información	PNI
7.5.2	**Creación y actualización**	
7.5.2	Al crear y actualización la información documentada, la organización deberá garantizar una apropiada:	
7.5.2 (a)	Identificación y descripción (e.g. un título, fecha, autor o número de referencia)	DD

Continuación Tabla 3

7.5.2 (b)	Formato (e.g. idioma, versión del software, gráficos) y los medios (e.g. papel, electrónico)	DD
7.5.2 (c)	Revisión y aprobación para una debida adecuación e idoneidad	DD
7.5.3	**Control de la información documentada**	
7.5.3	La información documentada requerida por el sistema de gestión de seguridad de la información y por la presente Norma Internacional deberá ser contralada para garantizar:	
7.5.3 (a)	La disponibilidad e idoneidad para su uso, donde y en el momento que sea necesario	PNI
7.5.3 (b)	Su adecuada protección (e.g. de pérdida de confidencialidad, uso inadecuado o pérdida de integridad)	PNI
7.5.3	Para el control de la información documentada, la organización deberá desarrollar las siguientes actividades, según corresponda:	PNI
7.5.3 (c)	Distribución, acceso, recuperación y uso	PNI
7.5.3 (d)	Almacenamiento y conservación, incluyendo la conservación de la legibilidad	PNI
7.5.3 (e)	Control de cambios (e.g. control de la versión)	PNI
7.5.3 (f)	Retención y disposición	PNI
7.5.3	Se deberá identificar y controlar, en la medida de lo posible, la información documentada de origen externo, determinado por la organización como necesaria para la planificación y operación del sistema de gestión de la seguridad de la información.	PNI
8	**Operación**	
8.1	**Planificación y control operacional**	
8.1	La organización deberá planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de la seguridad de la información e implementar acciones determinadas en el punto 6.1. La organización también deberá implementar planes para lograr los objetivos de seguridad de la información señalados en el punto 6.2. La organización deberá mantener información documentada de tal forma que garantice que se está llevando a cabo los procesos de acuerdo a lo planificado. La organización deberá mantener un control sobre los cambios planificados y revisar las consecuencias de los cambios involuntarios, tomando acción para mitigar cualquier efecto adverso, si el caso así lo ameritara. La organización deberá garantizar identificar y controlar todos los procesos tercerizados.	DD
8.2	**Evaluación de los riesgos de seguridad de la información**	
8.2	La organización deberá llevar a cabo evaluaciones de los riesgos de seguridad de la información a intervalos planificados o cuando se proponen o se dan cambios, tomando en cuenta los criterios establecidos en el punto 6.1.2 a). La organización deberá conservar la información documentada de los resultados de la evaluación de los riesgos de la seguridad de la información.	PNI
8.3	**Tratamiento de los riesgos de la seguridad de la Información**	
8.3	La organización deberá implementar el plan de tratamiento de los riesgos de seguridad de la información. La organización deberá conservar la información documentada de los resultados del tratamiento de los riesgos de la seguridad de la información.	PNI

Continuación Tabla 3

9	**Evaluación del desempeño**	
9.1	**Monitoreo, medición, análisis y evaluación**	
9.1	La organización deberá evaluar el desempeño de la seguridad de la información y la efectividad del sistema de gestión de la información.	PNI
9.1	La organización deberá determinar:	
9.1 (a)	Qué necesidades deben ser monitoreadas y sometidas a medición, incluyendo los procesos y controles de la seguridad de la información	PNI
9.1 (b)	Los métodos de monitoreo, medición, análisis y evaluación, según corresponda, con la finalidad de garantizar la validez de los resultados	PNI
9.1 (c)	Cuándo deberá ejecutarse el monitoreo y la medición	PNI
9.1 (d)	Quién deberá hacer el monitoreo y la medición	PNI
9.1 (e)	Cuándo deberán analizarse y evaluarse los resultados del monitoreo y de la medición	PNI
9.1 (f)	Quién deberá analizar y evaluar los resultados	PNI
9.1	La organización deberá conservar adecuadamente la información documentada como evidencia de los resultados del monitoreo y la medición.	PNI
9.2	**Auditorías internas**	
9.2	La organización deberá dirigir auditorías internas en intervalos planificados con la finalidad de proporcionar información con respecto a que si el sistema de gestión de la seguridad de la información:	PNI
9.2 (a)	Se ajusta a:	
9.2 (a1)	Los propios requisitos de la organización con respecto a su sistema de gestión de la información	PNI
9.2 (a2)	Los requisitos de la Norma Internacional	PNI
9.2 (b)	se implementa y mantiene de manera efectiva	PNI
9.2	La organización deberá:	
9.2 (c)	Planificar, establecer, implementar y mantener un programa o programas, incluyendo la frecuencia, métodos, responsabilidades, requisitos de planificación y reporte. El o los programas deberán tomar en cuenta la importancia de los procesos involucrados y los resultados de las auditorías previas	PNI
9.2 (d)	Definir los criterios y alcance de la auditoria	PNI
9.2 (e)	Seleccionar auditores y dirigir auditorías que aseguren la objetividad e imparcialidad del proceso auditor	PNI
9.2 (f)	Garantizar que los resultados de la auditoría sean informados a la gerencia correspondiente	PNI
9.2 (g)	Conservar información documentada como evidencia del o de los programas y los resultados de la auditoría	PNI
9.3	**Revisión por parte de la Dirección**	
9.3	La Alta Dirección deberá revisar el sistema de gestión de seguridad de la información a intervalos establecidos para garantizar su continua disponibilidad, adecuación y efectividad	PNI
9.3	La revisión por parte de la Dirección deberá incluir lo siguiente:	

Continuación Tabla 3

9.3 (a)	El estatus de las acciones de las anteriores revisiones por parte de la Dirección	PNI
9.3 (b)	Cambios en los asuntos externos e internos que tuvieron relevancia para el sistema de gestión de la seguridad de la información	PNI
9.3 ©	Retroalimentación sobre el desempeño de la seguridad de la información, incluyendo la tendencia en:	PNI
9.3 (c1)	Las no conformidades y las acciones correctivas	PNI
9.3 (c2)	Resultados del monitoreo y medición	PNI
9.3 (c3)	Resultados de la auditoría	PNI
9.3 (c4)	Cumplimiento de los objetivos de seguridad de la información	PNI
9.3 (d)	Retroalimentación por parte de las partes interesadas	PNI
9.3 (e)	Resultados de la evaluación de los riesgos y estatus del plan de tratamiento de los riesgos	PNI
9.3 (f)	Oportunidades de mejora continua	PNI
9.3	Los resultados de la revisión por parte de la dirección deberán incluir las decisiones con respecto a las oportunidades de mejora continua y cualquier necesidad de cambios en el sistema de gestión de seguridad de la información.	PNI
9.3	La organización deberá conservar la información documentada como evidencia de los resultados de las revisiones por parte de la dirección	PNI
10	**Mejora**	
10.1	**No conformidad y acción correctiva**	
10.1	Cuando ocurre una no conformidad, la organización debe:	
10.1 (a)	Reaccionar hacia la no conformidad, y según corresponda:	PNI
10.1 (a1)	Tomar acción para controlarla y corregirla	PNI
10.1 (a2)	Lidiar con las consecuencias	PNI
10.1 (b)	Evaluar la necesidad de acción para eliminar las causas de la no conformidad, con la finalidad de evitar la recurrencia o la ocurrencia en cualquier otro lugar, mediante:	PNI
10.1 (b1)	La revisión de la no conformidad	PNI
10.1 (b2)	La determinación de las causas de la no conformidad	PNI
10.1 (b3)	La verificación de si existe una no conformidad similar, o podría darse	PNI
10.1 ©	La implementación de una acción necesaria	PNI
10.1 (d)	La revisión de la efectividad de las acciones correctivas tomadas	PNI
10.1 (e)	La implementación de cambios al sistema de gestión de seguridad de la información, si fuera necesario.	PNI
10.1	Las acciones correctivas deben ser acordes a los efectos de las no conformidades encontradas.	PNI
10.1	La organización deberá conservar la información documentada como evidencia de:	PNI
10.1 (f)	La naturaleza de las no conformidades y cualquier acción tomada posteriormente	PNI
10.1 (g)	Los resultados de las acciones correctivas	PNI
10.2	**Mejora continua**	
10.2	La organización deberá mejorar de manera continua la idoneidad, adecuación y efectividad del sistema de gestión de la seguridad de la información.	PNI

NORMA ISO 27001:2013 (CLÁUSULAS)

El cumplimiento de los objetos de control de las cláusulas de la norma ISO27001:2013 se obtuvo los siguientes resultados como se observan en los siguientes gráficos y tablas:

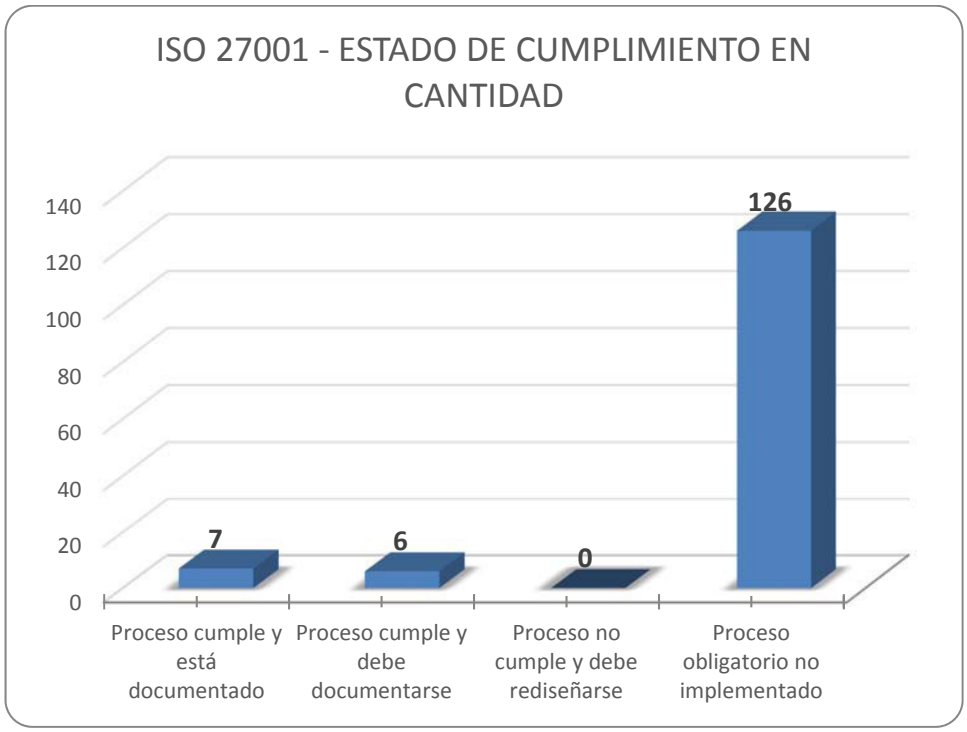

Figura 3.27 Cláusulas ISO/IEC 27001:2013, resultado actual del estado de cumplimiento en cantidad.

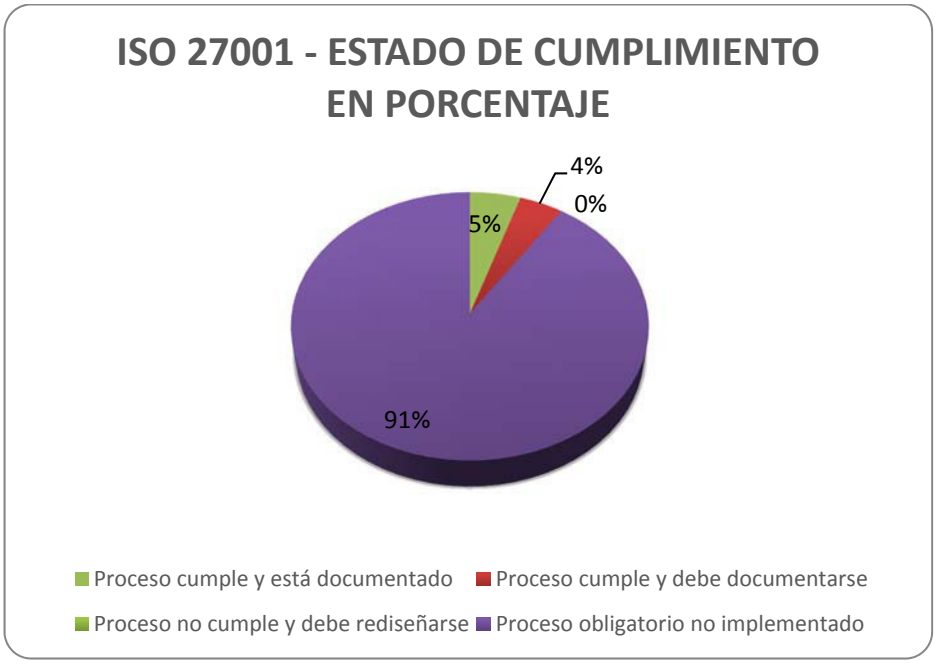

Figura 3.28 Cláusulas ISO/IEC 27001:2013, resultado actual del estado de cumplimiento en porcentaje.

El 5% de los controles están documentados. El 4% de los controles se llevan a cabo y el proceso necesita ser documentado para asegurar el proceso y mitigar los riegos. El 91% de los controles no están implementados.

En el diagrama de barras a continuación, se observa el nivel de cumplimiento de cada cláusula de manera clara:

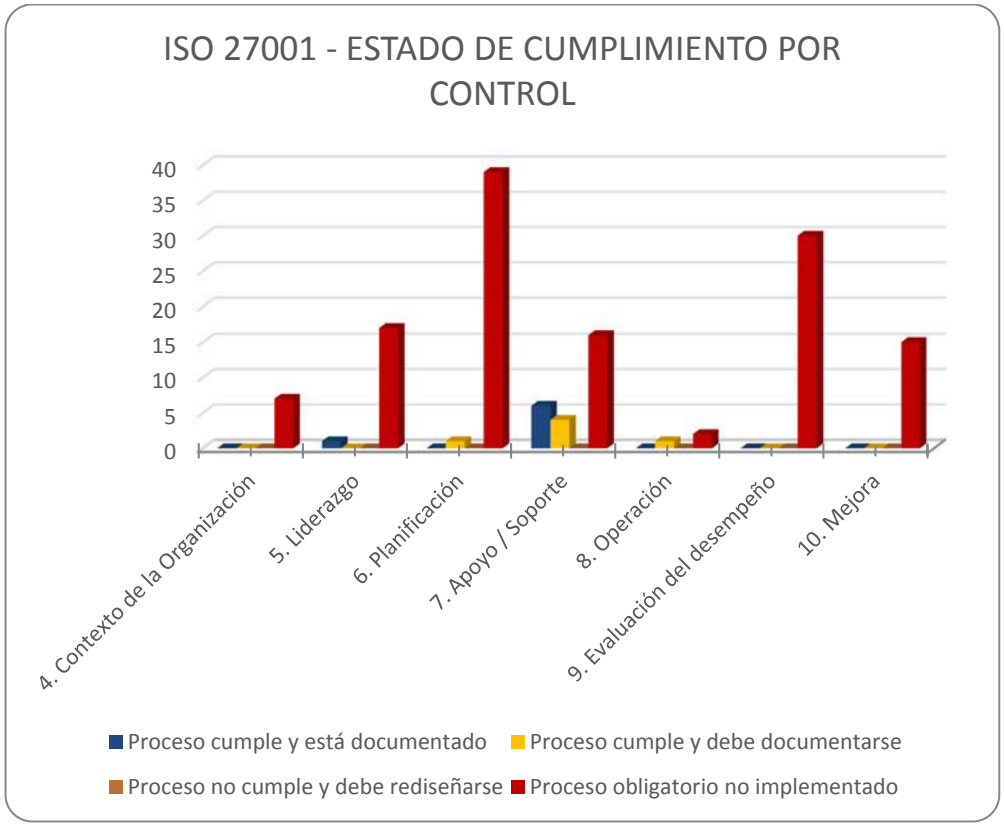

Figura 3.29 Cláusulas ISO/IEC 27001:2013, nivel de cumplimiento porcentaje de las cláusulas

Tabla 4. Resultados obtenidos objetos de control ISO/IEC 27001:2013

27001	Proceso cumple y está documentado	Proceso cumple y debe documentarse	Proceso no cumple y debe rediseñarse	Proceso obligatorio no implementado	TOTAL
4. Contexto de la Organización	0	0	0	7	7
5. Liderazgo	1	0	0	17	18
6. Planificación	0	1	0	39	40
7. Apoyo / Soporte	6	4	0	16	26
8. Operación	0	1	0	2	3
9. Evaluación del desempeño	0	0	0	30	30
10. Mejora	0	0	0	15	15
TOTAL	7	6	0	126	139

Tabla 5. Anexo A - ISO 27001:2013

27001 Anexo A		
Objetivos de Control	**Controles**	**Estado de Cumplimiento**
A.5 Políticas de seguridad de la información		
A.5.1 Gestión de la Gerencia para la seguridad de la información		
A.5.1.1 Políticas de la seguridad de de la información	La gerencia debe definir, aprobar, publicar y comunicar a los trabajadores y partes externas involucradas, una serie de políticas para la seguridad de la información.	D
A.5.1.2 Revisión de las políticas de seguridad de la información	Las políticas de seguridad de la información deben ser revisadas en intervalos planificados o si ocurren cambios significativos, para garantizar su idoneidad, adecuación y efectividad continuos.	DD
A.6 Organización de la seguridad de la información		
A.6.1 Organización interna		
A.6.1.1 Funciones y responsabilidades de la seguridad de la información	Se debe definir y asignar todas las responsabilidades de la seguridad de la información.	PNI
A.6.1.2 Segregación de tareas	Tareas o áreas de responsabilidad en conflicto deben ser segregadas para reducir las oportunidades de modificación no autorizada o involuntaria o el uso inadecuado de los activos de la organización.	PNI
A.6.1.3 Contacto con las autoridades	Se debe mantener contacto adecuado con las autoridades respectivas	PNI
A.6.1.4 Contactos con grupos especiales de interés	Se debe mantener contacto con grupos especiales de interés u otros forums y asociaciones de profesionales especializados en seguridad	PNI
A.6.1.5 Seguridad de la información en la gestión del proyecto	La seguridad de la información debe adaptarse a la gestión del proyecto, independientemente del tipo de proyecto.	PNI
A.6.2 Equipos móviles y trabajo a distancia		
Objetivo: Garantizar la seguridad del trabajo a distancia y del uso de los equipos móviles		
A.6.2.1 Política de los equipos móviles	Se debe adoptar políticas y medidas de soporte de seguridad para el manejo de los riesgos derivados del uso de equipos móviles.	PNI
A.6.2.2 Trabajo a distancia	Se debe implementar políticas y medidas de soporte de seguridad para proteger la información a la que se accede, procesa o almacena en los lugares de trabajo a distancia.	PNI
A.7 Seguridad de los recursos humanos		
A.7.1. Antes de reclutarlo		
A.7.1.1 Filtración	Se debe llevar a cabo la verificación de los antecedentes de todos los candidatos al empleo de acuerdo a las leyes y regulaciones vigentes y a la ética; y debe ser proporcional a los requisitos del negocio, la clasificación de la información a la que tendrá acceso y los riesgos que se perciban.	DD
A.7.1.2 Términos y condiciones del empleo	Los acuerdos contractuales con los trabajadores y contratistas debe fijar sus responsabilidades y las de la organización con respecto a la seguridad de la información.	PNI
A.7.2 Durante el trabajo		
Objetivo: Garantizar que los trabajadores y los contratistas sean conscientes y cumplan con las responsabilidades de la seguridad de la información		
A.7.2.1 Responsabilidades de la Gerencia	La Gerencia debe instar a todos los trabajadores y contratistas a aplicar la seguridad de la información de acuerdo a las políticas y procedimientos establecidos por la organización.	D

Continuación Tabla 5

A.7.2.2 Concientización, educación y capacitación sobre seguridad de la información	Todos los trabajadores de la organización y los contratistas, si así lo requiriesen, deben recibir una adecuada educación de concientización y capacitación, así como actualizaciones regulares sobre las políticas y procedimientos organizaciones, de acuerdo a las funciones de trabajo que desempeñen.	DD
A.7.2.3 Procesos disciplinarios	Debe haber un proceso disciplinario formal que debe ser comunicado en el lugar, para tomar acción contra los trabajadores que comentan alguna infracción contra la seguridad de la información.	D
A.7.3 Término y cambio de empleo		
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o término del empleo		
A.7.3.1 Término o cambio de responsabilidades de empleo	Se debe definir, comunicar y reforzar a todos los trabajadores y contratistas, las responsabilidades y tareas de seguridad de la información que permanecerán válidos después del término del empleo.	PNI
A.8 Gestión de los Activos		
A.8.1 Responsabilidades sobre los activos		
Objetivo: Identificar los activos de la organización y definir las responsabilidades adecuadas de protección		
A.8.1.1 Inventario de activos	Se debe identificar los activos y las instalaciones asociados a la información y al procesamiento de la información y se debe diseñar y mantener un inventario de dichos activos.	D
A.8.1.2 Propiedad de los activos	Los activos que se encuentren identificados en el inventario deben de ser asignados a un “propietario”.	D
A.8.1.3 Uso aceptable de los activos	Se debe implementar, documentar e implementar las reglas para el uso aceptable de la información y de los activos relacionados a la información y a las instalaciones de procesamiento de la información.	D
A.8.1.4 Retorno de los activos	Todos los trabajadores y usuarios internos y externos deberán devolver todos los activos de la organización que estén en su posesión una vez terminado su empleo, contrato o acuerdo.	D
A.8.2 Clasificación de la información		
Objetivo: Garantizar que la información reciba un nivel adecuado de protección de acuerdo a su importancia dentro de la organización		
A.8.2.1 Clasificación de la información	La información debe ser clasificada en términos de los requisitos y valores legales, siendo crítica y sensible ante la divulgación y modificación no autorizada.	PNI
A.8.2.2 Etiquetado de la información	Se debe desarrollar e implementar una serie de procedimientos adecuados para el etiquetado de la información, de acuerdo al esquema de clasificación de la información adoptado por la organización.	PNI
A.8.2.3 Manejo de los activos	Se debe desarrollar e implementar procedimientos de manejo de los activos de acuerdo al esquema de clasificación de la información adoptado por la organización.	D

