UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

OCTUBRE 2018 – MARZO 2019

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN SISTEMAS

TEMA:

ANÁLISIS DE LOS ESTÁNDARES DEL EMPLEO DEL SERVIDOR DE BASE DE DATOS DEL GAD MUNICIPAL DE VENTANAS

EGRESADO:

ERNESTO ISRAEL JIMENEZ VERGARA

TUTORA:

ING. MOREIRA SANTOS MARÍA GENOVEVA, MIE

AÑO 2019

Introducción

El presente caso de estudio titulado “Análisis de los estándares del empleo del servidor de base de datos del GAD municipal de Ventanas”, tiene la finalidad de analizar la aplicación de estándares requeridos para el uso correcto del servidor administrado en el departamento de TIC de la institución.

La razón del presente estudio es para conocer los criterios principales de la aplicación de estándares la cual se encamina en dos direcciones, la primera es empírica es decir por costumbre o por la forma de laborar de una persona, la segunda corresponde al cumplimiento de las reglas que son proporcionadas por diversas entidades mediante un documento al cual han denominado ‘estándar’.

Estas reglas pueden ser usadas las veces que sean necesarias por las instituciones que opten por cumplir los requerimientos proporcionados por aquella documentación, para lograr este fin es necesario recopilar información que permita un análisis racional, además de fundamentar teóricamente las razones por la cual es necesario y útil su aplicación.

El análisis de los estándares aplicados o no aplicados en el servidor brinda a la institución de conocimiento suficiente para tomar decisiones; evitar plagio, optimizar los procesos que conlleven a la atención de un cliente además de facilitar el trabajo de las áreas que dependan de sus servicios.

Debido al amplio contexto de los estándares el presente estudio contiene un límite en su análisis, es decir estudiar tan solo ciertos reglamentos considerados importantes y notorios que se requieren para el uso de un servidor, dejando a un lado ciertas problemáticas al menos que indirectamente se relacionen con el objeto estudiado.

Desarrollo

El Gobierno Autónomo Descentralizado Municipal del Cantón Ventanas es un organismo de gobierno seccional encargado de la administración del cantón de forma autónoma, tiene como propósito sostener las acciones de desarrollo las cuales dinamizan proyectos que aseguran el desarrollo social, económico y ambiental de la población, conformado por el alcalde, concejo cantonal, además de diferentes direcciones municipales.

Las cualidades del departamento de tecnologías de la información y comunicación del GAD municipal del cantón Ventanas es la de encargarse de la administración de los recursos físicos y lógicos de tecnología, además de los servicios digitales que utilizan varias de las direcciones de la institución.

Investigar o analizar brinda nuevos descubrimientos mediante un elaborado proceso, es así como el presente estudio utiliza metodologías o técnicas para recopilar datos, cada una de ellas debe abstraerse en la **sub-línea de investigación** correspondiente a la carrera de ingeniería de sistemas la cual es el modelo de trasmisión de datos y telecomunicaciones.

Para proceder con el estudio se necesita recolectar información, haciendo uso de la metodología de observación de campo en el departamento de TIC, el medio comunicacional utilizado será la interacción personal ya que se tiene acceso al departamento.

Se utilizará adicionalmente una técnica que permita obtener una mayor comprensión del objeto a estudiar como lo es la entrevista, registrando la información obtenida en herramientas de investigación como; guía para la observación y de entrevista.

El presente análisis abarcara únicamente la aplicación de estándares basados en el empleo del servidor de base de datos del GAD Municipal del cantón Ventanas, limitándose a la verificación de instalaciones, así como su respectiva estructura, políticas de seguridad, niveles de fiabilidad, consideraciones ambientales.

Actualmente ninguna empresa u organización de cualquiera naturaleza puede funcionar sin un área tecnológica, sin embargo, esta necesita la aplicación correcta de ciertas normativas o estándares para su correcto funcionamiento además de estar al tanto de la importancia de aplicarlos.

Aunque existen varias conceptualizaciones para la palabra estándar, debe ser adaptable y universal dependiendo de la situación en la que se utilice. Según (Lopez, 2014) son "un documento con un contenido de tipo técnico-legal que establece un modelo o norma que refiere lineamientos a seguir para cumplir una actividad o procedimientos". Al nivel de software como de hardware, fue necesario establecer criterios homogéneos para resolver problemas expuestos en las siguientes interrogantes:

¿Cuál es la forma de aquel puerto? ¿En qué formato se almacena la información? ¿Qué características tendrá ese cable? ¿Qué semántica tiene el lenguaje de programación usado? ¿Qué protocolo son utilizados al establecer cierto tipo de conexión?, por tal motivo los estándares facilitan la compatibilidad, interoperabilidad y la competencia.