Continuación Tabla 5

A.8.3 Manejo de los medios de comunicación		
Objetivo: Prevenir la divulgación, modificación, retiro o destrucción no autorizada de la información almacenada en los medios de comunicación		
A.8.3.1 Gestión de medios de comunicación removibles	Se debe implementar procedimientos para la gestión de los medios de comunicación removibles de acuerdo al esquema de clasificación adoptado por la organización	PNI
A.8.3.2 Disposición de los medios comunicación	Los medios comunicación deben ser desechados de manera segura cuando ya no son necesarios, mediante procedimientos formales.	PNI
A.8.3.3 Transferencias física de los medios de comunicación	Los medios de comunicación que contienen información deben ser protegidos contra el acceso no autorizado, mal uso o corrupción durante su transporte.	PNI
A.9 Control de acceso		
A.9.1 Requisitos del negocio sobre control del acceso		
A.9.1.1 Política de control de acceso	Se debe establecer, documentar y revisar la política de control del acceso en base a los requisitos del negocio y de la seguridad de la información.	D
A.9.1.2 Acceso a la redes y a los servicios de las redes	Los usuarios deben tener acceso únicamente a la red o a los servicios de redes a los que han sido autorizados a usar.	D
A.9.2 Gestión del acceso al usuario		
Objetivo: Garantizar el acceso al usuario autorizado para evitar el acceso no autorizado a los sistemas y servicios		
A.9.2.1 Registro y des-registro del usuario	Se debe implementar un proceso registro y des-registro del usuario para habilitar los derechos de acceso.	PNI
A.9.2.2 Provisión de acceso al usuario	Se debe implementar un proceso formal de provisión de acceso al usuario, para asignar o revocar los derechos de acceso a todos los tipos de usuarios a todos los sistemas y servicios.	PNI
A.9.2.3 Gestión de los derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de los derechos de acceso privilegiado.	PNI
A.9.2.4. Gestión de información de autenticación secreta de usuarios	Se debe controlar la asignación de la información de autenticación secreta de usuarios mediante un proceso de gestión formal.	PNI
A.9.2.5 Verificación de los derechos de acceso de los usuarios	Los propietarios de los activos deben verificar los derechos de acceso de los usuarios a intervalos regulares.	PNI
A.9.2.6 Retiro o ajuste de los derechos de acceso	Los derechos de acceso a todos los trabajadores y terceros a la información y a las instalaciones de procesamiento de la información deben ser retirados al término del empleo, contrato o acuerdo, o ajustado luego de un cambio.	DD
A.9.3 Responsabilidades del usuario		
Objetivo: Hacer a los usuarios responsables de salvaguardar la autenticación de su información		
A.9.3.1 Uso de información secreta de autenticación	Se debe solicitar a los usuarios seguir las prácticas de la organización sobre el uso de la información secreta de autenticación.	D
A.9.4 Control de acceso a sistemas y aplicaciones		
Objetivo: Evitar el acceso no autorizado a los sistemas y aplicaciones		
A.9.4.1 Restricción del acceso a la información	Se debe restringir el acceso a la información y a las funciones de aplicación del sistema de acuerdo a la política de control de acceso.	DD
A.9.4.2 Procedimiento seguro de logeo	Si así lo requiere la política de control del acceso, se debe controlar el acceso a los sistemas y a las aplicaciones, mediante un procedimiento seguro de logeo.	DD

Continuación Tabla 5

A.9.4.3 Sistema de gestión de la clave	Los sistemas de gestión de la clave deben ser interactivos y deben asegurar la calidad de las claves.	DD
A.9.4.4 Uso de programas utilitarios de privilegio	Se debe restringir y controlar severamente el uso de programas utilitarios que puedan controlar manualmente el sistema y los controles de la aplicación.	PNI
A.9.4.5 Control del acceso para programar el código fuente	Se debe restringir el acceso al programa de código fuente.	PNI
A.10 Criptografía		
A.10.1 Controles de la criptografía		
Objetivo: Asegurar el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información		
A.10.1.1 Política del uso de controles criptográficos	Se debe desarrollar e implementar una política de uso de controles criptográficos para proteger la información.	DD
A.10.1.2 Gestión de las claves	Se debe desarrollar e implementar una política para el uso, protección y tiempo de vida de las claves criptográficas a lo largo de todo su ciclo de vida.	DD
A.11 Seguridad física y medioambiental		
A.11.1 Áreas seguras		
Objetivo: Evitar acceso físico no autorizado, daño e interferencia a la información e instalaciones de procesamiento de la información de la organización.		
A.11.1.1 Perímetro de seguridad física	Se debe determinar y utilizar los perímetros de seguridad para proteger las áreas que contienen información sensible y crítica y las instalaciones de procesamiento de la información.	PNI
A.11.1.2 Controles físicos de los ingresos	Se debe proteger las áreas seguras mediante controles adecuados de ingreso para garantizar el ingreso de sólo personal autorizado.	PNI
A.11.1.3 Seguridad de las oficinas, salas e instalaciones	Se debe diseñar y aplicar mecanismos de seguridad física a las salas, oficinas e instalaciones.	PNI
A.11.1.4 Protección contra las amenazas externas y medioambientales	Se debe diseñar y aplicar mecanismos de control contra los desastres naturales, ataques maliciosos o accidentes.	PNI
A.11.1.5 Trabajo en áreas seguras	Se debe diseñar y aplicar procedimientos para el trabajo en áreas seguras.	PNI
A.11.1.6 Distribución de las zonas de carga	Los puntos de acceso, tales como las zonas de distribución y carga y otros puntos por los que podría ingresar personal no autorizado a las instalaciones deben ser controlados, y en la medida de lo posible, alejados de las instalaciones de procesamiento de la información para evitar el acceso no autorizado.	PNI
A.11.2 Equipos		
Objetivo: Evitar la pérdida, daño, robo o actos en los que se comprometan activos y la interrupción de las operaciones de la organización.		
A.11.2.1 Ubicación y protección de los equipos	Los equipos deben ser ubicados y protegidos de tal forma que se reduzcan los riesgos como resultado de las amenazas y los peligros del medio ambiente, y las oportunidades de acceso no autorizado.	PNI
A.11.2.2 Servicios públicos de soporte	Los equipos deben ser protegidos contra las fallas de energía y otras alteraciones causadas por las fallas en los servicios públicos de soporte.	DD
A.11.2.3 Seguridad en el cableado	Se debe proteger de cualquier interferencia, intercepción o daño al cableado de energía o telecomunicaciones que transfiere datos o que sirve de apoyo en los servicios de información.	PNI

Continuación Tabla 5

A.11.2.4 Mantenimiento de los equipos	Se debe mantener de manera correcta el mantenimiento de los equipos para garantizar su disponibilidad e integridad continuas.	D
A.11.2.5 Retiro de los activos	El equipo, la información o el software no puede ser retirado de su lugar sin una previa autorización	PNI
A.11.2.6 Seguridad de los equipos y bienes fuera de las instalaciones	Se debe aplicar medidas de seguridad para los activos utilizados fuera de las instalaciones, tomando en cuéntalos diferentes riesgos de trabajar fuera de las instalaciones de la organización.	PNI
A.11.2.7 Disposición o re-uso seguro de los equipos	Todos los equipos que contienen medios de comunicación de la información deben ser revisados para garantizar que se haya extraído o que se haya sobre-escrito la información sensible y la licencia del software antes de desechar o re-usar el mismo.	PNI
A.11.2.8 Usuario de equipo abandonado (desatendido)	Los usuarios deben garantizar una adecuada protección a los equipos abandonados	DD
A.11.2.9 Política de escritorio y pantallas limpias	Se debe adoptar la política de escritorio limpio de papeles y de medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de la información.	PNI
A.12 Seguridad de las operaciones		
A.12.1 Procedimientos y responsabilidades operaciones		
A.12.1.1 Documentación de los procedimientos operacionales	Se debe documentar los procesos operacionales y ponerse a disposición de todos los usuarios que lo necesiten.	PNI
A.12.1.2 Cambios en la gerencia	Se debe mantener un control sobre los cambios en la organización, el negocio y los sistemas que afectan la seguridad de la información	PNI
A.12.1.3 Gestión de la capacidad	Debe ser monitoreado y mejorado el uso de recursos, así como las proyecciones hechas sobre los requisitos de capacidad del futuro, para garantiza el desempeño del sistema.	PNI
A.12.1.4 Separación de ambientes de desarrollo, prueba y de operaciones	Se debe separar los ambientes de desarrollo, prueba y operaciones para reducir los riesgos de acceso o cambios no autorizados dentro de ambiente de operaciones.	PNI
A.12.2 Protección contra el malware (programa malicioso)		
Objetivo: Garantizar que la información y las instalaciones de procesamiento de la información estén protegidos contra el malware		
A.12.2.1 Controles contra el malware	Se debe implementar mecanismos de control para la detección, prevención y recuperación, para proteger a la información contra el malware, junto con una concientización adecuada al usuario.	DD
A.12.3 Backup		
Objetivo: Proteger la información contra la pérdida		
A.12.3.1 Backup de la información	Se debe tomar y poner a prueba de manera regular, el back up de copias de la información, software e imágenes del sistema, de acuerdo a la política de back up de la organización.	D
A.12.4 Logeo y monitoreo		
Objetivo: Registrar eventos y generar evidencias		
A.12.4.1 Eventos de logeo	Se debe llevar a cabo y verificar regularmente eventos de logeo que registren las actividades, excepciones, faltas y cualquier evento de seguridad de la información.	PNI

Continuación Tabla 5

A.12.4.2 Protección de la información del logeo	Se debe proteger contra la falsificación y el acceso no autorizado a los medios de logeo y a la información del logeo	PNI
A.12.4.3 Logeo del administrador y operador	Debe logearse las actividades del sistema del administrador y del operador, y los logs deben ser protegidos y revisados de manera regular.	PNI
A.12.4.4 Sincronización de los relojes	Se debe sincronizar a una sola fuente de tiempo de referencia, los relojes de todos los sistemas de procesamiento de la información correspondientes dentro de la organización o del dominio de seguridad.	PNI
A.12.5 Control del software operacional		
Objetivo: Garantizar la integridad de los sistemas operacionales		
A.12.5.1 Instalación del software en los sistemas operacionales	Se debe implementar procedimientos para controlar la instalación del software en los sistemas operacionales	D
A.12.6 Gestión de las vulnerabilidades técnicas		
Objetivo: Evitar la explotación de las vulnerabilidades técnicas		
A.12.6.1 Gestión de las vulnerabilidades técnicas	Se debe obtener, de manera oportuna, información sobre las vulnerabilidades técnicas de los sistemas de la información a ser utilizados; evaluar la exposición de la organización a dichas vulnerabilidades y tomar las medidas adecuadas para manejar los riesgos asociados.	PNI
A.12.6.2 Restricciones en la instalación de software	Se debe establecer e implementar las reglas que gobiernen la instalación de los softwares.	D
A.12.7 Consideraciones de las auditorías sobre los sistemas de información		
Objetivo: Minimizar el impacto de las actividades de las auditorías en los sistemas operacionales		
A.12.7.1 Controles de la auditoría sobre los sistemas de información	Se debe planificar cuidadosamente los requisitos y actividades de la auditoría que involucren la verificación de los sistemas operacionales; y acordar minimizar las alteraciones a los procesos del negocio	PNI
A.13 Seguridad de las comunicaciones		
A.13.1 Gestión de la seguridad de las redes		
Objetivo: Garantizar la protección de la información en las redes y de sus instalaciones de procesamiento de la información		
A.13.1.1 Controles en las redes	Se debe administrar y controlar las redes para proteger la información de los sistemas y las aplicaciones	DD
A.13.1.2 Seguridad de los servicios de las redes	Se debe identificar los mecanismos de seguridad, los niveles del servicio y los requisitos de todos los servicios de redes e incluirlos en los acuerdos de servicios de redes, ya sea que los servicios sean proporcionados por la misma organización o por un tercero.	DD
A.13.1.3 Segregación en las redes	Se debe segregar grupos de servicios de información, usuarios y sistemas de información	PNI

Continuación Tabla 5

A.13.2. Transferencia de la información		
Objetivo: Mantener la seguridad de la información transferida dentro de la organización y con cualquier entidad externa		
A.13.2.1 Políticas y procedimientos de la transferencia de la información	Se debe dar lugar a las políticas, procedimientos y controles formales de transferencia a través del uso de todo tipo de equipos de comunicación	PNI
A.13.2.2 Acuerdos sobre la transferencias de la información	Los acuerdos deberán señalar la transferencia segura de la información del negocio entre la organización y terceros.	PNI
A.13.2.3 Mensajes electrónicos	Se debe proteger adecuadamente la información enviada mediante mensajes electrónicos.	PNI
A.13.2.4 Confidencialidad o acuerdos no divulgados	Se debe identificar, revisar regularmente y documentar los requisitos para la confidencialidad o acuerdos no divulgados que reflejan las necesidades de la organización sobre la protección de la información.	PNI
A.14 Adquisición, desarrollo y mantenimiento del sistema		
A.14.1 Requisitos de seguridad de los sistemas de información		
Objetivo: Garantizar que la seguridad de la información forme parte integral de los sistemas de información a lo largo de todo el ciclo de vida. Esto incluye también los requisitos del sistema de la información que proveen servicios mediante las redes públicas.		
A.14.1.1 Análisis y especificaciones de los requisitos de la seguridad de la información	Se debe incluir la seguridad de la información relacionada a los requisitos en los requerimientos de nuevos sistemas de información o en el mejoramiento de los sistemas de información existentes.	DD
A.14.1.2 Seguridad de los servicios de aplicación en las redes públicas	Se debe proteger la información que pasa a través de las redes públicas de las actividades fraudulentas, controversias contractuales y divulgación y modificaciones no autorizadas.	DD
A.14.1.3 Protección de las transacciones de los servicios de aplicación	Se debe proteger la información que provenga de las transacciones de los servicios de aplicación, para evitar las transmisiones incompletas, desvíos, duplicado o reproducción no autorizados de mensajes.	D
A.14.2 Seguridad en los procesos del programa de desarrollo y soporte		
Objetivo: Garantizar que se diseñe e implemente la seguridad de la información dentro del ciclo del programa de desarrollo de los sistemas de la información		
A.14.2.1 Política del programa de desarrollo seguro	Se debe establecer y aplicar reglas de desarrollo de software y sistemas a los programas de desarrollo dentro de la organización.	PNI
A.14.2.2 Procedimiento de control de los cambios de sistemas	Se debe controlar los cambios dentro del ciclo de vida de los programas de desarrollo, mediante el uso de procedimientos formales de control de cambios.	DD
A.14.2.3 Revisión técnica de las aplicaciones luego de los cambios de la plataforma operacional	Luego del cambio de las plataformas operacionales, se debe revisar y verificar las aplicaciones críticas del negocio, para garantizar que no haya un impacto adverso sobre las operaciones o la seguridad organizacional.	DD
A.14.2.4 Restricciones a los cambios de los paquetes de software	No se facilitará la modificación de los paquetes de sistemas; por el contrario, se les limitará a los cambios necesarios y todos los cambios deberán ser estrictamente controlados.	DD
A.14.2.5 Principios del sistema de seguridad para la ingeniería	Se debe establecer, documentar, mantener y aplicar los principios de sistemas de seguridad para la ingeniería, a todos los esfuerzos de implementación del sistema.	DD

Continuación Tabla 5

A.14.2.6 Ambiente seguro del programa de desarrollo	Las organizaciones deben establecer y proteger adecuadamente los ambientes seguros de desarrollo de los sistemas de desarrollo y la integración de los esfuerzos a lo largo del ciclo de vida del programa de desarrollo del sistema.	DD
A.14.2.7 Programa de desarrollo subcontratado	La organización debe supervisar y monitorear las actividades de desarrollo del sistema del ente subcontratado.	DD
A.14.2.8 Revisión de la seguridad del sistema	Se debe llevar a cabo revisiones de la funcionalidad de la seguridad durante el desarrollo	DD
A.14.2.9 Revisión de la aceptación del sistema	Se debe establecer programas de verificación de la aceptación y de los criterios relacionados con respecto a los nuevos sistemas de información, renovaciones y nuevas versiones.	DD
A .14.3 Datos de prueba		
Objetivo: garantizar la protección de los datos utilizados para la verificación		
A.14.3.1 Protección de los datos de prueba	Los datos de prueba deben ser seleccionados, protegidos y controlados cuidadosamente.	PNI
A.15 Relación con los proveedores		
A.15.1 Seguridad de la información en las relaciones con los proveedores		
Objetivo: Garantizar la protección de los activos de la información a los que los proveedores tiene acceso		
A.15.1.1 Política de seguridad de la información sobre las relaciones con los proveedores	Se debe acordar y documentar los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso de los proveedores a los activos de la organización.	D
A.15.1.2 Consideración de la seguridad en los acuerdos con los proveedores	Se debe establecer y acordar todos los requisitos relacionados a la seguridad de la información con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proveer con elementos de infraestructura tecnológica, información de la organización.	D
A.15.1.3 Cadena de suministro de tecnología de la información y comunicación	Los acuerdos con los proveedores deben incluir los requisitos para el manejo de los riesgos de seguridad de la información relacionados a los servicios de tecnología de la información y la comunicación y a la cadena de suministro del producto.	D
A.15.2 Gestión de la prestación del servicio por parte del proveedor		
Objetivo: Mantener un nivel acordado de seguridad de la información y de la prestación del servicio alineado a los acuerdos del proveedor		
A.15.2.1 Monitoreo y revisión del servicio de los proveedores	Las organizaciones deben monitorear, revisar y auditar regularmente la prestación de servicios del proveedor.	D
A.15.2.2 Cambios en la gestión del servicio de los proveedores	Se debe gestionar los cambios a la provisión de los servicios prestados por los proveedores, incluyendo el mantenimiento y la mejora de políticas, procedimientos y controles de la seguridad de la información, tomando en cuenta la sensibilidad de la información del negocio, los sistemas y los procesos involucrados así como la re-evaluación de los riesgos.	D

Continuación Tabla 5

A.16 Gestión de los incidentes de seguridad de la información		
A.16.1 Gestión de los incidentes de la seguridad de la información y la mejora		
Objetivo: Garantizar una aproximación consistente y efectiva a la gestión de los incidentes de seguridad de la información, incluyendo la comunicación sobre los eventos y debilidades de la seguridad		
A.16.1.1 Responsabilidades y procedimientos	Se debe establecer responsabilidades de la gerencia y procedimientos para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información	PNI
A.16.1.2 Reporte de los eventos de seguridad de la información	Se debe reportar los eventos de seguridad de la información a través de canales adecuados lo más pronto posible.	PNI
A.16.1.3 Reporte de las debilidades de la seguridad de la información	Se debe instar a los trabajadores y contratistas que hagan uso de los sistemas de información de la organización, a tomar nota e informar acerca de cualquier debilidad que se observe o sospeche con respecto a los sistemas o servicios del sistema de seguridad de la información.	PNI
A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de la información	Se debe evaluar los eventos de seguridad de la información; y tomar una decisión sobre si deben ser clasificados como incidentes de la seguridad de la información.	PNI
A.16.1.5 Respuesta a los incidentes de seguridad de la información	Se debe responder a los incidentes de seguridad de la información de acuerdo a los procedimientos documentados.	PNI
A.16.1.6 Aprendizaje de los incidentes de seguridad de la información	Se debe usar el conocimiento obtenido del análisis y resolución de los incidentes de la seguridad de la información, con la finalidad de reducir la probabilidad o impacto de futuros incidentes.	PNI
A.16.1.7 Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y conservación de la información que puede servir como evidencia.	PNI
A.17 Gestión de los aspectos de la seguridad de la información para la continuidad del negocio		
A.17.1 Continuidad de la seguridad de la información		
Objetivo: La continuidad de la seguridad de la información debe estar incrustada en los sistemas de gestión de la continuidad del negocio de la organización		
A.17.1.1 Continuidad de los planes de seguridad de la información	La organización debe determinar sus requisitos para la seguridad de la información y para la continuidad de la gestión de seguridad de la información en situaciones adversas, e.g. durante una crisis o desastre.	D
A.17.1.2 Implementación de la continuidad de la seguridad de la información	La organización deberá establecer, documentar, implementar y mantener los procesos, procedimientos y controles para garantizar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.	D
A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debe verificar los controles de la continuidad de la seguridad de la información establecidos e implementados, a intervalos regulares con la finalidad de asegurar la su validez y efectividad durante situaciones adversa.	D

Continuación Tabla 5

A.17.2 Redundancias		
Objetivo: Garantizar la disponibilidad de las instalaciones de procesamiento de la información		
A.17.2.1 Disponibilidad de instalaciones de procesamiento de la información	Se debe implementar las instalaciones de procesamiento de la información con una capacidad adicional suficiente para cumplir con los requisitos de disponibilidad.	D
A.18 Cumplimiento		
A.18.1 Cumplimiento de los requisitos legales y contractuales		
Objetivo: Evitar el incumplimiento de las obligaciones legales, regulatorias o contractuales relacionadas a la seguridad de la información y al cualquier requisito de seguridad		
A.18.1.1 Identificación de la ley aplicable y de los requisitos contractuales	Se debe identificar de manera explícita, documentar y mantener actualizados todos los requisitos legislativos regulatorios y contractuales así como el enfoque de la organización para cumplir con estos requisitos, con respecto a cada sistema de información y a la organización.	DD
A.18.1.2 Derechos de propiedad intelectuales	Se debe implementar procedimientos adecuados para garantizar el cumplimiento de los requisitos legislativos, regulatorios y contractuales relacionados a los derecho de propiedad intelectuales y al uso de productos registrados de software.	D
A.18.1.3 Protección de los registros	Los registros deben ser protegidos contra la pérdida, destrucción, falsificación, acceso no autorizado y lanzamiento no autorizado, de acuerdo a los requisitos legales, regulatorios, contractuales y del mismo negocio.	DD
A.18.1.4 Privacidad y protección de la información que permite identificar a las personas	Se debe garantizar la privacidad y la protección de la información que permita identificar a las personas de acuerdo a lo requerido en la legislación y las regulaciones pertinentes, si fuera aplicable.	DD
A.18.1.5 Regulación de los controles criptográficos	Se debe hacer uso de controles criptográficos en cumplimiento con los acuerdos, las leyes y las regulaciones correspondientes.	PNI
A.18.2 Revisiones de la seguridad de la información		
Objetivo: Garantizar que la seguridad de a información sea implementada y operada de acuerdo a las políticas y procedimientos organizacionales		
A.18.2.1 Revisión independiente de la seguridad de la información	Se debe revisar, a intervalos planificados o cuando ocurre algún cambio significativo,, el enfoque de la organización para gestionar la seguridad de la información y su implementación (i.e. objetivos de control, controles, políticas, procesos y procedimientos de la seguridad de la información).	PNI
A.18.2.2 Cumplimiento de las políticas y normas de seguridad de la información	Los gerentes deben revisar regularmente el cumplimiento de los procedimientos y del procesamiento de la información dentro de su área de responsabilidad, de acuerdo a las políticas, normas de seguridad adecuadas y a los otros requisitos de seguridad.	PNI
A.18.2.3 Revisión del cumplimiento técnico	Se debe revisar regularmente los sistemas de la información con respecto al cumplimiento de las políticas y normas de seguridad de la información de la organización.	D

De igual manera se obtuvieron los siguientes resultados como se observan en los siguientes gráficos y tablas:

Figura 3.30 ISO 27001: Anexo A – Estado de cumplimiento en cantidad

Figura 3.31 ISO 27001: Anexo A – Estado de cumplimiento en porcentaje

El 24% de los controles están documentados. El 24% de los controles se llevan a cabo y el proceso necesita ser documentado para asegurar el proceso y mitigar los riegos. El 52% de los controles no están implementados.

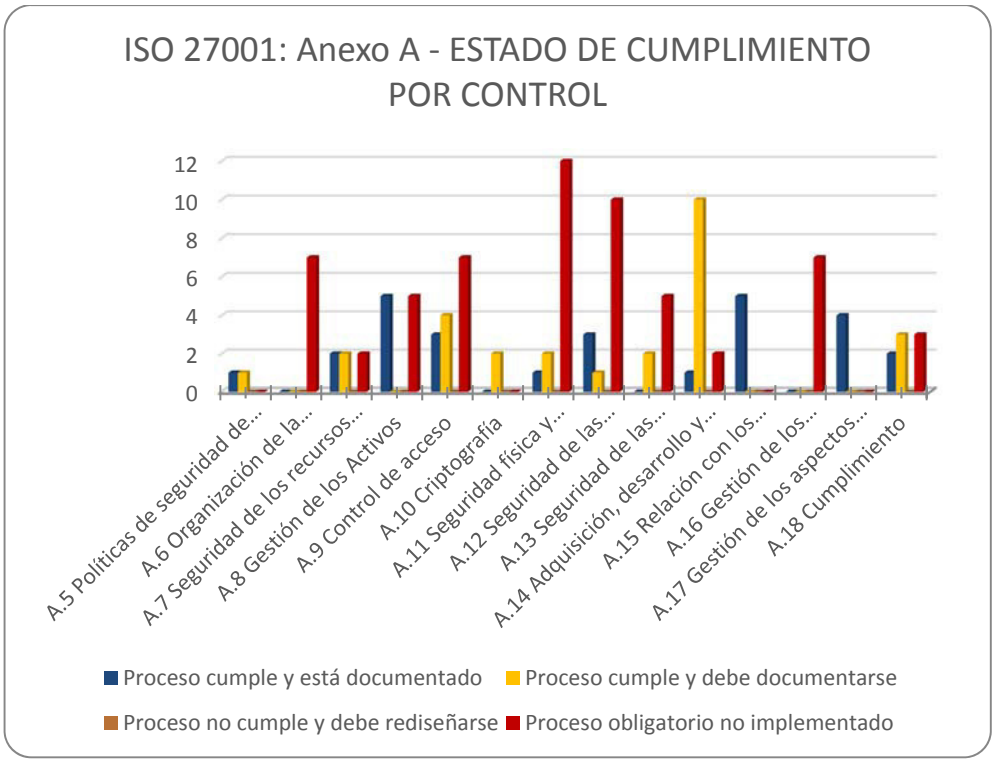

Figura 3.32 ISO 27001: Anexo A – Estado de cumplimiento por control.

Tabla 6. Resultados obtenidos Anexo A ISO/IEC 27001:2013

Anexo A	Proceso cumple y está documentado	Proceso cumple y debe documentarse	Proceso no cumple y debe rediseñarse	Proceso obligatorio no implementado	TOTAL
A.5 Políticas de seguridad de la información	1	1	0	0	2
A.6 Organización de la seguridad de la información	0	0	0	7	7
A.7 Seguridad de los recursos humanos	2	2	0	2	6
A.8 Gestión de los Activos	5	0	0	5	10
A.9 Control de acceso	3	4	0	7	14
A.10 Criptografía	0	2	0	0	2
A.11 Seguridad física y medioambiental	1	2	0	12	15
A.12 Seguridad de las operaciones	3	1	0	10	14
A.13 Seguridad de las comunicaciones	0	2	0	5	7
A.14 Adquisición, desarrollo y mantenimiento del sistema	1	10	0	2	13
A.15 Relación con los proveedores	5	0	0	0	5
A.16 Gestión de los incidentes de seguridad de la información	0	0	0	7	7
A.17 Gestión de los aspectos de la seguridad de la información para la continuidad del negocio	4	0	0	0	4
A.18 Cumplimiento	2	3	0	3	8
TOTAL	27	27	0	60	114

RESULTADOS

De lo expuesto anteriormente se puede ver claramente del análisis en ISO 27001:2013, que no existe ningún procedimiento relacionado con el contexto de la organización, evaluación del desempeño y mejora. Si bien es cierto se cuenta con un adecuado inventario de activos y se tiene un reglamento interno para la asignación de funciones y responsabilidad en cuanto a los procesos y controles, no se cuenta con planes de auditoría interna en relación con la seguridad de la información ni políticas de seguridad.

En cuanto al soporte se encontró que el departamento de TIC del GAD de Samborondón se ha esforzado por tener el personal idóneo a nivel técnico capaz de resolver los problemas que se encuentran. No se cuenta con un área designada para evaluar y gestionar los riesgos asociados.

Con relación a los controles del Anexo A de la ISO 27002:2013 de puede evidenciar claramente que la organización de la seguridad de la información y la gestión de los incidentes de seguridad de la información no son prioridad para la organización y se realiza lo mínimo para su funcionamiento. Si bien es cierto se cuenta con un contrato de INFRAESTRUCTURA de IAAS DATA CENTER VIRTUAL PARA ACCESO A TRAVÉS DEL INTERNET (CLOUD COMPUTING) con el proveedor Telconet S.A. dentro del cual se encuentran

la mayoría de los servidores de aplicaciones y bases de datos; lo cual garantiza el cumplimiento de la Norma ISO 27001 por ser Telconet S.A. una empresa oficialmente certificada por parte de la empresa certificadora Societé Générale de Surveillance – SGS del Ecuador, todavía se cuenta con servidores que no están dentro de este contrato como es el caso del servidor físico donde se encuentra implementado el Sistema de Información Geográfica del GAD Samborondón. Con respecto a la seguridad ligada al acceso físico no autorizado y daño e interferencia a la información se evidenció el desconocimiento de los controles relacionados a las áreas seguras y acceso a los equipos críticos.

Se anexa archivo con el detalle del SERVICIO DE INFRAESTRUCTURA DE IAAS DATA CENTAR VIRTUAL POR EL PERÍODO DE 15 MESES PARA ACCESO A TRAVÉS DEL INTERNET (CLOUD COMPUTING) - CONTRATO NO. 057-SIE-GADMCS-2018

CAPÍTULO 4

ANÁLISIS DE RIESGOS DEL PROCESO DE INFORMACIÓN GEOGRÁFICA

No se puede proteger aquello que no se conoce, por lo cual para lograr la planificación de la implementación de un esquema de seguridad basada en la norma ISO 27001:2013, para el proceso de administración del sistema de información geográfica en el gobierno autónomo descentralizado del cantón Samborondón es necesario realizar la evaluación de los activos, realizando una valoración de los mismos con el propósito de identificar los diferentes riesgos a los que se encuentra expuesta la organización desde el punto de vista de la seguridad y que podrían afectar al desarrollo de las diferentes actividades, de la

misma manera permitirá realizar una selección de medidas de seguridad a ser implementadas.

Para realizar el análisis de riesgos del proceso de administración del sistema de información geográfica del GAD Samborondón se utilizará la metodología MAGERIT, según la misma el análisis de riesgos es una aproximación metódica para determinar el riesgo, que se ha convertido en una herramienta para lograr estrategias, lineamientos de detección y protección de los activos de la organización.

4.1 Definición de los activos

Se define como activos a todos los bienes tangibles e intangibles que la organización necesite y tenga para su correcto funcionamiento; según la Norma española UNE 71504:2008, un activo es “componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización” Los activos pueden ser: talento humano, recursos administrativos, comunicaciones, hardware, software, información, datos, servicios. [10]

A continuación se detallan los activos de información involucrados:

Tabla 7. Identificación de activos de información

N°	Activo	Tipo de activo
1	Servidores	Hardware
2	Computadores/Laptos	Hardware
3	Impresoras	Hardware
4	GPS	Hardware
5	Tablets	Hardware
6	Cámaras fotográficas	Hardware
7	Servidores virtuales (proveedor externo)	Hardware
8	Sistema de vigilancia - CCTV	Hardware
9	Red de área local e inalámbrica	Comunicaciones
10	Documentos físicos	Datos/Soportes de información
11	Datos e información	Datos/Soportes de información
12	Personal Administrativo	Persona
13	Personal Técnico	Persona
14	Página Web	Servicio
15	Servicio de correo electrónico	Servicio
16	Base de datos	Software/Información
17	Base de datos GIS	Software/Información
18	Software / aplicaciones GIS	Software/Información
19	Software/aplicaciones propias del GAD	Software/Información
20	Sofware de digitalización de documentos	Software/Información
21	Sofware/Antivirus	Software/Información
22	Software /Sistema de vigilancia	Software/Información

A continuación se detallan los activos del Sistema de Información Geográfica involucrados:

Tabla 8. Identificación de activos del Sistema de Información Geográfica

N°	Activo	Tipo de activo
1	Servidores	Hardware
2	Computadores/Laptos	Hardware
3	Impresoras	Hardware
4	GPS	Hardware
9	Red de área local e inalámbrica	Comunicaciones
10	Documentos físicos	Datos/Soportes de información
11	Datos e información	Datos/Soportes de información
12	Personal Administrativo	Persona
13	Personal Técnico	Persona
14	Página Web	Servicio
15	Base de datos GIS	Software/Información
16	Software / aplicaciones GIS	Software/Información

En cuanto a la valoración de los activos nos permite conocer el nivel de protección requerido en base al impacto que tendría para la organización al no cumplir con las normas estándares de disponibilidad, integridad y confidencialidad; bajo esta premisa si el impacto para la organización es alto, el valor del activo deberá también ser alto.

El valor del activo es calculado en base a la afectación de la Disponibilidad, Integridad y Confidencialidad para cuyo efecto se usa la fórmula siguiente:

$$(4.1) \quad VA = (d + i + c) / 3$$

VA = Valor del activo

d = disponibilidad

i = integridad

c = confidencialidad

De la misma manera para valorar la afectación a la disponibilidad, integridad y confidencialidad se utilizará la escala de Likert, descrita a continuación:

Tabla 9. Escala de Likert

1	2	3	4	5
Muy bajo	Bajo	Medio	Alto	Muy alto

A continuación se muestra la tabla de valoración de los activos de información involucrados:

Tabla 10. Valoración de activos

Ámbito	Activo	D	I	C	VA
Hardware	Servidores	5	5	5	5.00
	Computadores/Laptos	4	4	3	3.67
	Impresoras	3	4	4	3.67
	GPS	3	5	4	4.00
	Tablets	4	5	5	4.67
	Cámaras fotográficas	4	5	5	4.67
	Servidores virtuales (proveedor externo)	5	5	5	5.00
	Sistema de vigilancia - CCTV	5	5	5	5.00
Comunicaciones	Red de área local e inalámbrica	5	5	5	5.00
Datos/Soportes de información	Documentos físicos	4	5	5	4.67
	Datos e información	5	5	5	5.00
Persona	Personal Administrativo	4	5	4	4.33
	Personal Técnico	4	5	5	4.67
Servicio	Página Web	5	5	4	4.67
	Servicio de correo electrónico	5	5	4	4.67
Software/Información	Base de datos	5	5	5	5.00
	Base de datos GIS	5	5	5	5.00
	Software / aplicaciones GIS	5	5	5	5.00
	Software/aplicaciones propias del GAD	5	5	5	5.00
	Sofware de digitalización de documentos	4	5	4	4.33
	Sofware/Antivirus	5	5	4	4.67
	Software /Sistema de vigilancia	5	5	5	5.00

A continuación se muestra la tabla de valoración de los activos del Sistema de Información Geográfica Involucrados:

Tabla 11. Valoración de activos del Sistema de Información Geográfica

Ámbito	Activo	D	I	C	VA
Hardware	Servidores	5	5	5	5.00
	Computadores/Laptos	4	4	3	3.67
	Impresoras	3	4	4	3.67
	GPS	3	5	4	4.00
Comunicaciones	Red de área local e inalámbrica	5	5	5	5.00
Datos/Soportes de información	Documentos físicos	4	5	5	4.67
	Datos e información	5	5	5	5.00
Persona	Personal Administrativo	4	5	4	4.33
	Personal Técnico	4	5	5	4.67
Servicio	Página Web	5	5	4	4.67
Software/Información	Base de datos GIS	5	5	5	5.00
	Software / aplicaciones GIS	5	5	5	5.00

4.2 Amenazas y vulnerabilidades de los activos del Sistema de Información Geográfica

Las amenazas están relacionadas con la posibilidad de que algún tipo de evento pueda presentarse en cualquier momento, dentro del cual exista un daño tangible o intangible sobre los activos informáticos involucrados en el proceso de administración del Sistema de Información Geográfica, también son conocidas como ataques realizados por personas internas o externas a la organización que pueden ocasionar daños a la infraestructura tecnológica, sistemas de información o información involucrados dentro del proceso de administración del Sistema de Información Geográfica del GAD. Debido a que la Seguridad Informática tiene como propósitos de garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los datos e información, las amenazas y los consecuentes daños que puede causar un evento exitoso, también hay que ver en relación con la confidencialidad, integridad, disponibilidad y autenticidad de los datos e información. [11]

Las vulnerabilidades son las posibilidades que se dan en el entorno, dentro del cual las características propician y se vuelven susceptibles a una amenaza. La vulnerabilidad se puede dar en cualquier evento sin importar su naturaleza interna o externa que pueda afectar los activos involucrados, los

datos o la información ante un ataque deliberado o accidental ya sea por individuos dentro o fuera de la organización.

Las vulnerabilidades están en directa interrelación con las amenazas porque si no existe una amenaza tampoco existe una vulnerabilidad o no tiene importancia, poner no se puede ocasionar un daño. [11]

La identificación de las amenazas potenciales a las que puede estar expuesta la organización va a ayudar y facilitar la identificación de las vulnerabilidades que afectan cada activo, lo cual permitirá tomar medidas eficaces para mitigar, minimizar o contrarrestar los riesgos.

Para el proceso de administración del Sistema de Información Geográfica del GAD municipal del cantón Samborondón se han identificado las amenazas de acuerdo a la siguiente clasificación: Accidentales, Ambientales y Deliberadas para de esta manera facilitar la ubicación.

Amenazas Accidentales: Causadas por personas dentro de la organización que por accidente hacen mal uso de los sistemas informáticos y de la información causando daños.

Amenazas Ambientales: Causadas por la naturaleza ya sean terremotos, incendios forestales, inundaciones que causen daño a los activos involucrados

Amenazas Deliberadas: Causadas por el personal interno y externo de la organización que deliberadamente hacen mal uso o abuso de los sistemas informáticos e información, personas que atacan los sistemas informáticos con fines políticos, para obtener beneficios económicos, lucro personal o simplemente para causar daño.

Dimensiones de valoración de los Activos

Las dimensiones de valoración ayudan a describir las cualidades más importantes de cada activo, y deben ser identificados por cada activo crítico:

Disponibilidad: Describe cuando y con qué frecuencia debe estar presente un activo para su uso.

Integridad: Describe autenticidad, exactitud, características que se les da a los activos de información para que no sean alterados de forma no autorizada.

Confidencialidad: Describe la necesidad de mantener la información privada e inaccesible para cualquier persona no autorizada para verla.

Nomenclaturas:

AC: Accidental; AM: Ambiental; DE: Deliberado; D: Disponibilidad; I: Integridad; C: Confidencialidad; S: Servicios; SW: Software; HW: Hardware; SI: Soportes de Información; P: Personas

Tabla 12. Identificación de amenazas

GRUPO N°		AMENAZAS	DIMENSIONES			TIPO DE ACTIVOS				
			D	I	C	S	SW	HW	SI	P
ACC	1	Amenaza física	X	X	X	X	X	X	X	X
	2	Ataque destructivo	X	X	X	X	X	X	X	X
	3	Avería de orígen físico o lógico	X			X	X	X	X	
	4	Caídas del sistema por agotamiento de recursos	X			X	X	X		
	5	Contaminación electromagnética	X			X		X		
	6	Corte del Suministro eléctrico	X			X		X		
	7	Daños por agua	X	X		X	X	X	X	X
	8	Deficiencias en la organización	X	X	X	X				X
	9	Degradación de los soportes de almacenamiento de la información	X	X					X	
	10	Destrucción de la información	X	X	X	X			X	
	11	Deterioro físico en el equipo	X					X		
	12	Difusión de software dañino	X	X	X	X	X		X	
	13	Error de hardware	X			X	X	X	X	
	14	Errores de configuración	X				X	X		
	15	Errores de los usuarios	X				X	X		
	16	Errores de mantenimiento	X			X		X		
	17	Fallo de servicios de comunicaciones	X			X	X	X	X	
	18	Fuego	X	X	X	X	X	X	X	X
	19	Indisponibilidad del personal	X							X
	20	Robo	X	X	X			X	X	X
AM	1	Daños por agua	X	X		X	X	X	X	X
	2	Desastres naturales	X	X	X	X	X	X	X	X
	3	Fuego	X	X	X	X	X	X	X	X
DE	1	Abuso de privilegos de acceso	X	X		X	X		X	
	2	Acceso no autorizado	X	X	X	X	X	X	X	X
	3	Alteración de la información		X					X	
	4	Amenaza física	X	X	X	X	X	X	X	X
	5	Ataque destructivo	X	X	X	X	X	X	X	X
	6	Avería de orígen físico o lógico	X			X	X			
	7	Caídas del sistema por agotamiento de recursos	X			X	X		X	
	8	Contaminación electromagnética	X			X		X		
	9	Corte del Suministro eléctrico	X			X		X		
	10	Daños por agua	X			X	X	X	X	X
	11	Degradación de los soportes de almacenamiento de la información	X	X	X			X		
	12	Destrucción de la información	X	X	X	X			X	
	13	Deterioro físico en el equipo	X					X		
	14	Difusión de software dañino	X			X	X			
	15	Divulgación de información		X	X				X	
	16	Errores de configuración	X			X	X	X		
	17	Errores de los usuarios	X	X	X	X	X	X	X	X
	19	Errores de mantenimiento	X			X		X		
	20	Errores del administrador	X			X	X	X	X	
	21	Escapes de información		X	X				X	
	22	Fallo de servicios de comunicaciones	X			X	X	X	X	
	23	Fuego	X	X	X	X	X	X	X	X
	24	Indisponibilidad del personal	X							X
	25	Ingeniería social		X	X				X	X
	26	Manipulación de la configuración	X	X	X	X	X	X		X
	27	Modificación de la información			X				X	
	28	Robo	X	X	X			X	X	X
	29	Suplantación de la identidad del usuario	X	X	X	X	X	X	X	X
	30	Vulnerabilidades de los programas		X	X	X		X	X	

Una vez identificadas las distintas amenazas que pueden afectar a cada activo, es necesario evaluar su probabilidad de ocurrencia en la cual se utilizará la escala de Likert descrita anteriormente.

Tabla 13. Probabilidad de amenazas

GRUPO	NOM	AMENAZAS	PROBABILIDAD				
			MB	B	M	A	MA
ACC	1	Amenaza física			3		
	2	Ataque destructivo			3		
	3	Avería de orígen físico o lógico				4	
	4	Caídas del sistema por agotamiento de recursos		2			
	5	Contaminación electromagnética		2			
	6	Corte del Suministro eléctrico			3		
	7	Daños por agua				4	
	8	Deficiencias en la organización				4	
	9	Degradación de los soportes de almacenamiento de la información			3		
	10	Destrucción de la información		2			
	11	Deterioro físico en el equipo				4	
	12	Difusión de software dañino					5
	13	Error de hardware			3		
	14	Errores de configuración		2			
	15	Errores de los usuarios			3		
	16	Errores de mantenimiento	1				
	17	Fallo de servicios de comunicaciones				4	
	18	Fuego			3		
	19	Indisponibilidad del personal			3		
	20	Robo				4	
AM	1	Daños por agua				4	
	2	Desastres naturales			3		
	3	Fuego			3		
DE	1	Abuso de privilegos de acceso			3		
	2	Acceso no autorizado					5
	3	Alteración de la información				4	
	4	Amenaza física			3		
	5	Ataque destructivo			3		
	6	Avería de orígen físico o lógico				4	
	7	Caídas del sistema por agotamiento de recursos		2			
	8	Contaminación electromagnética		2			
	9	Corte del Suministro eléctrico			3		
	10	Daños por agua				4	
	11	Degradación de los soportes de almacenamiento de la información			3		
	12	Destrucción de la información		2			
	13	Deterioro físico en el equipo				4	
	14	Difusión de software dañino					5
	15	Divulgación de información				4	
	16	Errores de configuración		2			
	18	Errores de los usuarios			3		
	19	Errores de mantenimiento	1				
	20	Errores del administrador		2			
	21	Escapes de información				4	
	22	Fallo de servicios de comunicaciones				4	
	23	Fuego			3		
	24	Indisponibilidad del personal			3		
	25	Ingeniería social			3		
	26	Manipulación de la configuración				4	
	27	Modificación de la información				4	
	28	Robo				4	
	29	Suplantación de la identidad del usuario				4	
	30	Vulnerabilidades de los programas				4	

En cuanto a lo que corresponde a las vulnerabilidades, se puede decir que son debilidades de seguridad que están asociadas con los activos de información de la organización, son condiciones que pueden hacer que una amenaza afecte a un activo.