La infraestructura empresarial ha expandido sus comunicaciones para aprovechar el valor de los negocios asociados a las tecnologías, sin alianzas o acuerdos en el que los fabricantes en conjunto con los consumidores aceptaran de manera extendida los estándares de tecnología, siendo estas especificaciones establecidas para la compatibilidad de los productos (P.Laudon, 2016).

Los datos recolectados serán presentados ordenadamente mediante un sistema de identificación de activos en modalidad de tablas, de modo que estos puedan ser analizados posteriormente. Según (Sampieri, 2014) “el proceso de recolectar los datos implica la elaboración un plan detallado de cada procedimiento con el propósito de conducir la reunión de datos”. Todo esto con el propósito específico de reconocer los activos para su posterior análisis. Ver tabla 1

DATOS / INFORMACION	NOMBRE DEL ACTIVO
DATOS /INFORMACION	1. [BD_GABVENTANAS] Base Datos GABVENTANAS
	2. [BD_CONTAGAB] Base Datos RUVENTANAS
	3. [BD_BIOMETRICO] Base de datos del BIOMETRICO
SERVICIOS	4. [SERV_CAT] Emisión de reportes de Catastro.
	5. [SERV_PAGO] Genera facture de pagos de Catastro.
APLICACIONES	6. [POR_WEB] Portal Web
	7. [SW_ARGII] Sistema de ARGII
	8. [SW_AUTOCAD] Sistema de AUTOCAD
	9. [SW_CATASTRO] Sistema de Catastro
	10. [SW _PRECIOS] Sistema Informático de Precios
	11. [SW_SIAF] Sistema Integrado de Administración Financiera (SIAF)
	12. [SI _PDT] *Sistema* Planilla Electrónica
	13. [SO] Sistema Operativo
	14. [SI_SQL]Sistema: Gestor de BASE DE DATOS
	15. [SI_SIGAMI] Sistema de área de Contabilidad.
	16. [ANT_VIR] Anti virus
EQUIPAMIENTO INFORMATICO	17. [SRV_BD] Servidor de Rack
	18. [SRV_BD] Servidor de Torre
	19. [PC] Computadora
REDES DE COMUNICACIONES	20. [ADSL] Conexión a internet.
EQUIPAMIENTO AUXILIAR	21. [CAB_RED] Cableado de Red.
COMUNICACIÓN AUXILIAR	22. [COM_NANO] Comunicación virtual por medio de Nano Station.
INSTALACIONES	23. [LOCAL] Local del GAB MUNICIPAL DEL CANTON VENTANAS.
	24. [GAB_R] Gabinete de Red
PERSONAL	25. [ING_SIST] Ingeniero en Sistemas.
	26. [TEC_SOPOR] Asistente: Soporte Técnico.
	27. [ING_CIVIL]Ingeniero Civil.

Tabla 1 Identificación de activos

Fuente: el autor

Según el análisis inicial de la tabla 1 “identificación de activos” el departamento cuenta equipamiento informático capaz de cumplir con los requerimientos respectivos de una infraestructura de red, prevención de daños por fallos o faltas repentinas del suministro eléctrico mediante un UPS que puede proporcionar y almacenar energía.

Los demás activos a analizar serán los servidores torre y en rack, de modo que se compruebe su aprovechamiento y cumplimiento respectivo de normativas para estimar su nivel de aprovechamiento protección y confiabilidad.

Los servidores existentes en el mercado son de dos tipos según su aspecto físico, Servidor torre tratándose de un ordenador con la forma típica de un gabinete “minitorre” el segundo tipo es el de un servidor de bastidor “rack”, este último es de un diseño Slim (delgado) especial para ser colocado de manera horizontal o vertical dependiendo del modelo en un estante / rack, sin embargo, ambos cumplen con la misma función. Según (Torres, 2017) “su principal objetivo es proveer recursos útiles para los usuarios, tales como almacenamiento web, de e-mail, protección de datos, entre muchos otros”.

Mediante el método de observación de campo se evidencia que existe hardware de un servidor Rack ubicado en el escritorio principal del jefe del departamento de TIC, no obstante, mediante la técnica de la entrevista se logró conocer que también cuentan con un servidor torre bajo el escritorio ubicado en el suelo, ambos hardware de servicios están dedicados al “almacenamiento de datos”.