Pueden clasificarse de la siguiente manera:

Seguridad Física y ambiental: Control de acceso físico inadecuado a las instalaciones de la organización, infraestructura no apropiada y poco segura, oficinas desprotegidas, deterioro de los equipos, susceptibilidad de equipos a variaciones de voltaje, etc.

Seguridad del talento humano: Falta de entrenamiento en seguridad, falta de mecanismos de monitoreo, carencia de políticas para el uso correcto de los equipos y sistemas, falta de procedimientos para entrega de activos, funcionarios no motivados, indisponibilidad del personal, etc.

Control de acceso: Segregación inapropiada de redes, falta de políticas de contraseñas, política incorrecta para control de acceso, falta de protección a equipos de comunicación móvil, acceso no autorizado, destrucción de la información, abusos de privilegios de acceso, etc.

Gestión de operaciones y comunicación: Poca o ninguna protección a equipos de comunicación, gestión de red inadecuada, falta de protección en redes públicas de conexión, control de cambio inadecuado, escapes de información, errores de configuración, etc.

Mantenimiento, desarrollo y adquisición de sistemas: Protección inapropiada de llaves criptográficas, vulnerabilidades de los programas, difusión de software dañino, robo, etc.

En la tablas 12 a la 23 se muestran los activos con sus respectivas amenazas y vulnerabilidades identificadas.

Tabla 14. Amenazas y vulnerabilidades Servidor GIS

Activo	Amenaza	Vulnerabilidad
Servidor GIS	Fuego	Edificación no apropiada y poco segura
	Daños por agua	Edificación no apropiada y poco segura
	Desastres natuales	Edificación no apropiada y poco segura
	Avería de orígen físico o lógico	Mantenimiento no adecuado de equipos
	Errores de mantenimiento	Mantenimiento no adecuado de equipos
	Acceso no autorizado	Puertas traseras activas no detectadas
	Deficiencias en la organización	Evaluación poco cuidadosa de la fuerza de trabajo
	Caídas del sistema por agotamiento de recursos	Cálculo no adecuado de consumo de energía
	Escapes de información	Falta de políticas de seguridad, acuerdos de confidencialidad
	Divulgación de información	Falta de políticas de seguridad, acuerdos de confidencialidad
	Deterioro físico en el equipo	Mantenimiento no adecuado de equipos
	Manipulación de la configuración	Deficiente administración de usuarios y permisos
	Suplantación de la identidad del usuario	Ausencia de políticas de contraseñas
	Abuso de privilegos de acceso	Deficiente administración de usuarios y permisos
	Difusión de software dañino	Poco conocimiento de reglamento interno
	Modificación de la información	Mala administración de accesos físicos y lógicos
	Robo	Escasa administración y monitoreo de recursos
	Ataque destructivo	Mala administración de accesos físicos y lógicos

Tabla 15. Amenazas y vulnerabilidades Computadores/Laptops

Activo	Amenaza	Vulnerabilidad
Computadores/Laptos	Fuego	Edificación no apropiada y poco segura
	Daños por agua	Edificación no apropiada y poco segura
	Desastres natuales	Edificación no apropiada y poco segura
	Avería de orígen físico o lógico	Mantenimiento no adecuado de equipos
	Errores de mantenimiento	Mantenimiento no adecuado de equipos
	Acceso no autorizado	Puertas traseras activas no detectadas
	Deficiencias en la organización	Evaluación poco cuidadosa de la fuerza de trabajo
	Caídas del sistema por agotamiento de recursos	Cálculo no adecuado de consumo de energía
	Divulgación de información	Falta de políticas de seguridad, acuerdos de confidencialidad
	Deterioro físico en el equipo	Mantenimiento no adecuado de equipos
	Manipulación de la configuración	Deficiente administración de usuarios y permisos
	Abuso de privilegos de acceso	Deficiente administración de usuarios y permisos
	Difusión de software dañino	Poco conocimiento de reglamento interno
	Modificación de la información	Mala administración de accesos físicos y lógicos

Tabla 16. Amenazas y vulnerabilidades Impresoras

Activo	Amenaza	Vulnerabilidad
Impresoras	Fuego	Edificación no apropiada y poco segura
	Daños por agua	Edificación no apropiada y poco segura
	Desastres natuales	Edificación no apropiada y poco segura
	Errores de mantenimiento	Mantenimiento no adecuado de equipos
	Caídas del sistema por agotamiento de recursos	Cálculo no adecuado de consumo de energía
	Manipulación de la configuración	Deficiente administración de usuarios y permisos

Tabla 17. Amenazas y vulnerabilidades GPS

Activo	Amenaza	Vulnerabilidad
GPS	Daños por agua	Edificación no apropiada y poco segura
	Desastres natuales	Edificación no apropiada y poco segura
	Amenaza física	Edificación no apropiada y poco segura
	Robo	Escasa administración y monitoreo de recursos

Tabla 18. Amenazas y vulnerabilidades Red área local el inalámbrica

Activo	Amenaza	Vulnerabilidad
Red de área local e inalámbrica	Fuego	Edificación no apropiada y poco segura
	Desastres natuales	Edificación no apropiada y poco segura
	Contaminación electromagnética	Líneas de comunicación no protegidas
	Corte del Suministro eléctrico	Fallos de hardware por voltaje inestable
	Fallo de servicios de comunicaciones	Acceso no autorizado a la red
	Errores de configuración	Entrenamiento de seguridad insuficiente
	Escapes de información	Falta de políticas de seguridad, acuerdos de confidencialidad
	Deterioro físico en el equipo	Mantenimiento no adecuado de equipos
	Acceso no autorizado	Puertas traseras activas no detectadas
	Ataque destructivo	Mala administración de accesos físicos y lógicos

Tabla 19. Amenazas y vulnerabilidades Documentos físicos

Activo	Amenaza	Vulnerabilidad
Documentos físicos	Fuego	Edificación no apropiada y poco segura
	Daños por agua	Edificación no apropiada y poco segura
	Desastres natuales	Edificación no apropiada y poco segura
	Destrucción de la información	Corrupción
	Robo	Control de acceso insuficiente en el GAD

Tabla 20. Amenazas y vulnerabilidades Datos e información

Activo	Amenaza	Vulnerabilidad
Datos e información	Fuego	Edificación no apropiada y poco segura
	Daños por agua	Edificación no apropiada y poco segura
	Desastres natuales	Edificación no apropiada y poco segura
	Degradación de los soportes de almacenamiento de la información	Susceptibilidad de daño en almacenamiento de medios
	Errores de los usuarios	Entrenamiento de seguridad insuficiente
	Deficiencias en la organización	Evaluación poco cuidadosa de la fuerza de trabajo
	Alteración de la información	Uso impropio/no controlado
	Destrucción de la información	Corrupción
	Modificación de la información	Mala administración de accesos físicos y lógicos
	Robo	Control de acceso insuficiente en el GAD
	Ataque destructivo	Mala administración de accesos físicos y lógicos
	Ingeniería social	Entrenamiento de seguridad insuficiente

Tabla 21. Amenazas y vulnerabilidades Personal Administrativo

Activo	Amenaza	Vulnerabilidad
Personal Administrativo	Degradación de los soportes de almacenamiento de la información	Susceptibilidad de daño en almacenamiento de medios
	Escapes de información	Falta de políticas de seguridad, acuerdos de confidencialidad
	Alteración de la información	Uso impropio/no controlado
	Destrucción de la información	Corrupción
	Divulgación de información	Falta de políticas de seguridad, acuerdos de confidencialidad
	Indisponibilidad del personal	Ausencia de personal
	Suplantación de la identidad del usuario	Ausencia de políticas de contraseñas
	Difusión de software dañido	Poco conocimiento de reglamento interno
	Modificación de la información	Mala administración de accesos físicos y lógicos
	Robo	Control de acceso insuficiente en el GAD
	Indisponibilidad del personal	Ausencia de personal
	Ingeniería social	Entrenamiento de seguridad insuficiente

Tabla 22. Amenazas y vulnerabilidades Personal Técnico

Activo	Amenaza	Vulnerabilidad
Personal Técnico	Escapes de información	Falta de políticas de seguridad, acuerdos de confidencialidad
	Alteración de la información	Uso impropio/no controlado
	Destrucción de la información	Corrupción
	Divulgación de información	Falta de políticas de seguridad, acuerdos de confidencialidad
	Indisponibilidad del personal	Ausencia de personal
	Suplantación de la identidad del usuario	Ausencia de políticas de contraseñas
	Difusión de software dañido	Poco conocimiento de reglamento interno
	Modificación de la información	Mala administración de accesos físicos y lógicos
	Robo	Control de acceso insuficiente en el GAD
	Indisponibilidad del personal	Ausencia de personal
	Ingeniería social	Entrenamiento de seguridad insuficiente

Tabla 23. Amenazas y vulnerabilidades Página Web

Activo	Amenaza	Vulnerabilidad
Página Web	Vulnerabilidades de los programas	Instalación desinstalación no controlada
	Caídas del sistema por agotamiento de recursos	Cálculo no adecuado de consumo de energía
	Ataque destructivo	Mala administración de accesos físicos y lógicos
	Acceso no autorizado	Puertas traseras activas no detectadas

Tabla 24. Amenazas y vulnerabilidades Base de datos GIS

Activo	Amenaza	Vulnerabilidad
Base de datos GIS	Vulnerabilidades de los programas	Instalación desinstalación no controlada
	Caídas del sistema por agotamiento de recursos	Cálculo no adecuado de consumo de energía
	Ataque destructivo	Mala administración de accesos físicos y lógicos
	Acceso no autorizado	Puertas traseras activas no detectadas
	Errores del administrador	Mantenimiento no adecuado de equipos
	Difusión de software dañido	Poco conocimiento de reglamento interno
	Abuso de privilegos de acceso	Deficiente administración de usuarios y permisos
	Modificación de la información	Mala administración de accesos físicos y lógicos
	Destrucción de información	Corrupción
	Ingeniería social	Entrenamiento de seguridad insuficiente

Tabla 25. Amenazas y vulnerabilidades Software/Información

Activo	Amenaza	Vulnerabilidad
Software/Información	Vulnerabilidades de los programas	Instalación desinstalación no controlada
	Caídas del sistema por agotamiento de recursos	Cálculo no adecuado de consumo de energía
	Ataque destructivo	Mala administración de accesos físicos y lógicos
	Acceso no autorizado	Puertas traseras activas no detectadas
	Errores del administrador	Mantenimiento no adecuado de equipos
	Difusión de software dañido	Poco conocimiento de reglamento interno
	Abuso de privilegos de acceso	Deficiente administración de usuarios y permisos
	Modificación de la información	Mala administración de accesos físicos y lógicos
	Destrucción de información	Corrupción
	Ingeniería social	Entrenamiento de seguridad insuficiente

4.3 Valoración de los riesgos

Los riesgos son problemas potenciales, que pueden afectar a la infraestructura o sistemas de información involucrados en el proceso sino no te tienen las medidas adecuadas para salvaguardar los datos e información, los riesgos pueden presentarse por las vulnerabilidades y amenazas en cualquier momento.

Para realizar la valoración de los riesgos de los activos involucrados en el proceso de administración del Sistema de Información Geográfica del GAD de Samborondón se ha considerado el valor del activo (impacto/afectación en su confidencialidad, disponibilidad e integridad) y la probabilidad de la amenaza.

Riesgo = Valor del activo x Probabilidad

Tabla 26. Valoración de los riesgos en servidor GIS

SERVIDOR GIS			
Amenaza	**VA**	**P**	**Riesgo (VA X P)**
Acceso no autorizado	5	5	25
Difusión de software dañino	5	5	25
Daños por agua	5	4	20
Avería de orígen físico o lógico	5	4	20
Deficiencias en la organización	5	4	20
Escapes de información	5	4	20
Divulgación de información	5	4	20
Deterioro físico en el equipo	5	4	20
Manipulación de la configuración	5	4	20
Suplantación de la identidad del usuario	5	4	20
Modificación de la información	5	4	20
Robo	5	4	20
Fuego	5	3	15
Desastres natuales	5	3	15
Abuso de privilegos de acceso	5	3	15
Ataque destructivo	5	3	15
Caídas del sistema por agotamiento de recursos	5	2	10
Errores de mantenimiento	5	1	5

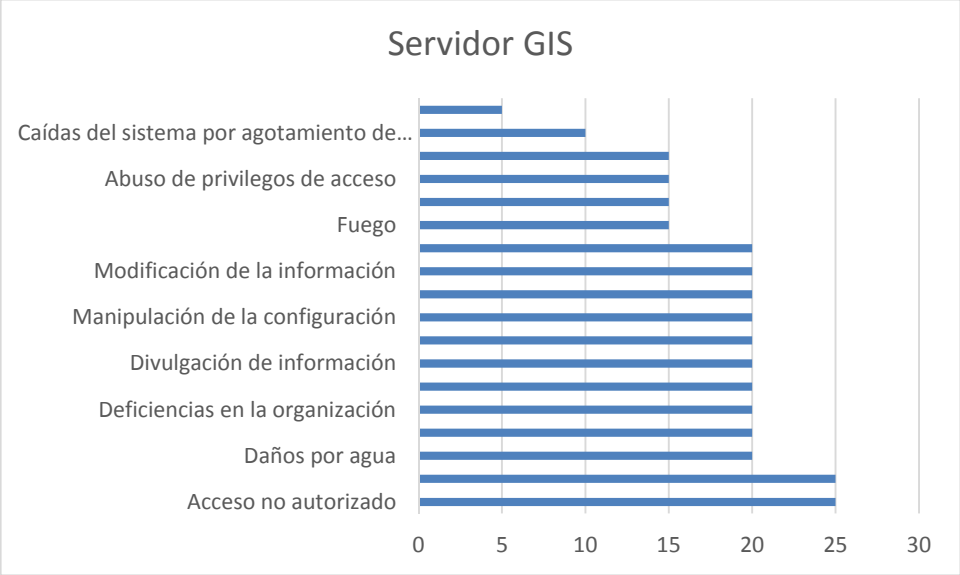

Figura 4.1 Riesgos en Servidor GIS

Tabla 27. Valoración de los riesgos en computadores/laptops

COMPUTADORES/LAPTOPS			
Amenaza	**VA**	**P**	**Riesgo (VA X P)**
Acceso no autorizado	3.67	5	18.35
Difusión de software dañino	3.67	5	18.35
Daños por agua	3.67	4	14.68
Avería de orígen físico o lógico	3.67	4	14.68
Deficiencias en la organización	3.67	4	14.68
Divulgación de información	3.67	4	14.68
Deterioro físico en el equipo	3.67	4	14.68
Manipulación de la configuración	3.67	4	14.68
Modificación de la información	3.67	4	14.68
Fuego	3.67	3	11.01
Desastres natuales	3.67	3	11.01
Abuso de privilegos de acceso	3.67	3	11.01
Caídas del sistema por agotamiento de recursos	3.67	2	7.34
Errores de mantenimiento	3.67	1	3.67

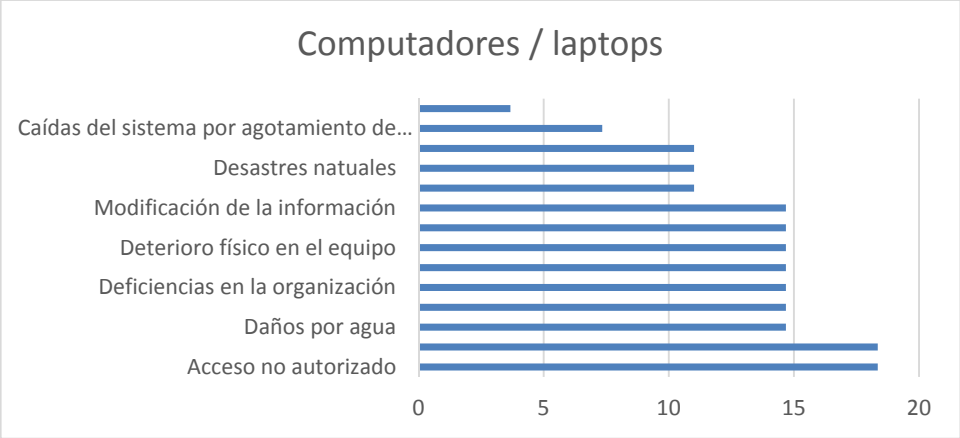

Figura 4.2 Riesgos en Servidor computadores/laptops

Tabla 28. Valoración de los riesgos en impresoras

IMPRESORAS			
Amenaza	**VA**	**P**	**Riesgo (VA X P)**
Daños por agua	3.67	4	14.68
Manipulación de la configuración	3.67	4	14.68
Fuego	3.67	3	11.01
Desastres natuales	3.67	3	11.01
Caídas del sistema por agotamiento de recursos	3.67	2	7.34
Errores de mantenimiento	3.67	1	3.67

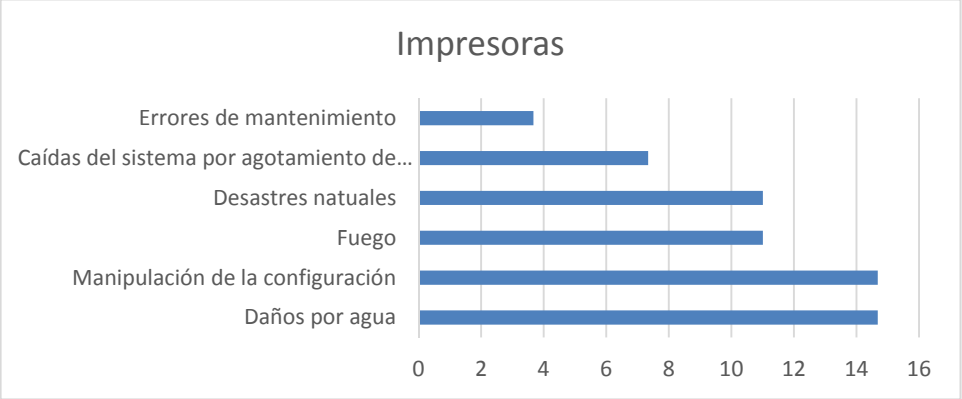

Figura 4.3 Riesgos en impresoras

Tabla 29. Valoración de los riesgos en GPS

GPS			
Amenaza	**VA**	**P**	**Riesgo (VA X P)**
Daños por agua	4	4	16
Robo	4	4	16
Desastres natuales	4	3	12
Amenaza física	4	3	12

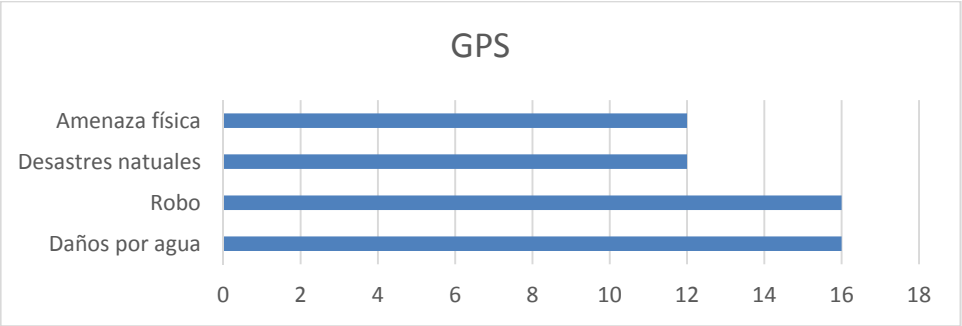

Figura 4.4 Riesgos en GPS

Tabla 30. Valoración de los riesgos en red local e inalámbrica

RED DE ÁREA LOCAL E INALÁMBRICA			
Amenaza	**VA**	**P**	**Riesgo (VA X P)**
Acceso no autorizado	5	5	25
Fallo de servicios de comunicaciones	5	4	20
Escapes de información	5	4	20
Deterioro físico en el equipo	5	4	20
Fuego	5	3	15
Desastres natuales	5	3	15
Corte del Suministro eléctrico	5	3	15
Ataque destructivo	5	3	15
Contaminación electromagnética	5	2	10
Errores de configuración	5	2	10

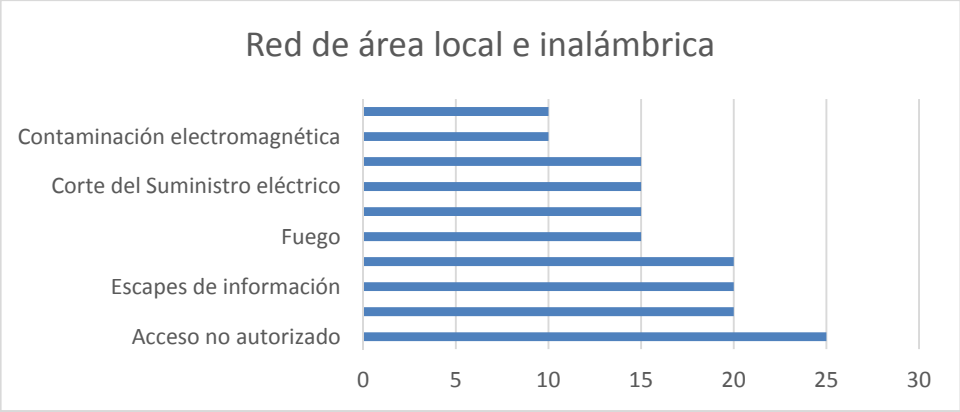

Figura 4.5 Riesgos en red de área local e inalámbrica

Tabla 31. Valoración de los riesgos en documentos físicos

DOCUMENTOS FÍSICOS			
Amenaza	**VA**	**P**	**Riesgo (VA X P)**
Daños por agua	4	4	16
Robo	4	4	16
Fuego	4	3	12
Desastres natuales	4	3	12
Destrucción de la información	4	2	8

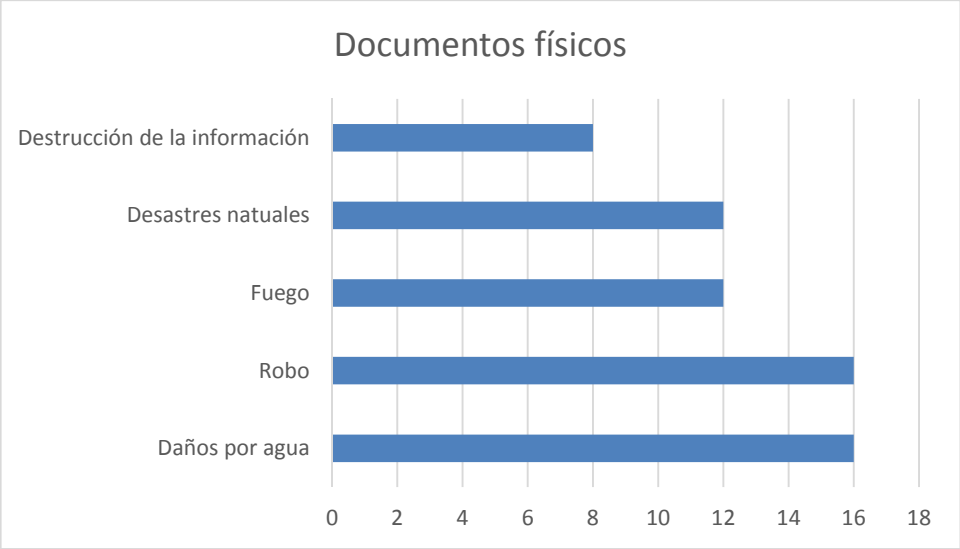

Figura 4.6 Riesgos en documentos físicos

Tabla 32. Valoración de los riesgos en datos e información

DATOS E INFORMACIÓN			
Amenaza	**VA**	**P**	**Riesgo (VA X P)**
Daños por agua	5	4	20
Deficiencias en la organización	5	4	20
Alteración de la información	5	4	20
Modificación de la información	5	4	20
Robo	5	4	20
Fuego	5	3	15
Desastres natuales	5	3	15
Degradación de los soportes de almacenamiento de la información	5	3	15
Errores de los usuarios	5	3	15
Ataque destructivo	5	3	15
Ingeniería social	5	3	15
Destrucción de la información	5	2	10

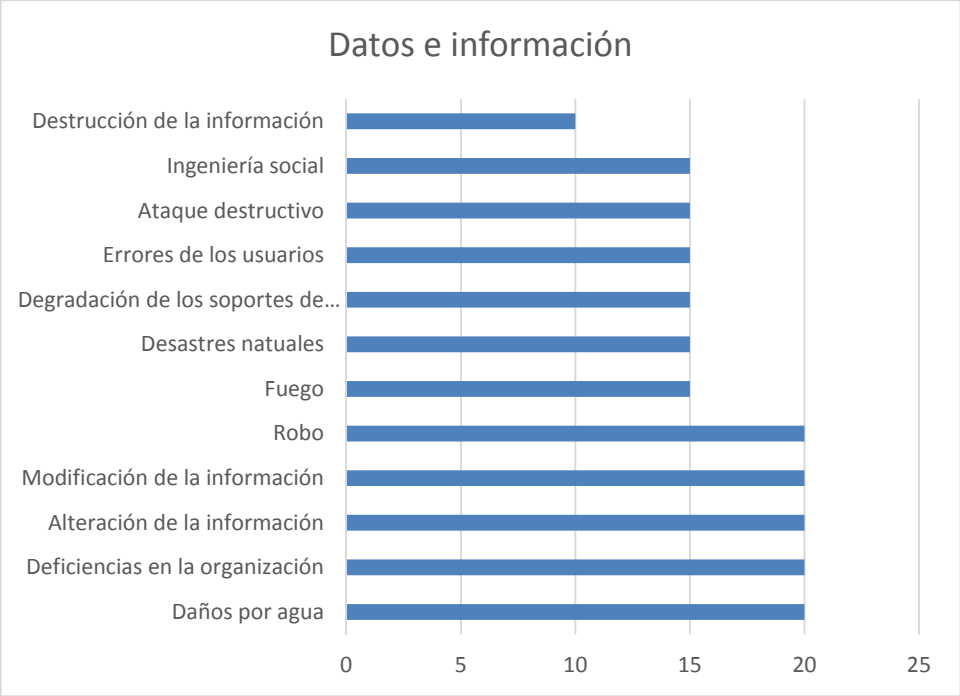

Figura 4.7 Riesgos en datos e información

Tabla 33. Valoración de los riesgos en personal administrativo

PERSONAL ADMINISTRATIVO			
Amenaza	**VA**	**P**	**Riesgo (VA X P)**
Difusión de software dañido	4.33	5	21.65
Escapes de información	4.33	4	17.32
Alteración de la información	4.33	4	17.32
Divulgación de información	4.33	4	17.32
Suplantación de la identidad del usuario	4.33	4	17.32
Modificación de la información	4.33	4	17.32
Robo	4.33	4	17.32
Degradación de los soportes de almacenamiento de la información	4.33	3	12.99
Indisponibilidad del personal	4.33	3	12.99
Indisponibilidad del personal	4.33	3	12.99
Ingeniería social	4.33	3	12.99
Destrucción de la información	4.33	2	8.66

Figura 4.8 Riesgos en personal administrativo

Tabla 34. Valoración de los riesgos en personal técnico

PERSONAL TÉCNICO			
Amenaza	**VA**	**P**	**Riesgo (VA X P)**
Difusión de software dañido	4.67	5	23.35
Escapes de información	4.67	4	18.68
Alteración de la información	4.67	4	18.68
Divulgación de información	4.67	4	18.68
Suplantación de la identidad del usuario	4.67	4	18.68
Modificación de la información	4.67	4	18.68
Robo	4.67	4	18.68
Indisponibilidad del personal	4.67	3	14.01
Indisponibilidad del personal	4.67	3	14.01
Ingeniería social	4.67	3	14.01
Destrucción de la información	4.67	2	9.34

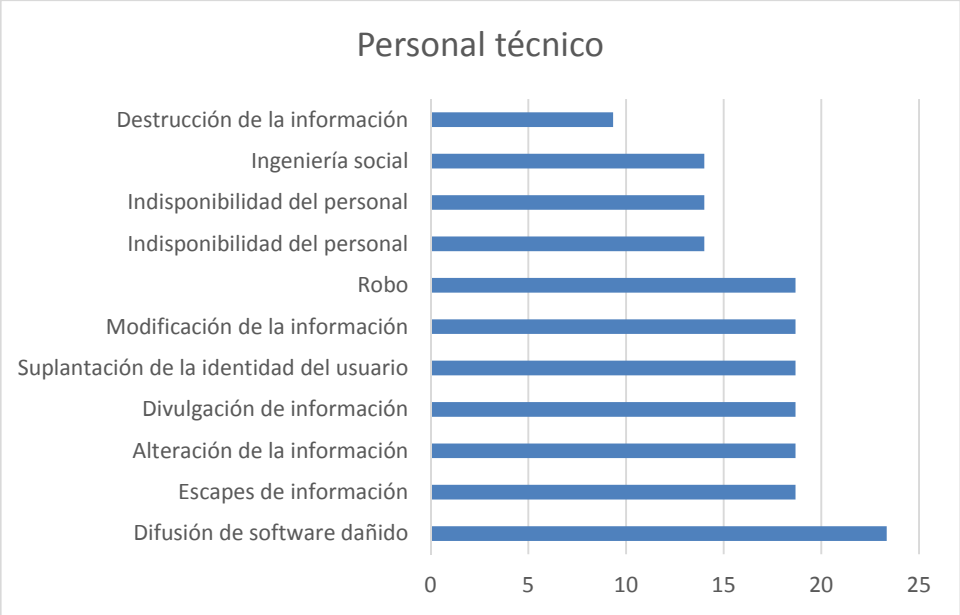

Figura 4.9 Riesgos en personal técnico

Tabla 35. Valoración de los riesgos en página web

PÁGINA WEB			
Amenaza	**VA**	**P**	**Riesgo (VA X P)**
Acceso no autorizado	4.67	5	23.35
Vulnerabilidades de los programas	4.67	4	18.68
Ataque destructivo	4.67	3	14.01
Caídas del sistema por agotamiento de recursos	4.67	2	9.34

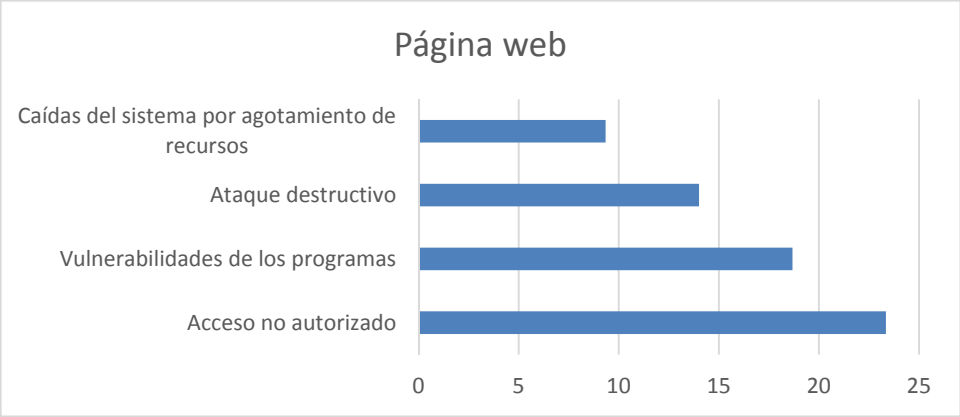

Figura 4.10 Riesgos en página web

Tabla 36. Valoración de los riesgos en base de datos GIS

BASE DE DATOS GIS			
Amenaza	**VA**	**P**	**Riesgo (VA X P)**
Acceso no autorizado	5	5	25
Difusión de software dañido	5	5	25
Vulnerabilidades de los programas	5	4	20
Modificación de la información	5	4	20
Ataque destructivo	5	3	15
Abuso de privilegos de acceso	5	3	15
Ingeniería social	5	3	15
Caídas del sistema por agotamiento de recursos	5	2	10
Errores del administrador	5	2	10
Destrucción de información	5	2	10

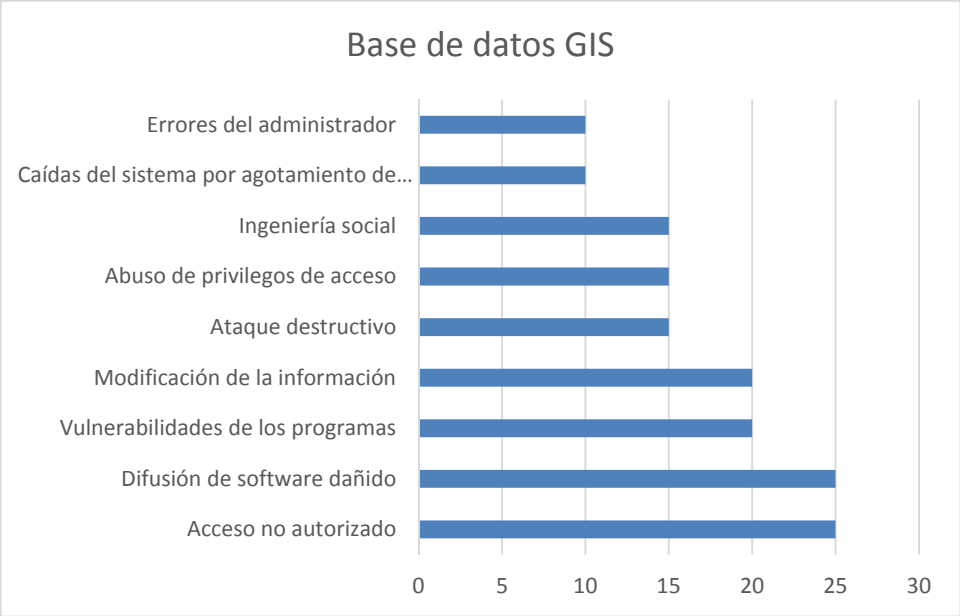

Figura 4.11 Riesgos en base de datos GIS

Tabla 37. Valoración de los riesgos en software/aplicaciones GIS

SOFTWARE / APLICACIONES GIS			
Amenaza	**VA**	**P**	**Riesgo (VA X P)**
Acceso no autorizado	5	5	25
Difusión de software dañido	5	5	25
Vulnerabilidades de los programas	5	4	20
Modificación de la información	5	4	20
Ataque destructivo	5	3	15
Abuso de privilegos de acceso	5	3	15
Ingeniería social	5	3	15
Caídas del sistema por agotamiento de recursos	5	2	10
Errores del administrador	5	2	10
Destrucción de información	5	2	10

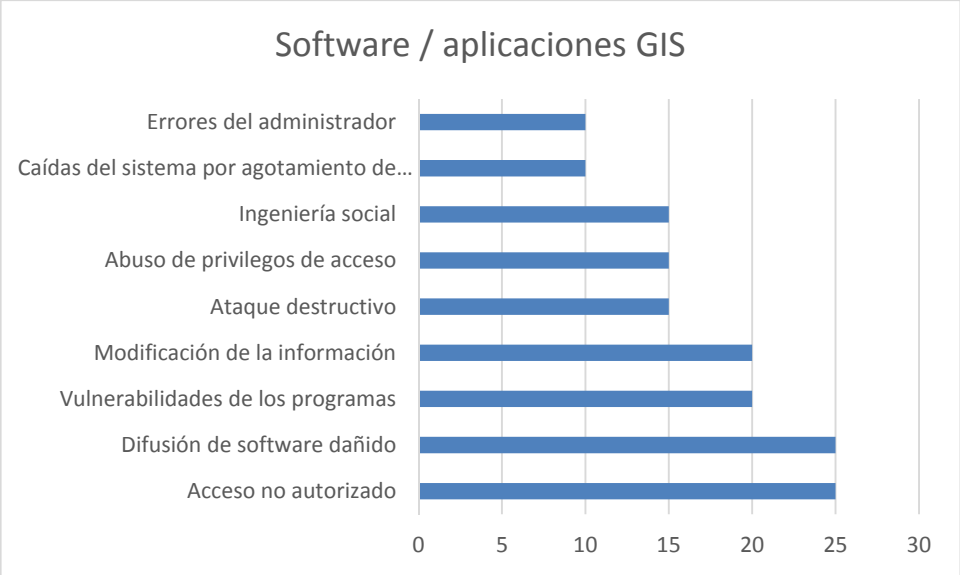

Figura 4.12 Riesgos en software/aplicaciones GIS

4.4 Análisis de riesgos

Una vez realizada la valoración de los riesgos de los activos involucrados en el proceso de administración del Sistema de Información Geográfica del GAD de Samborondón con los datos obtenidos se realizó el cálculo correspondiente para obtener los criterios de aceptación de riesgos para los cual se realizaron las siguientes tablas:

Tabla 38. Exposición al riesgo en valores

Valor Activo						
	Muy alto	5	10	15	20	25
	Alto	4	8	12	16	20
	Medio	3	6	9	12	15
	Bajo	2	4	6	8	10
	Muy bajo	1	2	3	4	5
		Muy bajo	Bajo	Medio	Alto	Muy alto
		Probabilidad				

Tabla 39. Exposición al riesgo en porcentajes

Valor Activo						
	Muy alto	20%	40%	60%	80%	100%
	Alto	16%	32%	48%	64%	80%
	Medio	12%	24%	36%	48%	60%
	Bajo	8%	16%	24%	32%	40%
	Muy bajo	4%	8%	12%	16%	20%
		Muy bajo	Bajo	Medio	Alto	Muy alto
		Probabilidad				

Tabla 40. Criterios de aceptación del riesgo

Niveles de Aceptación del Riesgo		
Exposición al riesgo	**Nivel**	**Objetivo**
64% - 100%	Alto	Aplica controles para llevar al nivel medio
36% - 63.99%	Medio	Aplica controles para llegar al nivel bajo
16% - 35.99%	Bajo	Aplica controles para llegar al nivel leve
4% - 15.99%	Leve	No aplica controles

Tabla 41. Nivel del riesgo por amenaza en Servidor GIS

SERVIDOR GIS					
Amenaza	**VA**	**P**	**Riesgo (VA X P)**	**% de riesgo**	**Nivel**
Acceso no autorizado	5	5	25	100	Alto
Difusión de software dañino	5	5	25	100	Alto
Daños por agua	5	4	20	80	Alto
Avería de orígen físico o lógico	5	4	20	80	Alto
Deficiencias en la organización	5	4	20	80	Alto
Escapes de información	5	4	20	80	Alto
Divulgación de información	5	4	20	80	Alto
Deterioro físico en el equipo	5	4	20	80	Alto
Manipulación de la configuración	5	4	20	80	Alto
Suplantación de la identidad del usuario	5	4	20	80	Alto
Modificación de la información	5	4	20	80	Alto
Robo	5	4	20	80	Alto
Fuego	5	3	15	60	Medio
Desastres natuales	5	3	15	60	Medio
Abuso de privilegos de acceso	5	3	15	60	Medio
Ataque destructivo	5	3	15	60	Medio
Caídas del sistema por agotamiento de recursos	5	2	10	40	Medio
Errores de mantenimiento	5	1	5	20	Medio

Tabla 42. Nivel del riesgo por amenaza en Computadores/Laptops

COMPUTADORES/LAPTOPS					
Amenaza	VA	P	Riesgo (VA X P)	% de riesgo	Nivel
Acceso no autorizado	3.67	5	18.35	73.4	Alto
Difusión de software dañino	3.67	5	18.35	73.4	Alto
Daños por agua	3.67	4	14.68	58.72	Medio
Avería de orígen físico o lógico	3.67	4	14.68	58.72	Medio
Deficiencias en la organización	3.67	4	14.68	58.72	Medio
Divulgación de información	3.67	4	14.68	58.72	Medio
Deterioro físico en el equipo	3.67	4	14.68	58.72	Medio
Manipulación de la configuración	3.67	4	14.68	58.72	Medio
Modificación de la información	3.67	4	14.68	58.72	Medio
Fuego	3.67	3	11.01	44.04	Medio
Desastres natuales	3.67	3	11.01	44.04	Medio
Abuso de privilegos de acceso	3.67	3	11.01	44.04	Medio
Caídas del sistema por agotamiento de recursos	3.67	2	7.34	29.36	Bajo
Errores de mantenimiento	3.67	1	3.67	14.68	Leve

Tabla 43. Nivel del riesgo por amenaza en Impresoras

IMPRESORAS					
Amenaza	VA	P	Riesgo (VA X P)	% de riesgo	Nivel
Daños por agua	3.67	4	14.68	58.72	Medio
Manipulación de la configuración	3.67	4	14.68	58.72	Medio
Fuego	3.67	3	11.01	44.04	Medio
Desastres natuales	3.67	3	11.01	44.04	Medio
Caídas del sistema por agotamiento de recursos	3.67	2	7.34	29.36	Bajo
Errores de mantenimiento	3.67	1	3.67	14.68	Leve

Tabla 44. Nivel del riesgo por amenaza en GPS

GPS					
Amenaza	VA	P	Riesgo (VA X P)	% de riesgo	Nivel
Daños por agua	4	4	16	64	Alto
Robo	4	4	16	64	Alto
Desastres natuales	4	3	12	48	Medio
Amenaza física	4	3	12	48	Medio

Tabla 45. Nivel del riesgo por amenaza en red de área local e inalámbrica

RED DE ÁREA LOCAL E INALÁMBRICA					
Amenaza	VA	P	Riesgo (VA X P)	% de riesgo	Nivel
Acceso no autorizado	5	5	25	100	Alto
Fallo de servicios de comunicaciones	5	4	20	80	Alto
Escapes de información	5	4	20	80	Alto
Deterioro físico en el equipo	5	4	20	80	Alto
Fuego	5	3	15	60	Medio
Desastres natuales	5	3	15	60	Medio
Corte del Suministro eléctrico	5	3	15	60	Medio
Ataque destructivo	5	3	15	60	Medio
Contaminación electromagnética	5	2	10	40	Medio
Errores de configuración	5	2	10	40	Medio

Tabla 46. Nivel del riesgo por amenaza en documentos físicos

DOCUMENTOS FÍSICOS					
Amenaza	VA	P	Riesgo (VA X P)	% de riesgo	Nivel
Daños por agua	4	4	16	64	Alto
Robo	4	4	16	64	Alto
Fuego	4	3	12	48	Medio
Desastres natuales	4	3	12	48	Medio
Destrucción de la información	4	2	8	32	Bajo

Tabla 47. Nivel del riesgo por amenaza en datos e información

DATOS E INFORMACIÓN					
Amenaza	VA	P	Riesgo (VA X P)	% de riesgo	Nivel
Daños por agua	5	4	20	80	Alto
Deficiencias en la organización	5	4	20	80	Alto
Alteración de la información	5	4	20	80	Alto
Modificación de la información	5	4	20	80	Alto
Robo	5	4	20	80	Alto
Fuego	5	3	15	60	Medio
Desastres natuales	5	3	15	60	Medio
Degradación de los soportes de almacenamiento de la información	5	3	15	60	Medio
Errores de los usuarios	5	3	15	60	Medio
Ataque destructivo	5	3	15	60	Medio
Ingeniería social	5	3	15	60	Medio
Destrucción de la información	5	2	10	40	Medio

Tabla 48. Nivel del riesgo por amenaza en personal administrativo

PERSONAL ADMINISTRATIVO					
Amenaza	VA	P	Riesgo (VA X P)	% de riesgo	Nivel
Difusión de software dañido	4.33	5	21.65	86.6	Alto
Escapes de información	4.33	4	17.32	69.28	Alto
Alteración de la información	4.33	4	17.32	69.28	Alto
Divulgación de información	4.33	4	17.32	69.28	Alto
Suplantación de la identidad del usuario	4.33	4	17.32	69.28	Alto
Modificación de la información	4.33	4	17.32	69.28	Alto
Robo	4.33	4	17.32	69.28	Alto
Degradación de los soportes de almacenamiento de la información	4.33	3	12.99	51.96	Medio
Indisponibilidad del personal	4.33	3	12.99	51.96	Medio
Indisponibilidad del personal	4.33	3	12.99	51.96	Medio
Ingeniería social	4.33	3	12.99	51.96	Medio
Destrucción de la información	4.33	2	8.66	34.64	Bajo