Aunque el hardware cumpla con su función principal debido a la exposición podría presentar inconveniente causados por eventos no intencionales por parte de quienes laboran en el departamento, o intencionales por personal no autorizado, debido a la ubicación del departamento acceden a la oficina empleados del municipio en cualquier horario por motivos de que el acceso al departamento es libre y no existe restricción.

El hardware dedicado a prestar servicios cuenta con un SO para servidores comprado a la empresa Microsoft. El cual según (Carrera, 2018) se encarga de "gestionar la memoria y archivos del ordenador o coordinar la comunicación entre hardware". De modo que sea reconocida cada una de sus partes, los instalados son:

- Servidor torre: Windows server 2003
- Servidor Rack: Windows server 2012 R2 Standard

El Servidor torre que cuenta con Windows server 2003 presta sus servicios al sistema catastral Rural, sin licenciamiento por lo que el sistema ha sido activado mediante un crack o mayormente conocido como un parche, su utilización no es continúa sin embargo debe permanecer encendido si llegase a ser necesario su uso.

El servidor Rack o por sus siglas en ingles Rack Server que cuenta con Windows server 2012 presta servicios al sistema catastral Urbano, como se menciona anteriormente presta servicios de almacenamiento de datos en los que almacena y proporciona información a sus respectivos clientes, aunque este sistema operativo cuenta con una licencia original.

Es necesario conocer las diferencias entre ambos servidores de modo que se conozca las razones por la que se desea establecer un solo hardware dedicado a prestar el servicio de "almacenamiento de datos". Ver tabla 2

Dispositivos de hardware	Servidor Tower	Servidor Rack
Memoria RAM	1 GB	16 GB
Disco duro	300 GB	1 TB
Tipo	Torre (Tower)	Estante (Rack)
Procesador	Intel Core Duo 2.33 GHz	Intel Xeon 2.2GHz
Tecnología RAID	x	Raid 1

Tabla 2 Características físicas de los servidores Torre / rack

Fuente: el autor

Son notables las diferencias entre ambos servidores, no solo por su capacidad de lectura o almacenamiento, si no mas bien por ser un hardware potente el cual permite un mayor tiempo de encendido al poseer un procesador específico para servidores además de que cuenta con Windows server licenciado por lo que se puede aprovechar la tecnología RAID que contiene este equipo.

Existen estándares que brindan una guía para implementar un centro de datos o Data Center, aunque existen una variada conceptualización una forma de entenderlo (Narváez, 2016) menciona que "espacio físico adecuado para albergar varios recursos de las 'Tecnologías de Información' como almacenamiento, computo, red, entre otros, que brindan procesamiento de datos centralizados", de tal modo que al reconocer cuál sería su funcionalidad u objetivo este tendría una apreciación más clara de lo que se debería establecer en todo departamento tecnológico.

Uno de los propósitos de los Centro de Datos es aplicar medidas que permiten concentrar el área de trabajo y así cumplir con más de un estándar iniciando por su espacio. Según (Mullins, 2017) "independientemente del tamaño o de la actividad de la empresa, todos Centro de Datos tienen necesidades similares que incluyen proporcionar disponibilidad, rendimiento, fiabilidad y seguridad", siguiendo las directrices para quienes deseen diseñar e instalar un "Data Center" incluyendo los de tamaño para estructuras pequeñas.

Debido al progreso de las tecnologías surge una actualización hacia los estándares. Así como lo afirma (Villarubia, 2017) diciendo que "el Comité de Ingeniería de Sistemas de Cableado de Telecomunicaciones TR-42 de TIA ha aprobado el estándar TIA-942-B". Que entre sus cambios más importantes como inclusión de OM5 permitiendo un tipo de fibra, además de añadir la categoría 8 como un tipo de cable de par trenzado. Ver tabla 3

Requerimientos		Cumplimiento
1. Diseño y especificaciones del espacio del sitio		
Áreas funcionales	(ES) “Salas de entrada”	No cumple
	(PDA) “Área de distribución principal”	No cumple
	(HDA) “Áreas de Distribución Horizontal”	No cumple
	(EDA) “Área de Distribución de Equipos”	No cumple
	(ZDA) “Área de Distribución de Zona”	No cumple
	Backbone y cableado horizontal	No cumple
2. Infraestructura o estándares de cableado		
Resumen de sus áreas funcionales	“Estándar de la Infraestructura de cableado” - TIA-568	Si cumple
	“Estándar de la Infraestructura de cableado” - TIA-569.	No cumple
3. Estimación de los niveles de fiabilidad		
Niveles de fiabilidad	TIER 1 “básico”	No cumple
	TIER 2 “componentes redundantes”	No cumple
	TIER 3 “mantenible de forma concurrente”	No cumple
	TIER 4 “tolerante a fallas”	No cumple
4. Consideraciones eléctricas y ambientales		
Suministros eléctricos	Arquitectura	No cumple
	Energía eléctrica	Si cumple
	Especificaciones de sistemas informáticos	
Enfriamiento	Supresión de fuego	No cumple
	Niveles de humedad	No cumple
	Temperaturas	Si cumple