Tabla 49. Nivel del riesgo por amenaza en personal técnico

PERSONAL TÉCNICO					
Amenaza	VA	P	Riesgo (VA X P)	% de riesgo	Nivel
Difusión de software dañido	4.67	5	23.35	93.4	Alto
Escapes de información	4.67	4	18.68	74.72	Alto
Alteración de la información	4.67	4	18.68	74.72	Alto
Divulgación de información	4.67	4	18.68	74.72	Alto
Suplantación de la identidad del usuario	4.67	4	18.68	74.72	Alto
Modificación de la información	4.67	4	18.68	74.72	Alto
Robo	4.67	4	18.68	74.72	Alto
Indisponibilidad del personal	4.67	3	14.01	56.04	Medio
Indisponibilidad del personal	4.67	3	14.01	56.04	Medio
Ingeniería social	4.67	3	14.01	56.04	Medio
Destrucción de la información	4.67	2	9.34	37.36	Medio

Tabla 50. Nivel del riesgo por amenaza en página web

PÁGINA WEB					
Amenaza	VA	P	Riesgo (VA X P)	% de riesgo	Nivel
Acceso no autorizado	4.67	5	23.35	93.4	Alto
Vulnerabilidades de los programas	4.67	4	18.68	74.72	Alto
Ataque destructivo	4.67	3	14.01	56.04	Medio
Caídas del sistema por agotamiento de recursos	4.67	2	9.34	37.36	Medio

Tabla 51. Nivel del riesgo por amenaza en base de datos GIS

BASE DE DATOS GIS					
Amenaza	VA	P	Riesgo (VA X P)	% de riesgo	Nivel
Acceso no autorizado	5	5	25	100	Alto
Difusión de software dañido	5	5	25	100	Alto
Vulnerabilidades de los programas	5	4	20	80	Alto
Modificación de la información	5	4	20	80	Alto
Ataque destructivo	5	3	15	60	Medio
Abuso de privilegos de acceso	5	3	15	60	Medio
Ingeniería social	5	3	15	60	Medio
Caídas del sistema por agotamiento de recursos	5	2	10	40	Medio
Errores del administrador	5	2	10	40	Medio
Destrucción de información	5	2	10	40	Medio

Tabla 52. Nivel del riesgo por amenaza en software/aplicaciones GIS

SOFTWARE / APLICACIONES GIS					
Amenaza	VA	P	Riesgo (VA X P)	% de riesgo	Nivel
Acceso no autorizado	5	5	25	100	Alto
Difusión de software dañido	5	5	25	100	Alto
Vulnerabilidades de los programas	5	4	20	80	Alto
Modificación de la información	5	4	20	80	Alto
Ataque destructivo	5	3	15	60	Medio
Abuso de privilegos de acceso	5	3	15	60	Medio
Ingeniería social	5	3	15	60	Medio
Caídas del sistema por agotamiento de recursos	5	2	10	40	Medio
Errores del administrador	5	2	10	40	Medio
Destrucción de información	5	2	10	40	Medio

Los activos involucrados dentro de proceso de administración del Sistema de Información Geográfica del GAD cantonal de Samborondón están en alto riesgo de accesos no autorizados, alteración de la información, difusión de software dañino, fugas y escapes de la información, fallo en el servicio de comunicaciones, robo, suplantación de identidad de los usuarios.

Se recomienda realizar un plan de tratamiento de riesgos, así como un plan de acción sobre cómo implementar los diversos controles definidos por la Declaración de Aplicabilidad.

También se sugiere establecer procedimientos, políticas y controles que protejan la información, procedimientos para la manipulación de la misma de manera que se proteja de accesos no autorizados o uso indebido.

En cuanto a la documentación es importante que estén protegidos contra pérdida, destrucción o actos mal intencionados.

Es necesario implementar controles de detección, prevención y recuperación que sirvan como protección contra códigos maliciosos e implementar procedimientos adecuados de concientización de los usuarios.

En lo relacionado a los riesgos medios y bajos, es necesario iniciar de forma gradual acciones para reducirlos tomando como base los siguientes controles del Anexo A de la ISO 27001:2013.

A.6 Organización de la seguridad de la información

A.7.1.2 Términos y condiciones del empleo

A.7.3.1 Término o cambio de responsabilidades de empleo

A.8.2.1 Clasificación de la información

A.8.2.2 Etiquetado de la información

A.8.3 Manejo de los medios de comunicación

A.9.2 Gestión del acceso al usuario

A.9.4.4 Uso de programas utilitarios de privilegio

A.9.4.5 Control del acceso para programar el código fuente

A.11 Seguridad física y medioambiental

A.11.2.1 Ubicación y protección de los equipos

A.11.2.3 Seguridad en el cableado

A.11.2.5 Retiro de los activos

A.11.2.6 Seguridad de los equipos y bienes fuera de las instalaciones

A.11.2.7 Disposición o re-uso seguro de los equipos

A.11.2.9 Política de escritorio y pantallas limpias

A.12 Seguridad de las operaciones

A.12.4 Logeo y monitoreo

A.12.6.1 Gestión de las vulnerabilidades técnicas

A.12.7.1 Controles de la auditoría sobre los sistemas de información

A.13.1.3 Segregación en las redes

A.13.2. Transferencia de la información

A.14.2.1 Política del programa de desarrollo seguro

A.14.3.1 Protección de los datos de prueba

A.16.1 Gestión de los incidentes de la seguridad de la información y la mejora

A.18.1.5 Regulación de los controles criptográficos

A.18.2.1 Revisión independiente de la seguridad de la información

A.18.2.2 Cumplimiento de las políticas y normas de seguridad de la información.

CAPÍTULO 5

PLANIFICACIÓN E IMPLEMENTACIÓN DEL ESQUEMA DE SEGURIDAD

5.1 Acciones de tratamiento de riesgos

Una vez realizado el análisis de los riesgos es necesario desarrollar el plan de tratamiento de riesgos, que consiste en la selección y aplicación adecuada de los controles, con el fin de poder modificar el riesgo, para evitar de este modo los daños a los que estaría expuesta la organización.

Cualquier sistema de tratamiento de riesgos debe garantizar como mínimo:

- Un funcionamiento efectivo y eficiente de la organización

- Controles internos efectivos

- Conformidad con las leyes y reglamentos vigentes

Las acciones que se tomen para modificar, reducir o eliminar el riesgo contribuirán para mejorar el correcto desempeño de la organización.

Existen dos principales estrategias para el tratamiento de riesgos: Estrategia de evitación y estrategia de minimización.

Estrategia de evitación: Se trata de minimizar la probabilidad de que el riesgo se presente. Para lo cual se manejan cuatro opciones: transferencia, reducción, elusión y diversificación.

Estrategia de minimización: Se trata de reducir el impacto del riesgo, estas estrategias se plantean cuando han fallado las estrategias de evitación y por lo tanto el riesgo pasa a ser un hecho.

En cuanto a las cuatro opciones manejadas dentro de la “estrategia de la evitación” para prevenir que los riesgos pasen a ser una realidad negativa para la organización se detallan y explican a continuación:

Transferencia:

Es el conjunto de procedimientos que tienen como objetivo eliminar el riesgo transfiriéndolo de un lugar a otro. Lo cual puede consistir en vender un activo dudoso, asegurar una actividad con importantes riesgos.

Reducción:

Implica reducir la probabilidad de ocurrencia de un riesgo y/o reducir sus consecuencias implementando controles y procedimientos garantizando que se encuentren en el lugar apropiado. Con el propósito de minimizar cualquier consecuencia adversa.

Elusión:

Eludir conlleva dos opciones, no proceder con el proyecto o actividad que incorporaría el riesgo o escoger medios alternativos para la actividad, que logren el mismo resultado y no incorporen el riesgo detectado.

Diversificación:

Consiste en extender el riesgo desde una determinada área, a otras secciones con la finalidad de impedir la pérdida de ingresos para la organización.

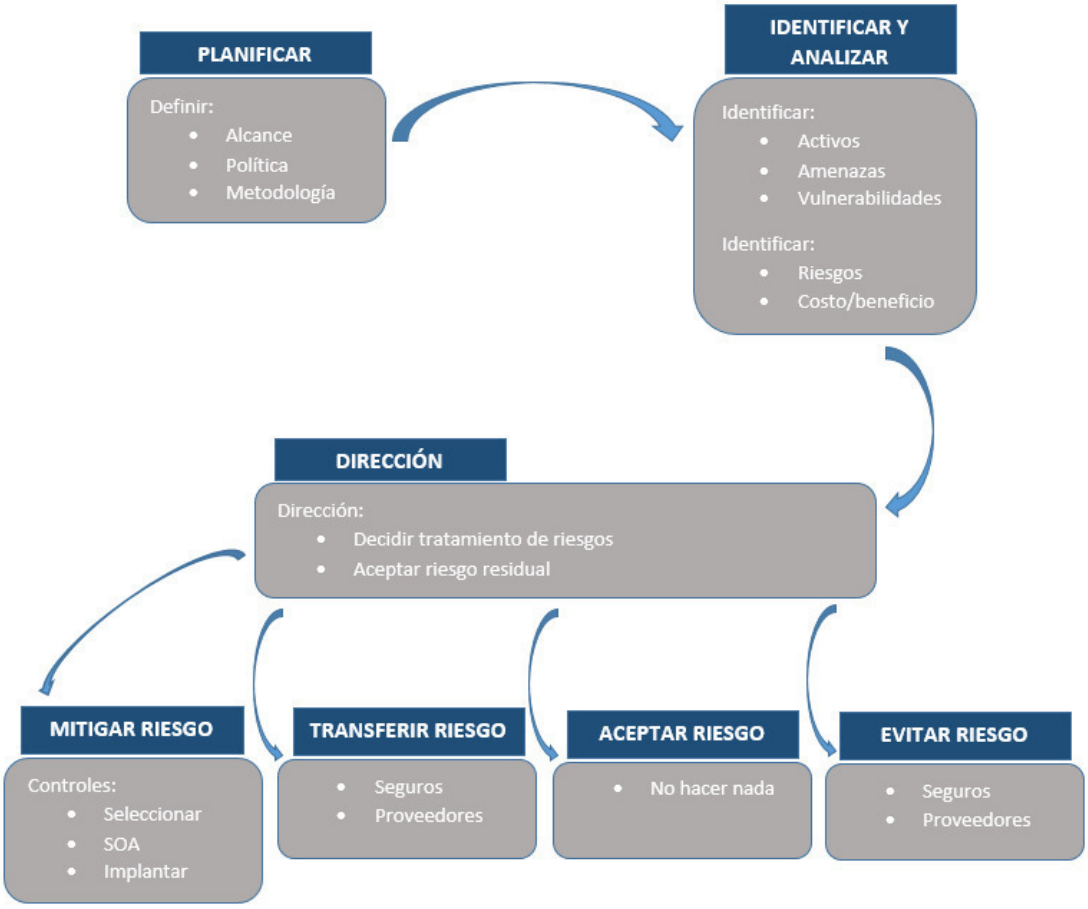

Figura 5.1 Opciones de tratamiento de riesgos

5.2 Reformulación del impacto y sus consecuencias

Usando la información obtenida a lo largo de este documento podemos realizar la reformulación del impacto donde se determinan los efectos adversos resultantes al potencializarse una amenaza y sus consecuencias para el GAD.

A continuación se detalla una breve descripción de cada pilar de seguridad y su impacto respectivo en caso de no cumplirse.

Pérdida de confidencialidad:

Se refiere a la divulgación no autorizada de información de la organización a individuos no autorizados. Este impacto pone en peligro al GAD por no contar con mecanismos seguros de acceso a la información.

Pérdida de disponibilidad:

Si algo crítico de un sistema de información no está disponible para los usuarios finales, el GAD se verá afectado ya que no se podrán realizar consultas y descargas de información del sitio web institucional.

Pérdida de integridad:

La violación de la integridad es el primer paso de un ataque exitoso contra la confidencialidad o disponibilidad del sistema. En caso que la pérdida de la integridad del sistema no sea corregida puede desencadenar en datos dañados, alterados, con errores. Pone en peligro al GAD por no mantener con exactitud a la información y no salvaguardar los sistemas que la generan.

En la siguiente tabla se muestra la magnitud del impacto sobre la vulnerabilidad ejercida y el pilar afectado.

Tabla 53. Magnitud del impacto sobre vulnerabilidad explotada y pilar afectado

Amenaza	Vulnerabilidad	Pilar	Impacto
Acceso no autorizado	Control de acceso insuficiente en el GAD Falta de autenticación en la red Falta de protección física de las puertas en centro de cómputo Falta de mecanismos de monitoreo	Integridad	Alto
Alteración de la información	Contraseñas no protegidas, claves, certificados	Disponibilidad, integridad	Alto
Avería de orígen físico o lógico	Falta de mantenimiento planificado Capacidad inadecuada	Disponibilidad, integridad	Alto
Daños por agua	Desastre natural Área propensa a inundación Desastre provocado por personas	Disponibilidad	Alto
Deficiencias en la organización	Control inadecuado de reclutamiento	Integridad	Alto
Deterioro físico en el equipo	Falta de mantenimiento planificado	Disponibilidad, integridad	Alto
Difusión de software dañino	Susceptibilidad a los ataques internos	Disponibilidad, integridad	Alto
Divulgación de información	Protección inadecuada para acceso público Transferencia de contraseñas	Confidencialidad	Alto
Escapes de información	Protección inadecuada para acceso público Contraseñas no protegidas, claves, certificados	Confidencialidad	Alto
Fallo de servicios de comunicaciones	Inadecuada administración de la red	Disponibilidad	Alto
Manipulación de la configuración	Control de configuración inadecuado	Integridad	Alto
Modificación de la información	Entrenamiento de seguridad insuficiente Control inadecuado de reclutamiento	Confidencialidad, integridad	Alto
Robo	Remoción de equipo para mantenimiento Control de acceso insuficiente en el GAD Trabajo de terceros no supervisado Localización-almacenamiento no protegido Control inadecuado de reclutamiento Falta de protección física de las puertas en centro de cómputo	Disponibilidad	Alto
Suplantación de la identidad del usuario	Administración deficiente de contraseñas Transferencia de contraseñas	Confidencialidad, integridad	Alto
Vulnerabilidades de los programas	Instalación desinstalación no controlada Uso no controlado	Disponibilidad, integridad	Alto
Abuso de privilegos de acceso	Uso impropio/no controlado Falta de autenticación en la red	Integridad	Medio
Amenaza física	Control de acceso insuficiente en el GAD Desastre provocado por personas	Integridad	Medio
Ataque destructivo	Falta de protección contra virus y código malicioso Falta de autenticación en la red	Disponibilidad, integridad	Medio
Avería de orígen físico o lógico	Uso incorrecto de hardware y software	Disponibilidad, integridad	Medio
Caídas del sistema por agotamiento de recursos	Falta de mecanismos de monitoreo Inadecuada administración de la red	Disponibilidad	Medio
Contaminación electromagnética	Susceptibilidad a la radiación electromagnética	Disponibilidad	Medio
Corte del Suministro eléctrico	Líneas de comunicación no protegidas	Disponibilidad	Medio
Degradación de los soportes de almacenamiento de la información	Degradación del hardware	Confidencialidad, integridad	Medio
Desastres naturales	Desastre natural	Disponibilidad	Medio
Destrucción de la información	Susceptibilidad de daño en almacenamiento de medios	Integridad	Medio
Errores de configuración	Control de configuración inadecuado	Integridad	Medio
Errores de los usuarios	Control inadecuado de reclutamiento	Integridad	Medio
Errores de mantenimiento	Falta de mantenimiento planificado	Integridad	Medio
Errores del administrador	Entrenamiento de seguridad insuficiente	Integridad	Medio
Fuego	Desastre natural Desastre provocado por personas	Disponibilidad	Medio
Indisponibilidad del personal	Ausencia de personal	Disponibilidad	Medio
Ingeniería social	Protección inadecuada para acceso público Administración deficiente de contraseña Corrupción	Disponibilidad, integridad	Medio

Teniendo en cuenta los datos obtenidos de la tabla anterior en relación a las vulnerabilidades, pilar de la seguridad de la información afectado y el impacto podemos determinar las consecuencias que tendría para el GAD

Desembolso económico

Costo por reparación de los activos involucrados e infraestructura afectada. En caso de extorsión por robo de información costo por recuperación de información robada. El costo por instalar nuevos sistemas de seguridad.

Cambio en el modelo de negocio

Replanteamiento en la forma en que se recopilan los datos e información para asegurarse que no vuelva a ser vulnerable. Cierre del sitio web por incapacidad de hacer frente a ataques.

Pérdida de datos/información

Robo de datos e información geográfica sensible relacionada a temas como el desarrollo productivo, ordenamiento territorial, uso y ocupación del suelo, uso de espacios públicos, vialidad urbana, catastros multifinalitarios urbanos y rurales, acceso a riberas y lechos de río, lago y lagunas, explotación de materiales áridos y pétreos, gestión ambiental, registro de la propiedad, planes y programas de vivienda de interés social, control de construcciones, regulación de actividad turística, infraestructura de desarrollo social, patrimonio cultural y natural, gestión de riesgos, entre otras. Información considerada relevante para la planificación y la gestión pública local y nacional.

Pérdida de reputación

Incapacidad del GAD para protegerse de ataques internos y externos.

El alto riesgo de que los activos involucrados en la gestión, procesamiento y publicación de la información del sistema de información geográfica del GAD enfrenten fugas de datos si no se aplican las medidas de prevención y

seguridad adecuadas puede lograr que la información y sus activos caigan en manos equivocadas.

El sistema de información geográfica utiliza mínimo nivel de autenticación, lo cual disminuye la posibilidad de actuar contra los atacantes. Para ataques elaborados como envío de spam, virus, accesos no autorizados se requiere acceder al servidor a través de una vulnerabilidad.

En una fuga de información, ésta puede caer en personas no adecuadas por lo que se conoce como error humano conocido también como comportamiento irresponsable o deliberado de un funcionario. Independientemente de su origen, ya que puede que la fuga haya sido desde adentro del GAD mediante algún dispositivo de almacenamiento extraíble o la explotación de alguna vulnerabilidad del servidor para ingresar y robar información.

Una de las formas de protección consiste en la aplicación de controles, que son políticas, procesos, procedimientos, mecanismos de protección de la infraestructura física y de seguridad, así como la adecuada selección y entrenamiento del personal que utiliza los activos involucrados en la administración del sistema de información geográfica.

5.3 Asignación de controles e indicadores

Para realizar la planificación de la implementación del esquema de seguridad se realizará la selección de controles especificados en el Anexo A de la norma ISO 2001:2013, la misma que ofrece catorce categorías que sirven como referencia para extraer los controles necesarios que puedan ayudar a reducir los riesgos identificados en el análisis de activos involucrados. A continuación se detallan los catorce controles (cláusulas del 5 al 18) involucrados.

A.5 Políticas de la seguridad de la información

A.6 Organización de la seguridad de la información

A.7 Seguridad de los Recursos Humanos

A.8 Gestión de activos

A.9 Control de acceso

A.10 Criptografía

A.11 Seguridad física y medioambiental

A.12 Seguridad de las operaciones

A.13 Seguridad de las comunicaciones

A.14 Adquisición, desarrollo y mantenimiento de sistemas

A.15 Relación con los proveedores

A.16 Gestión de incidentes de seguridad de la información

A.17 Aspectos de la seguridad de la información de la gestión de la continuidad del negocio

A.18 Cumplimiento

En las tablas siguientes se muestran los controles seleccionados para las amenazas de cada activo involucrado dentro del proceso de administración del Sistema de Información Geográfica del cantón Samborondón

Tabla 54. Controles del Anexo A de la norma ISO 2001:2013 aplicados a amenazas en el servidor GIS

SERVIDOR GIS	
Amenaza	**Control**
Acceso no autorizado	A.6.1.2 - Segregación de tareas A.9.1.1 - Política de control de acceso A.9.3 - Responsabilidades del usuario A.9.4 - Control de acceso a sistemas y aplicaciones
Difusión de software dañino	A.7.2.2 - Concientización, educación y capacitación sobre la seguridad de la información A.9.4 - Control de acceso a sistemas y aplicaciones A.12.2 - Protección contra el malware (programa malicioso) A.12.6.2 - Restricciones en la instalación de software
Daños por agua	A.11.1.4 - Protección contra las amenazas externas y mediambientales
Avería de orígen físico o lógico	A.6.1.2 - Segregación de tareas A.11.2.4 - Mantenimiento de los equipos
Deficiencias en la organización	A.6.1.1 Funciones y responsabilidades de la seguridad de la información A.6.1.2 - Segregación de tareas A.7.2.2 - Concientización, educación y capacitación sobre la seguridad de la información
Escapes de información	A.8.1.3 - Uso aceptable de los activos A.8.3 - Manejo de los medios de comunicación
Divulgación de información	A.9.3 - Responsabilidades del usuario A.13.2 - Transferencia de la información
Deterioro físico en el equipo	A.8.1.3 - Uso aceptable de los activos A.12.1 - Procedimientos y responsabilidades operaciones A.12.3.1 - Backup de la información
Manipulación de la configuración	A.6.1.2 - Segregación de tareas A.9.1.1 - Política de control de acceso A.12.3.1 - Backup de la información
Suplantación de la identidad del usuario	A.9.1.1 - Política de control de acceso A.9.3 - Responsabilidades del usuario
Modificación de la información	A.9.1.1 - Política de control de acceso A.9.2.2 - Provisión de acceso al usuario
Robo	A.8.1 - Responsabilidades sobre los activos A.11.1.2 - Controles físicos de los ingresos A.11.2 - Equipos
Fuego	A.11.1.3 - Seguridad de las oficinas, salas e instalaciones A.11.1.4 - Protección contra las amenazas externas y mediambientales
Desastres naturales	A.11.1.4 - Protección contra las amenazas externas y mediambientales
Abuso de privilegos de acceso	A.11.1.1 - Perímetro de seguridad física A.11.1.2 - Controles físicos de los ingresos
Ataque destructivo	A.11.1.2 - Controles físicos de los ingresos A.12.1 - Procedimientos y responsabilidades operaciones
Caídas del sistema por agotamiento de recursos	A.12.1 - Procedimientos y responsabilidades operaciones A.12.4 - Logeo y monitoreo
Errores de mantenimiento	A.11.2.4 - Mantenimiento de los equipos A.12.1 - Procedimientos y responsabilidades operaciones

Tabla 55. Controles del Anexo A de la norma ISO 2001:2013 aplicados a amenazas en computadores/laptops

COMPUTADORES/LAPTOPS	
Amenaza	**Control**
Acceso no autorizado	A.6.1.2 - Segregación de tareas A.9.1.1 - Política de control de acceso A.9.3 - Responsabilidades del usuario A.9.4 - Control de acceso a sistemas y aplicaciones
Difusión de software dañino	A.7.2.2 - Concientización, educación y capacitación sobre la seguridad de la información A.9.4 - Control de acceso a sistemas y aplicaciones A.12.2 - Protección contra el malware (programa malicioso) A.12.6.2 - Restricciones en la instalación de software
Daños por agua	A.11.1.4 - Protección contra las amenazas externas y mediambientales
Avería de orígen físico o lógico	A.6.1.2 - Segregación de tareas A.11.2.4 - Mantenimiento de los equipos
Deficiencias en la organización	A.6.1.1 Funciones y responsabilidades de la seguridad de la información A.6.1.2 - Segregación de tareas A.7.2.2 - Concientización, educación y capacitación sobre la seguridad de la información
Divulgación de información	A.9.3 - Responsabilidades del usuario A.13.2 - Transferencia de la información
Deterioro físico en el equipo	A.8.1.3 - Uso aceptable de los activos A.12.1 - Procedimientos y responsabilidades operaciones A.12.3.1 - Backup de la información
Manipulación de la configuración	A.6.1.2 - Segregación de tareas A.9.1.1 - Política de control de acceso A.12.3.1 - Backup de la información
Modificación de la información	A.9.1.1 - Política de control de acceso A.9.2.2 - Provisión de acceso al usuario
Fuego	A.11.1.3 - Seguridad de las oficinas, salas e instalaciones A.11.1.4 - Protección contra las amenazas externas y mediambientales
Desastres naturales	A.11.1.4 - Protección contra las amenazas externas y mediambientales
Abuso de privilegos de acceso	A.11.1.1 - Perímetro de seguridad física A.11.1.2 - Controles físicos de los ingresos
Caídas del sistema por agotamiento de recursos	A.12.1 - Procedimientos y responsabilidades operaciones A.12.4 - Logeo y monitoreo
Errores de mantenimiento	A.11.2.4 - Mantenimiento de los equipos A.12.1 - Procedimientos y responsabilidades operaciones

Tabla 56. Controles del Anexo A de la norma ISO 2001:2013 aplicados a amenazas en impresoras

IMPRESORAS	
Amenaza	**Control**
Daños por agua	A.11.1.4 - Protección contra las amenazas externas y mediambientales
Manipulación de la configuración	A.6.1.2 - Segregación de tareas A.9.1.1 - Política de control de acceso
Fuego	A.11.1.3 - Seguridad de las oficinas, salas e instalaciones A.11.1.4 - Protección contra las amenazas externas y mediambientales
Desastres naturales	A.11.1.4 - Protección contra las amenazas externas y mediambientales
Caídas del sistema por agotamiento de recursos	A.12.1 - Procedimientos y responsabilidades operaciones A.12.4 - Logeo y monitoreo
Errores de mantenimiento	A.11.2.4 - Mantenimiento de los equipos A.12.1 - Procedimientos y responsabilidades operaciones

Tabla 57. Controles del Anexo A de la norma ISO 2001:2013 aplicados a amenazas en GPS

GPS	
Amenaza	**Control**
Daños por agua	A.11.1.4 - Protección contra las amenazas externas y mediambientales
Robo	A.8.1 - Responsabilidades sobre los activos A.11.1.2 - Controles físicos de los ingresos A.11.2 - Equipos A.11.2.6 - Seguridad de los equipos y bienes fuera de las instalaciones
Desastres naturales	A.11.1.4 - Protección contra las amenazas externas y mediambientales
Amenaza física	A.8.2.3 - Manejo de los activos A.11.1.5 - Trabajo en áreas seguras

Tabla 58. Controles del Anexo A de la norma ISO 2001:2013 aplicados a amenazas en red local e inalámbrica

RED DE ÁREA LOCAL E INALÁMBRICA	
Amenaza	**Control**
Acceso no autorizado	A.9.1.2 - Acceso a las redes y a los servicios de las redes A.13.1.1 - Controles en las redes A.13.1.2 - Seguridad de los servicios de las redes
Fallo de servicios de comunicaciones	A.11.2.3 - Seguridad en el cableado A.11.2.4 - Mantenimiento de los equipos
Escapes de información	A.8.1.3 - Uso aceptable de los activos A.8.3 - Manejo de los medios de comunicación
Deterioro físico en el equipo	A.8.1.3 - Uso aceptable de los activos A.12.1 - Procedimientos y responsabilidades operaciones A.12.3.1 - Backup de la información
Fuego	A.11.1.3 - Seguridad de las oficinas, salas e instalaciones A.11.1.4 - Protección contra las amenazas externas y mediambientales
Desastres naturales	A.11.1.4 - Protección contra las amenazas externas y mediambientales
Corte del Suministro eléctrico	A.11.2.2 - Servicios públicos de soporte
Ataque destructivo	A.11.1.2 - Controles físicos de los ingresos A.12.1 - Procedimientos y responsabilidades operaciones
Contaminación electromagnética	A.11.2.4 - Mantenimiento de los equipos
Errores de configuración	A.12.1.1 - Documentación de los procedimiento operacionales A.13.1.3 - Segregación en las redes

Tabla 59. Controles del Anexo A de la norma ISO 2001:2013 aplicados a amenazas en documentos físicos

DOCUMENTOS FÍSICOS	
Amenaza	**Control**
Daños por agua	A.11.1.4 - Protección contra las amenazas externas y mediambientales
Robo	A.11.1.2 - Controles físicos de los ingresos
Fuego	A.11.1.3 - Seguridad de las oficinas, salas e instalaciones A.11.1.4 - Protección contra las amenazas externas y mediambientales
Desastres naturales	A.11.1.4 - Protección contra las amenazas externas y mediambientales
Destrucción de la información	A.9.1.1 - Política de control de acceso

Tabla 60 Controles del Anexo A de la norma ISO 2001:2013 aplicados a amenazas en datos e información

DATOS E INFORMACIÓN	
Amenaza	**Control**
Daños por agua	A.11.1.4 - Protección contra las amenazas externas y mediambientales
Deficiencias en la organización	A.6.1.1 Funciones y responsabilidades de la seguridad de la información A.6.1.2 - Segregación de tareas A.7.2.2 - Concientización, educación y capacitación sobre la seguridad de la información
Alteración de la información	A.9.1.1 - Política de control de acceso A.9.2.2 - Provisión de acceso al usuario
Modificación de la información	A.9.1.1 - Política de control de acceso A.9.2.2 - Provisión de acceso al usuario
Robo	A.8.1 - Responsabilidades sobre los activos A.11.1.2 - Controles físicos de los ingresos A.11.2 - Equipos
Fuego	A.11.1.3 - Seguridad de las oficinas, salas e instalaciones A.11.1.4 - Protección contra las amenazas externas y mediambientales
Desastres naturales	A.11.1.4 - Protección contra las amenazas externas y mediambientales
Degradación de los soportes de almacenamiento de la información	A.8.1.3 - Uso aceptable de los activos A.8.2.3 - Manejo de los activos A.9.1.1 - Política de control de acceso A.12.3.1 - Backup de la información
Errores de los usuarios	A.7.2.2 - Concientización, educación y capacitación sobre la seguridad de la información A.12.3.1 - Backup de la información
Ataque destructivo	A.11.1.2 - Controles físicos de los ingresos A.12.1 - Procedimientos y responsabilidades operaciones
Ingeniería social	A.7.2.2 - Concientización, educación y capacitación sobre la seguridad de la información
Destrucción de la información	A.9.1.1 - Política de control de acceso A.12.3.1 - Backup de la información

Tabla 61. Controles del Anexo A de la norma ISO 2001:2013 aplicados a amenazas en personal administrativo

PERSONAL ADMINISTRATIVO	
Amenaza	**Control**
Difusión de software dañido	A.7.2.2 - Concientización, educación y capacitación sobre la seguridad de la información A.9.4 - Control de acceso a sistemas y aplicaciones A.12.2 - Protección contra el malware (programa malicioso) A.12.6.2 - Restricciones en la instalación de software
Escapes de información	A.7.2.2 - Concientización, educación y capacitación sobre la seguridad de la información A.7.2.3 - Procesos disciplinarios A.8.3 - Manejo de los medios de comunicación
Alteración de la información	A.9.1.1 - Política de control de acceso A.9.2.2 - Provisión de acceso al usuario
Divulgación de información	A.7.2.2 - Concientización, educación y capacitación sobre la seguridad de la información
Suplantación de la identidad del usuario	A.9.1.1 - Política de control de acceso A.9.3 - Responsabilidades del usuario
Modificación de la información	A.7.2.3 - Procesos disciplinarios A.9.1.1 - Política de control de acceso A.9.2.2 - Provisión de acceso al usuario
Robo	A.7 - Seguridad de los recursos humanos A.7.2.3 - Procesos disciplinarios A.11.1.2 - Controles físicos de los ingresos
Degradación de los soportes de almacenamiento de la información	A.8.1.3 - Uso aceptable de los activos A.8.2.3 - Manejo de los activos A.9.1.1 - Política de control de acceso A.12.3.1 - Backup de la información
Indisponibilidad del personal	A.6.1.2 - Segregación de tareas
Ingeniería social	A.7.2.2 - Concientización, educación y capacitación sobre la seguridad de la información
Destrucción de la información	A.7.2.3 - Procesos disciplinarios A.9.1.1 - Política de control de acceso A.12.3.1 - Backup de la información

Tabla 62. Controles del Anexo A de la norma ISO 2001:2013 aplicados a amenazas en personal técnico

PERSONAL TÉCNICO	
Amenaza	**Control**
Difusión de software dañido	A.7.2.2 - Concientización, educación y capacitación sobre la seguridad de la información A.9.4 - Control de acceso a sistemas y aplicaciones A.12.2 - Protección contra el malware (programa malicioso) A.12.6.2 - Restricciones en la instalación de software
Escapes de información	A.7.2.2 - Concientización, educación y capacitación sobre la seguridad de la información A.7.2.3 - Procesos disciplinarios A.8.3 - Manejo de los medios de comunicación
Alteración de la información	A.9.1.1 - Política de control de acceso A.9.2.2 - Provisión de acceso al usuario
Divulgación de información	A.7.2.2 - Concientización, educación y capacitación sobre la seguridad de la información
Suplantación de la identidad del usuario	A.9.1.1 - Política de control de acceso A.9.3 - Responsabilidades del usuario
Modificación de la información	A.7.2.3 - Procesos disciplinarios A.9.1.1 - Política de control de acceso A.9.2.2 - Provisión de acceso al usuario
Robo	A.7 - Seguridad de los recursos humanos A.7.2.3 - Procesos disciplinarios A.11.1.2 - Controles físicos de los ingresos
Indisponibilidad del personal	A.6.1.2 - Segregación de tareas
Ingeniería social	A.7.2.2 - Concientización, educación y capacitación sobre la seguridad de la información
Destrucción de la información	A.7.2.3 - Procesos disciplinarios A.9.1.1 - Política de control de acceso A.12.3.1 - Backup de la información

Tabla 63. Controles del Anexo A de la norma ISO 2001:2013 aplicados a amenazas en página web

PÁGINA WEB	
Amenaza	**Control**
Acceso no autorizado	A.6.1.2 - Segregación de tareas A.9.1.1 - Política de control de acceso A.9.3 - Responsabilidades del usuario A.9.4 - Control de acceso a sistemas y aplicaciones
Vulnerabilidades de los programas	A.12.6.1 - Gestión de las vulnerabilidades técnicas A.13.1.2 - Seguridad de los servicios de las redes
Ataque destructivo	A.9.1.1 - Política de control de acceso A.12.1 - Procedimientos y responsabilidades operaciones A.12.3.1 - Backup de la información A.14.1.2 - Seguridad de los servicios de aplicación en las redes públicas
Caídas del sistema por agotamiento de recursos	A.12.1 - Procedimientos y responsabilidades operaciones A.12.4 - Logeo y monitoreo

Tabla 64. Controles del Anexo A de la norma ISO 2001:2013 aplicados a amenazas en base de datos GIS

BASE DE DATOS GIS	
Amenaza	**Control**
Acceso no autorizado	A.6.1.2 - Segregación de tareas A.9.1.1 - Política de control de acceso A.9.3 - Responsabilidades del usuario A.9.4 - Control de acceso a sistemas y aplicaciones
Difusión de software dañido	A.8.1.3 - Uso aceptable de los activos A.8.3 - Manejo de los medios de comunicación
Vulnerabilidades de los programas	A.12.6.1 - Gestión de las vulnerabilidades técnicas A.13.1.2 - Seguridad de los servicios de las redes
Modificación de la información	A.9.1.1 - Política de control de acceso A.9.2.2 - Provisión de acceso al usuario
Ataque destructivo	A.11.1.2 - Controles físicos de los ingresos A.12.1 - Procedimientos y responsabilidades operaciones
Abuso de privilegos de acceso	A.11.1.1 - Perímetro de seguridad física A.11.1.2 - Controles físicos de los ingresos
Ingeniería social	A.7.2.2 - Concientización, educación y capacitación sobre la seguridad de la información
Caídas del sistema por agotamiento de recursos	A.12.1 - Procedimientos y responsabilidades operaciones A.12.4 - Logeo y monitoreo
Errores del administrador	A.7.2.2 - Concientización, educación y capacitación sobre la seguridad de la información A.12.3.1 - Backup de la información
Destrucción de información	A.9.1.1 - Política de control de acceso A.12.3.1 - Backup de la información

Tabla 65. Controles del Anexo A de la norma ISO 2001:2013 aplicados a amenazas en software/aplicaciones GIS

SOFTWARE / APLICACIONES GIS	
Amenaza	**Control**
Acceso no autorizado	A.6.1.2 - Segregación de tareas A.9.1.1 - Política de control de acceso A.9.3 - Responsabilidades del usuario A.9.4 - Control de acceso a sistemas y aplicaciones
Difusión de software dañido	A.8.1.3 - Uso aceptable de los activos A.8.3 - Manejo de los medios de comunicación
Vulnerabilidades de los programas	A.12.6.1 - Gestión de las vulnerabilidades técnicas A.13.1.2 - Seguridad de los servicios de las redes
Modificación de la información	A.9.1.1 - Política de control de acceso A.9.2.2 - Provisión de acceso al usuario
Ataque destructivo	A.11.1.2 - Controles físicos de los ingresos A.12.1 - Procedimientos y responsabilidades operaciones
Abuso de privilegos de acceso	A.11.1.1 - Perímetro de seguridad física A.11.1.2 - Controles físicos de los ingresos
Ingeniería social	A.7.2.2 - Concientización, educación y capacitación sobre la seguridad de la información
Caídas del sistema por agotamiento de recursos	A.12.1 - Procedimientos y responsabilidades operaciones A.12.4 - Logeo y monitoreo
Errores del administrador	A.7.2.2 - Concientización, educación y capacitación sobre la seguridad de la información A.12.3.1 - Backup de la información
Destrucción de información	A.9.1.1 - Política de control de acceso A.12.3.1 - Backup de la información

5.4 Definición de proyectos

Actualmente ya se conoce el estado actual del proceso de administración del Sistema de Información Geográfica del GAD municipal de Samborondón y sus activos involucrados por lo que es necesario plantear proyectos que ayuden a alcanzar niveles de seguridad esperados.

Los proyectos que se proponen a continuación son el resultado de análisis de riesgos trabajados en conjunto con la persona responsable de TICs y obedecen a los resultados obtenidos. Para el caso particular del GAD se presentarán tres proyectos los cuales consisten en plan de capacitación, plan de continuidad del negocio y plan de mitigación de riesgos.

Los objetivos de los proyectos son:

Plan de capacitación:

Construir y mejorar los niveles de educación en el manejo de la seguridad de la información del GAD municipal del cantón Samborondón.

Plan de continuidad del negocio:

Llevar los riesgos a un nivel aceptable

Asegurar la continuidad del negocio ante diversas situaciones

Plan de mitigación de riesgos:

Establecer acciones para mitigar los riesgos por alteración de la información, avería de origen físico o lógico, difusión de software dañino, modificación de la información, suplantación de la identidad del usuario, vulnerabilidades de los programas, ataque destructivo, ingeniería social.

Los proyectos planteados son el resultado del análisis de los riesgos ya que se detectó un bajo nivel en la concientización del personal y capacitación. Además se pudo establecer con este análisis la necesidad de acciones adicionales en los equipos de cómputo y la red institucional que ayuden a mitigar la difusión de software dañino.

La tabla a continuación muestra la relación de los proyectos con los riesgos identificados para mitigar y los pilares de la seguridad de la información que se ven impactados.

Tabla 66. Relación de proyectos con riesgos identificados por encima del valor aceptable, con acciones a tomar

Proyecto	Amenaza	Pilar	Acciones	Impacto	Priodidad
Plan de capacitación	Deficiencias en la organización	Integridad	Campaña publicitaria Concientización Cursos de capacitación y/o actualización	Medio Alto Alto	Alto
	Divulgación de información	Confidencialidad			
	Escapes de información	Confidencialidad			
	Manipulación de la configuración	Integridad			
	Abuso de privilegos de acceso	Integridad			
	Destrucción de la información	Integridad			
	Errores de configuración	Integridad			
	Errores de los usuarios	Integridad			
	Errores de mantenimiento	Integridad			
	Errores del administrador	Integridad			
Plan de continuidad del negocio	Acceso no autorizado	Integridad	Generación de plan de acción. Establecimiento de equipo de respuesta. Diseño e implementación de un adecuado centro de cómputo.	Alto Medio Alto	Medio
	Daños por agua	Disponibilidad			
	Deterioro físico en el equipo	Disponibilidad, integridad			
	Fallo de servicios de comunicaciones	Disponibilidad			
	Robo	Disponibilidad			
	Amenaza física	Integridad			
	Avería de orígen físico o lógico	Disponibilidad, integridad			
	Caídas del sistema por agotamiento de recursos	Disponibilidad			
	Contaminación electromagnética	Disponibilidad			
	Corte del Suministro eléctrico	Disponibilidad			
	Degradación de los soportes de almacenamiento de la información	Confidencialidad, integridad			
	Desastres natuales	Disponibilidad			
	Fuego	Disponibilidad			
	Indisponibilidad del personal	Disponibilidad			
Plan de mitigación de riesgos	Alteración de la información	Disponibilidad, integridad	Bloqueo de puertos de comunicación utilizados por software Inspección de tráfico, bloquedo de tráfico Inspección y medicion de tráfico para control del canal Establecimiento de políticas (generales, de seguridad para equipos tecnológicos, de acceso al centro de cómputo, de respaldo y recuperación del sistema de información geográfica, de seguridad para las comunicaciones, redes y uso del internet)	Medio Medio Medio Alto	Alto
	Avería de orígen físico o lógico	Disponibilidad, integridad			
	Difusión de software dañino	Disponibilidad, integridad			
	Modificación de la información	Confidencialidad, integridad			
	Suplantación de la identidad del usuario	Confidencialidad, integridad			
	Vulnerabilidades de los programas	Disponibilidad, integridad			
	Ataque destructivo	Disponibilidad, integridad			
	Ingeniería social	Disponibilidad, integridad			

5.4.1 PLAN DE CAPACITACIÓN

Alcance

El plan de capacitación involucra a personal administrativo y técnico, con el propósito que se tenga educación en aspectos básicos y avanzados de seguridad de la información respectivamente. El plan de concientización está orientado a sensibilizar a todos los funcionarios del GAD para que identifiquen las amenazas que enfrenta la información y que se sigan los procedimientos necesarios para que éstas no se materialicen. Disminuir el riesgo presente con respecto a deficiencias en la organización, divulgación de información y escapes de información, amenazas identificadas en este proyecto.

Fases

Diseño del plan de capacitación: En esta etapa se revisará y diseñaran los cursos relacionados con la seguridad de información para el personal, de la misma manera se procederá con los talleres prácticos. Se estima de 25 a 30 días para el desarrollo de esta fase.

Consecución de recursos: Durante esta fase se realizará la gestión de recursos financieros y de talento humano que se necesitan para poner en funcionamiento el plan de capacitación. Se calcula que esta fase puede tardar hasta 6 meses.

Ejecución del plan: De acuerdo a lo planificado, la ejecución del plan de capacitación tendría una duración de 6 meses

Entrega de informe: En esta fase se entregaran los informes, ayudas memoria y documentos de soporte del plan de capacitación, esta etapa tendrá una duración de 15 días.

5.4.2 PLAN DE CONTINUIDAD DEL NEGOCIO

Alcance

El plan de continuidad de negocio busca generar el camino a seguir para restituir en el menor tiempo posible la operatividad del negocio en caso de que quede fuera de servicio por causa de un evento que impida su funcionamiento parcial o total; contempla las acciones a realizar con relación al hardware, software y talento humano involucrado en los procesos definidos en este plan.

También se consideran los riesgos y soluciones del ambiente físico relacionado con el proceso de administración del sistema de información geográfica del GAD.

El plan de continuidad del negocio busca reducir el nivel de riesgo de las amenazas de Acceso no autorizado, daños por agua, deterioro físico en el equipo, fallo de servicios de comunicaciones, robo, Amenaza física, avería de origen físico o lógico, caídas del sistema por agotamiento de recursos, contaminación electromagnética, corte del suministro eléctrico, degradación de los soportes de almacenamiento de la información, desastres naturales, fuego e indisponibilidad del personal

Fases

Evaluación del estado actual de los activos involucrados: Se realizará un análisis de riesgos para identificar los activos con que se cuenta, asignación de los controles y procedimientos que deben ser desarrollados. Esto se ha elaborado a lo largo del presente documento.