Tabla 3 Análisis de requerimientos norma TIA-942

Fuente: El autor

Las especificaciones del TIER que se pretende alcanzar depende de los recursos económicos disponibles, debido a las dimensiones del departamento el modelo ideal para construir en las bases de la oficina de TIC es el TIER 1. Según (Revuelta, 2016) contiene un “único camino para energía y sistema de enfriamiento, sin redundancia”, centralizando el área de los dispositivos de energía, almacenamiento o de telecomunicaciones.

Ya se ha mencionado que los equipos del departamento están en sitios diferentes a los que deberían estar según las especificaciones por parte de las normas, la razón de aquello es que el departamento es pequeño, es decir, las especificaciones del espacio como: sala de entrada, área de distribución entre otras, son la misma oficina.

Los estándares del cableado corresponden a la ANSI/TIA/EIA-568 en su asignación o protocolo más conocido como T568B, designado para el cableado de las telecomunicaciones dentro del edificio, abordando los tipos de cables, la base o el límite de las distancias, así como también los conectores.

La estructura que cubre al cableado es un gabinete elaborado con materiales de madera, además de estar al costado de cierta estructura producida por las escaleras y que se dirigen al techo en la cual caen residuos de agua producto de la tubería residual de agua de los aires acondicionados del edificio y que en cierto tiempo empieza a gotear.

Los dispositivos de red finales o intermedios son mejorados en lo que trascurre el tiempo, esto ocasiona que los estándares ya sea del cableado o de las estructuras de los mismos se actualicen según las nuevas especificaciones. Muchas de esas mejoras están enfocadas a la calidad y a la velocidad de las comunicaciones, si el cableado es antiguo y el dispositivo exige mayores prestaciones el conector formaría un cuello de botella al menos que se lo reemplace.

Los puntos reconocidos en la tabla 3 representan el objetivo de converger las tecnologías para que funcionen en una sola área, el almacenamiento o computo puede ser administrado por un servidor así mismo en lo que corresponde a la red puede tratarse del cableado estructurado, con un suministro de energía lo suficientemente potente y confiable capaz de prevenir el apagado brusco de los equipos en caso de fallos del suministro eléctrico.

Se puede cumplir a gran medida las recomendaciones ya que el cableado estructurado se encuentra ubicado en un espacio en el cual podrían ubicarse los demás recursos de un Data Center, sin embargo, esta estructura implementada para cubrirlo es un agravante a cierta consideración ambiental que requiere la supresión del fuego.

Para obtener un área segura para estos equipos se debería reemplazar la vieja estructura de madera y por un gabinete que contenga puertas laterales con cerraduras de modo que se pueda proteger a un armario rack, es por eso que al ya poseer un servidor rack los costos de su implantación se verán reducidos considerablemente, ya que el sitio que sirve para "almacenar la información" es tan importante como la "información misma".

El requerimiento de enfriamiento es cumplido parcialmente, aunque no sea lo adecuado se comparte el suministro de aire acondicionado del departamento, así se puede que los equipos sufran un sobrecalentamiento. La razón de este esquema es para representar gráficamente que al implementar un Data Center debe realizarse una planeación estratégica con el proposito de que los recursos sean aprovechados, además de prevenir daños a su estructura instalando un sistema enfriamiento adecuado para la los equipos instalados.

En los centros de datos la disponibilidad es un representativo de calidad, por motivo de que las entidades disponen de información requerida para sus negocios con una continuidad conocida como "27/7". "24 (veinte cuatro) horas de los 7 (siete) 'días de la semana', aparte esta información debe estar en espacios óptimos para que no haya ninguna interrupción tanto física como algún atacante a dicha información" (Ramos, 2017).

El análisis realizado es necesario para validad la importancia de aplicar estándares. Los cuales, según (Rico, 2015) afirma que "forman 'parte de la estructura' específica de una gran empresa y sólo utilizan el hardware para su propio negocio o bien tienen una línea de negocio en la que también alquilan alojamiento web", una normativa o estandarización puede ser aplicada luego de exponer los detalles de su utilidad.