Desarrollo del plan: En esta etapa se definirán los procedimientos de alerta y actuación ante los eventos que pueden llegar a activar el plan,

también se definirá el equipo necesario para el correcto desarrollo del plan junto con sus funciones y responsabilidades.

Pruebas: En esta etapa se realizarán las pruebas necesarias para comprobar que el plan funciona de manera adecuada.

Capacitación: En esta etapa se programará la realización de capacitaciones y entrenamiento respectivo al personal a cargo del plan de contingencias y se realizará un plan de concientización dirigido a los funcionarios del GAD cantonal de Samborondón.

Finalmente, se consideran los riesgos y soluciones del ambiente físico relacionados con la administración del sistema de información geográfica y sus activos involucrados para ser implementados en un adecuado centro de cómputo.

5.4.3 PLAN DE MITIGACIÓN DE RIESGOS

Alcance

El plan de mitigación de riesgos busca establecer mecanismos, acciones y recursos que limiten de la mejor manera la propagación de programas maliciosos, programas autoejecutables, programas que intercambien información en los equipos de cómputo así como en las aplicaciones y la red institucional del GAD. De la misma manera se busca restringir el acceso a información almacenada en los diversos equipos tecnológicos, de acuerdo a los niveles de acceso.

Objetivos

Establecer las acciones encaminadas a mitigar los riesgos más relevantes detectados en el análisis de riesgos aplicado a la administración del sistema de información geográfica del GAD ante la eventualidad de toda acción que pueda una inoperatividad ya sea total o parcial.

5.5 Elaboración de las políticas de seguridad

Los activos asociados al proceso de administración del Sistema de Información Geográfica del cantón Samborondón son recursos importantes y vitales, sin ellos el GAD quedaría limitado en la ejecución de procesos y compromisos gubernamentales, por este motivo el departamento de Tecnologías de Información y Comunicación, tiene la responsabilidad de preservarlos, utilizarlos y mejorarlos. Se deben tomar las acciones necesarias para asegurar que el Sistema de Información Geográfica y la información que contiene estén apropiadamente protegidos de diversas clases de amenazas y riesgos tales como: Accidentes y desastres naturales, hackers, sabotaje, espionaje, violación de la privacidad, intrusos, etc.

Esta información perteneciente al GAD debe protegerse de acuerdo a su valor e importancia, se deben emplear medidas de seguridad independientemente de cómo se almacena la información (física o digital), cómo se procesa (servidor, computadores o laptops, etc.). Tal protección incluye restricciones de accesos a los usuarios de acuerdo a sus funciones.

Todas las áreas del GAD están en el deber y en la responsabilidad de dedicar tiempo y recursos suficientes para asegurar que los activos de información

estén suficientemente protegidos. Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así, reducir los riesgos. En tal virtud el área de Tecnologías de Información y Comunicación llevará a cabo un análisis de riesgos y se revisarán las políticas de seguridad anualmente. Para fortalecer este proceso se realizará un informe en el que se muestre el estado actual del GAD en cuanto a seguridad informática y los logros obtenidos.

A todos los funcionarios, contratistas y consultores debe proporcionárseles información y advertencias para que ellos puedan proteger y manejar adecuadamente los recursos informáticos del GAD. La finalidad de estas políticas es proporcionar instrucciones específicas sobre cómo mantener los activos de tecnología (estén o no conectados a la red) así como la información que se encuentra en ellos.

RESPONSABILIDADES

Los siguientes entes son responsables, en diferentes niveles de la seguridad en el GAD:

El Departamento de Tecnologías de Información y Comunicación (TIC), es responsable de implantar y velar por el cumplimiento de las políticas y procedimientos de seguridad en el GAD. También es responsable de evaluar, adquirir e implantar productos de seguridad informática y realizar las actividades necesarias para garantizar un ambiente informático seguro. Debe ocuparse de proporcionar apoyo técnico en los asuntos relacionados con la seguridad y en particular los casos de infecciones de virus, intrusiones, fraudes y otros incidentes.

El responsable de TIC, es la persona encargada de dirigir las investigaciones sobre incidentes y problemas relacionados con la seguridad, establecer los controles de accesos apropiados para cada usuario, supervisar el uso de los recursos informáticos, revisar las bitácoras de acceso y llevar a cabo las tareas de seguridad relacionadas a los sistemas que administra. También es la persona encargada de informar a sus superiores sobre las actividades sospechosas.

Los funcionarios, son responsables de cumplir con todas las políticas del GAD relacionadas a la seguridad informática y principalmente:

- Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos

- Proteger cuidadosamente sus contraseñas.

- Elegir una contraseña robusta

- No divulgar información sensible del GAD a personas no autorizadas

- No hacer mal uso de los recursos informáticos y de comunicaciones.

- No permitir el uso de los sistemas informáticos a personas no autorizadas

- Reportar inmediatamente a su jefe inmediato o a un funcionario de TIC cualquier evento ocurrido que pueda comprometer la seguridad de la información del GAD y los recursos informáticos.

POLÍTICAS GENERALES

Propósito

El propósito de esta política es establecer las directrices, procedimientos y requisitos para asegurar la protección apropiada de los recursos informáticos y de la información del GAD.

- Los servicios de la red municipal de datos son de uso exclusivo para los funcionarios del GAD municipal de Samborondón y para los usuarios externos previamente autorizados.

- Se considera como falta grave el robo, daño o alteración de la información de los sistemas informáticos del GAD, el uso de los sistemas para ejecutar actos como penetración a otras redes, piratería informática, etc.

- La información de los sistemas debe estar siempre disponible.

- Las redes de computadores ya sean cableadas o inalámbricas son consideradas “redes inseguras”

- Las medidas de seguridad deben ser identificadas e implementadas teniendo en cuenta el tipo de riesgo.

- Los bienes tecnológicos entregados a los funcionarios del GAD municipal de Samborondón para la ejecución de sus funciones son propiedad del GAD. El uso de estos bienes debe ser única y necesariamente para actividades relacionadas con las funciones asignadas.

- Cada funcionario tiene autorización para acceder a la información inherente a las funciones que realiza.

- Cada funcionario (usuario) tendrá acceso exclusivamente a las actividades vinculadas al usuario creado considerando los privilegios otorgados por Tecnologías de Información y Comunicación

- Todos los funcionarios del GAD deberán tener su credencial en la cual tendrá su foto, nombres y apellidos, número de cédula y área en la que labora.

- Todo el personal externo al GAD deberá recibir una tarjeta de identificación en la cual estará identificada el área que va a visitar, para acceder a esta tarjeta deberá entregar su identificación que debe ser únicamente la cédula de identidad, licencia de conducir o pasaporte.

- Al ingresar o salir de las oficinas, los funcionarios deberán registrar en el lector biométrico su ingreso o salida.

- Está prohibido fumar dentro de las instalaciones

- Está prohibido el consumo de bebidas alcohólicas dentro de las instalaciones y fuera de las instalaciones en el horario de trabajo.

- Los equipos del sistema contra incendios deben recibir el mantenimiento respectivo.

- Es necesario aplicar la política de escritorios limpios

POLÍTICAS DE SEGURIDAD PARA EQUIPOS TECNOLÓGICOS

Propósito

El propósito de esta política es establecer las directrices, los procedimientos y requisitos para asegurar la protección apropiada de los equipos tecnológicos del GAD

- Todo equipo tecnológico tendrá un custodio quien será el responsable por su cuidado y buen uso.

- Los equipos tecnológicos del GAD solo deben usarse en un ambiente seguro. Se considera que un ambiente es seguro cuando se han implantado las medidas de control apropiadas para proteger el hardware, software y la información.

- Los funcionarios del GAD solo podrán usar el software que tenga licencia, en caso de que sea necesario usar un programa de licencia libre deberá hacerse el requerimiento al responsable del área indicando los motivos y a

su vez el responsable realizará el requerimiento a Tecnologías de Información y Comunicación.

- Está prohibido realizar cambios de configuración en el hardware y el software de los equipos tecnológicos.

- Los equipos del GAD solo deben usarse para actividades relacionadas a las funciones de cada funcionario y no para otros fines, tales como juegos, pasatiempos o asuntos personales.

- Está prohibida la instalación de software obtenido del internet

- Los equipos tecnológicos deben protegerse de riesgos medioambientales (agua, polvo, fuego)

- Cualquier falla en los equipos cómputo y de comunicaciones debe ser reportada inmediatamente ya que podrías causar serios problemas como pérdida de información o indisponibilidad de servicios.

- Deben protegerse los equipos para disminuir el riesgo de robo, destrucción y mal uso.

- Está prohibido mover o reubicar los equipos de cómputo sin un permiso respectivo. En caso de ser necesario llevar un equipo fuera del GAD se requiere una autorización escrita.

- La pérdida o robo de cualquier componente de hardware o software debe ser reportada inmediatamente.

- Si un equipo tiene acceso a información sensible o confidencial es necesario que tenga un mecanismo de control de acceso especial.

- Todos los equipos deben tener instalado el software antivirus adquirido por el GAD.

- Las contraseñas entregadas a cada funcionario son personales e intransferibles, cada funcionario es responsable por la contraseña asignada.

- Las contraseñas caducan cada 60 días, estas contraseñas deben contener obligatoriamente una letra mayúscula, números, caracteres especiales y letras minúsculas.

- Las contraseñas que se usan para acceder a los diversos servicios del GAD, deben estar encriptadas.

- Al ingresar incorrectamente una contraseña ya sea por error voluntario o involuntario la cuenta se bloqueará al tercer intento fallido y se desbloqueará luego de quince minutos.

- Los equipos deben tener bloqueo de puertos USB y unidad CD/DVD, su habilitación se hará bajo solicitud del jefe inmediato y autorización del responsable de Tecnologías de Información y Comunicación.

- Está prohibido abrir el case del equipo de cómputo asignado. Esta actividad solo está autorizada para el personal de Tecnologías de Información y Comunicación.

- Está prohibido la conexión de equipos que no pertenecen al GAD a la red cableada (LAN)

- El uso del WIFI institucional para personas externas al GAD estará regulado por una política de asignación de accesos temporales.

- El acceso a los servicios de red e internet son regulados por el firewall.

- El uso o acceso de determinados servicios están asignados en el perfil de cada usuario.

- Los intentos de accesos no autorizados serán monitoreados periódicamente.

- Transcurridos diez minutos sin registrar actividad, el equipo de cómputo se bloqueará automáticamente

- Los funcionarios del GAD solo podrán usar el software que tenga licencia, en caso de que sea necesario usar un programa de licencia libre deberá hacerse el requerimiento al responsable del área indicando los motivos y a su vez el responsable realizará el requerimiento a Tecnologías de Información y Comunicación.

- Está prohibida la instalación de software obtenido del internet o software que provenga de una fuente no confiable.

- Está prohibida la instalación de software no autorizado, incluyendo el software que haya sido adquirido por el usuario.

- El acceso a los servicios de red e internet son regulados por el firewall.

- El uso o acceso de determinados servicios están asignados en el perfil de cada usuario.

- Solo puede descargarse información de redes externas de acuerdo a los procedimientos establecidos. Es obligatorio el uso del antivirus para examinar todo la información externa o incluso de otros departamentos del GAD.

- La información original no debe ser borrada o eliminada hasta que se haya comprobado que puede ser recuperada desde los archivos encriptados mediante el proceso de descifrado.

- La información concerniente al Sistema de Información Geográfica podrá ser actualizada o modificada de acuerdo a la asignación de derecho que se haya realizado encargado y se mantendrá un registro de dichos cambios.

- Se llevará registro de todos los accesos internos y externos al Sistema de Información Geográfica y se guardará una copia de seguridad de ésta información.

POLÍTICAS DE ACCESO AL CENTRO DE CÓMPUTO

Propósito

El propósito de esta política es establecer las directrices, los procedimientos y requisitos para asegurar la protección apropiada de los equipos tecnológicos e información alojada en ellos que se encuentran dentro del centro de cómputo.

- La gestión del acceso al centro de cómputo del GAD estará a cargo de Tecnologías de Información y Comunicación

- Todo acceso físico al centro de cómputo será restringido, debiéndose gestionar y documentar de acuerdo al procedimiento respectivo para acceso físico al centro de cómputo

- El acceso al centro de cómputo y racks de redes de Tecnologías de Información están restringidos y solo pueden ingresar los administradores de los servicios tecnológicos respectivos.

- Todo acceso autorizado al centro de cómputo será guardado en una bitácora

- No podrán ser almacenados dentro de ningún espacio dentro del centro de cómputo materiales inflamables o peligrosos.

- El centro de cómputo debe mantenerse limpio y ordenado en todo momento, además se prohíbe el ingreso de todo tipo de comidas y bebidas.

- El ingreso al centro de cómputo deberá realizarse con el sistema biométrico y con llaves del mismo.

- Los permisos de acceso concedidos podrán ser permanentes o temporales.

- Cualquier requerimiento de ingreso al centro de cómputo debe seguir el procedimiento respectivo.

- Todo tercero que ingrese al centro de cómputo debe hacerlo acompañado por un funcionario autorizado de Tecnologías de Información y Comunicación durante el tiempo que lo requiera.

- Está prohibido tomar fotografías o videos en el interior del centro de cómputo sin la autorización respectiva.

POLÍTICAS DE SEGURIDAD PARA LAS COMUNICACIONES, REDES Y USO DEL INTERNET

Propósito

El propósito de esta política es establecer las directrices, los procedimientos y los requisitos para asegurar la protección adecuada del GAD al estar conectada a redes de computadoras y acceso a internet a través de la red institucional.

- El acceso a internet está autorizado por el jefe inmediato si considera al internet como herramientas que faciliten la ejecución de las funciones del servidor público.

- Cada funcionario es responsable del respectivo uso

- La institución tendrá la responsabilidad de todo el contenido del sitio web (http://www.samborondon.gob.ec/)

- Cualquier software o archivos descargados a través del internet del GAD son propiedad del GAD.

- Queda prohibido el acceder, cargar, descargar o distribuir material pornográfico o sexualmente explícito.

- No está permitido el uso de la red institucional para obtener ganancias financieras o comerciales.

- Se prohíbe degradar o alterar el rendimiento de la red

- Ningún funcionario puede utilizar las instalaciones del GAD conscientemente para descargar o distribuir software pirateado.

- Se prohíbe el uso de los servicios de internet del GAD para propagar deliberadamente códigos maliciosos, virus, gusanos, caballos de troya, etc.

- Los servidores de red y equipos de comunicaciones deben estar ubicados en áreas apropiadas, protegidos contra daños y robo.

- Está prohibido el acceso al área asignada para los servidores y equipos de comunicaciones a personas no autorizadas

- Está prohibido el uso de contraseñas grupales para facilitar el acceso a aplicaciones, bases de datos, archivos, redes, computadoras y demás recursos del sistema.

- La contraseña inicial asignada a un nuevo usuario solo debe ser válida para el primer inicio de sesión. En este momento el usuario debe elegir otra contraseña que cumpla con los parámetros solicitados previamente.

- Las contraseñas predefinidas que traen los equipos nuevos deben ser cambiadas inmediatamente al ponerse a funcionar al equipo.

- Los privilegios de accesos a los usuarios deben ser ratificados periódicamente.

- Está prohibido el uso de cuentas anónimas o de invitados.

- Privilegios especiales solo deben ser asignados a los usuarios directamente responsables de la administración o seguridad de los sistemas

- No deben concederse cuentas a personas que no sean funcionarios del GAD.

- En caso de ser necesario el acceso remoto a los sistemas debe existir una autenticación más robusta basada en contraseñas dinámicas, token de autenticación o tarjetas inteligentes.

POLÍTICAS DE SEGURIDAD PARA LA ADMINISTRACIÓN DEL SISTEMA DE INFORMACIÓN GEOGRÁFICA

Propósito

El propósito de esta política es establecer las directrices, los procedimientos y los requisitos para asegurar la protección adecuada del Sistema de Información Geográfica del GAD.

- Toda actividad será registrada y archivada mediante archivos de log o bitácoras de los sistemas.

- Los registros de log almacenará nombres de usuario, nivel de privilegios, IP de donde se accedió, fecha y hora de acceso, actividad desarrollada, intentos de conexión fallidos o acertados, archivos a los que se tuvo acceso a fin de conocer las acciones que se realizan.

- Se prohíbe el acceso a la configuración del sistema operativo del servidor, esta acción es solo permitida para personal de TIC.

- Se llevará un registro global del mantenimiento efectuado sobre el servidor y los cambios realizados desde su instalación.

POLÍTICAS DE RESPALDO Y RECUPERACIÓN DE INFORMACIÓN DEL SISTEMA DE INFORMACIÓN GEOGRÁFICA

Propósito

El propósito de esta política es establecer las directrices, los procedimientos y requisitos para asegurar el manejo adecuado de respaldos de los datos e información que forman parte del Sistema de Información Geográfica del GAD

- Los respaldos de información se realizarán mediante la herramienta correspondiente y ésta información será almacenada en una unidad de almacenamiento externo.

- Las copias de respaldo de la información se realizarán diariamente en un horario definido.

- Es necesario realizar pruebas de restauración al menos 2 veces al año.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. El presente trabajo permitió elaborar una planificación de un esquema de seguridad para la administración de un sistema de información, en este caso en particular información geográfica que está implementado y es administrado por los funcionarios responsables del manejo de ésta información dentro del GAD municipal del cantón Samborondón, el cual fue de mucha ayuda para desarrollar destrezas y mejorar habilidades, como por ejemplo el manejo de

metodologías y realización de auditoría, de esta manera se pudo realizar trabajos relacionados a la gestión de la seguridad de la información.

2. La información es el activo más importante de las organizaciones, instituciones, empresas, personas, et. Siendo el GAD municipal del cantón Samborondón una institución pública es vital que este activo este protegido contra cualquier ataque o amenaza que pueda atentar contra los pilares de la seguridad de la información, por lo cual es fundamental considerar las recomendaciones que da norma ISO 27001:2013.
3. Los activos involucrados en el proceso de administración del sistema de información geográfica del GAD presentan niveles medio y alto de riesgo en su gran mayoría de acuerdo a las amenazas presentadas para cada activo, se espera que los controles asignados ayuden a reducir el riesgo llevándolos al siguiente nivel inferior.
4. El análisis de riesgos del proceso de administración del sistema de información geográfica mostró una necesidad de crear un plan de continuidad del negocio que permita estar listos en caso de incidentes que comprometan el funcionamiento normal. De la misma manera se evidenció la necesidad de involucrar no solo al personal involucrado en la administración del sistema sino a todos los funcionarios en el alineamiento de los procesos para cumplir con lo establecido en la norma ISO 27001.2013.

5. Se han diseñado políticas de seguridad para el proceso de administración del sistema considerando los dominios de la norma ISO 27001:2013 para mitigar/minimizar los riesgos que se puedan presentar. Cabe señalar que el cumplimiento de las políticas de seguridad no garantiza que el riesgo sea eliminado debido a que siempre estará presente, pero con la ayuda de las políticas de seguridad disminuirá la materialización del mismo.

RECOMENDACIONES

1. Realizar una segunda auditoría con el fin de determinar para determinar el estado de los controles que fueron propuestos en este proyecto. Esta auditoría será la que permita establecer el mecanismo a seguir para mejorar el nivel de madurez cuestiones de seguridad dentro del GAD.
2. Se recomienda realizar revisiones y actualizaciones periódicas a las políticas de seguridad con la finalidad de identificar nuevas amenazas que puedan poner en riesgo la seguridad de la información del sistema y sus activos.
3. Es importante poner en marcha el plan de capacitación y trabajar continuamente en la concientización de los funcionarios del GAD en los aspectos relacionados a la seguridad de la información.
4. Es necesario contar con un funcionario dentro del departamento de TIC quien será el responsable del monitoreo del cumplimiento de las políticas de seguridad establecidas en este proyecto.
5. De la misma manera se recomienda capacitar y certificar al personal de TIC para que puedan realizar auditorías internas, de esta manera se logrará evitar la contratación de auditores externos y el costo que representa.

BIBLIOGRAFÍA

[1] Álvaro Gómez, Enciclopedia de la Seguridad Informática. 2ª Edición, 2014

[2] The ISO 27000 Directory, Introduction To ISO 27002 (ISO27002), http://www.27000.org/iso-27002.htm , fecha de consulta octubre 2018

[3] El portal de ISO 27001 en español, http://www.iso27000.es/iso27000.html , fecha de consulta octubre 2018

[4] NORMA INTERNACIONAL ISO/IEC 27001, Segunda edición 2013-10-01

[5]MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método, https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html , fecha de consulta octubre 2018

[6] Plan Cantonal de Desarrollo & Plan de Ordenamiento Territorial 2012-2022, Cantón Samborondón – Provincia del Guayas, http://www.samborondon.gob.ec/pdf/LOTAIP/PlanCantonalDeDesarrollo&PlanDeOrdenamientoTerritorial.pdf , fecha de consulta octubre 2018

[7] Calidad y Gestión, GAP ANÁLISIS PARA IMPLEMENTACIÓN DE ISO 9001:2015, https://calidadgestion.wordpress.com/tag/analisis-de-brechas/ , fecha de consulta noviembre 2018

[8] ProtektNet Especialistas en Seguridad Informática, Análisis de Brecha de Seguridad de la información, https://protektnet.com/servicios/cumplimiento-normativo/analisis-de-brecha-de-seguridad-de-la-informacion/ , fecha de consulta noviembre 2018

[9] SGSI Blog especializado en Sistemas de Gestión de Seguridad de la Información, La norma ISO 27002 complemento para la ISO 27001, https://www.pmg-ssi.com/2016/06/la-norma-iso-27002-complemento-para-la-iso-27001/ , fecha de consulta noviembre 2018

[10] NORMA ESPAÑOLA UNE 71504:2008, 2008-07-16

[11] Libro Virtual Seguridad Informática, https://es.calameo.com/read/00411161427e42237c86b , fecha de consulta diciembre 2018

ANEXOS