Las entidades públicas o privadas manejan información que en la actualidad representan un flujo de datos digitales que se transmiten a través de una red interna/externa llamada un sistema de comunicación. Así como lo afirman (Garcia Teodoro, Diaz Verdejo, & Lopez Soler, 2014) “el conjunto de elementos y dispositivos involucrados en la transmisión de información entre dos puntos remotos”. Por tal motivo la trasmisión de esta información debe estar centralizada en un sitio en el cual se pueda controlar su tráfico además de brindar la seguridad necesaria.

Actualmente a la **información** se la considera un **activo** más para las **organizaciones** ya que su manejo, interpretación e integridad de la misma son de vital importancia para quien la posea. Según (Gonzales, 2015) afirma que: “la información es un recurso vital para toda organización y el buen uso de ésta puede significar el “éxito” o el “fracaso” para una empresa”.

La información en la actualidad está siendo creada procesada y visualizada digitalmente gracias al avance tecnológico, volviéndose un requisito para la construcción de una empresa, ya que esta necesita de tecnóloga e información para lograr sus metas, según (López, 2014) “Actualmente es casi imposible encontrar una empresa que por muy pequeña que sea no disponga de ordenadores o de algún tipo de máquina”.

Aunque los datos que se alberga pueden o no pertenecer a un producto con fines lucrativos, esta contiene datos sensibles que deben ser protegidos e inalterados, ya que un cambio en sus valores podría significar perdidas significantes para la organización.

La **Convergencia entre tecnología e información** para empresas, aunque por muy pequeñas que sean utilizan tecnología “hardware y software” para administrar su información sin embargo no está garantizada la administración segura de los datos.

Para que una institución alcance el éxito las labores que realiza, debe conocer que conseguir esa meta ya no depende del como una persona maneje sus recursos materiales, volviendo más importante el aprovechar los datos que se encuentren archivados en medios físicos (tangibles) o digitales (intangibles).

Así como el éxito de una organización depende de la forma en la que se administra la información su fracaso este sujeto al mismo objeto, es decir si no se protege la información esta podría ser utilizada con fines malignos y ocasionar un grave daño a la organización o hacia una persona cuya información haya sido alterada entiéndase como "eliminación" o "modificación" no autorizada.

La información creada en medios físicos puede ser vistas por quien tenga acceso al área en donde este ubicado el documento, por lo tanto, existe la posibilidad de que incluso personas no autorizadas accedan y visualicen y extraigan la información que se busca proteger, de modo que el almacenamiento digital en cierto punto es más seguro.

La "**norma ISO/IEC 27001"** fue desarrollada, de modo que se permita establecer un número de controles destinados a reducir los riesgos de la seguridad además de poder certificar organizaciones o un cierto número de procesos que podrían ser certificables. Por otra parte, está la norma "ISO/IEC 27002" la cual está basada en un guía de recomendaciones o buenas prácticas, es decir, para lograr una certificación se deben sus controles, ya que ambas normas están destinadas a ser usadas de forma complementaria.

No todos sus controles deben ser cumplidos ya que la organización debe priorizar y optar por aquellos controles que se alineen a sus estrategias, además debe tener en cuenta la capacidad presupuestaria por ser aplicables a organizaciones de diferente índole, es decir fines lucrativos o no, de variado tamaño; ("pequeña", "mediana", "grande"), de diferentes tipos: ("público", "privado").

Al seguir **las normas que protegen la información** son fundamentales para toda organización, el SGSI tiene 3 objetivos principales, que en el mundo tecnológico son conocidos como "la triada CID", confidencialidad, integridad y disponibilidad, todas ellas referentes a la información.

La información en la web permite aprender mucho sobre estas normativas sin embargo los detalles a conocer de la ISO/IEC 27001 es que contiene 114 controles, 14 de ellos son dedicados a la seguridad, mientras que la norma ISO/IEC 270002 contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios, el análisis de buenas prácticas será dirigido mediante los siguientes controles:

- Dominio 1 "políticas de seguridad"
- Dominio 2 "organización de la seguridad de la información"
- Dominio 3 "gestión de activos"
- Dominio 5 "controles de acceso"
- Dominio 7 "seguridad física y del entorno"
- Dominio 12 "gestión de incidentes en la seguridad de la información"

CONTROLES DE BUENAS PRACTICAS ISO/IEC 27002-2013	CUMPLIMIENTO
CONTROL 5 DOMINIO 1: "POLÍTICAS DE SEGURIDAD"	
Dirección de gestión	
Documentos de política	NO CUMPLE
Revisado de la política	NO CUMPLE
CONTROL 6 DOMINIO 2: "ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION"	
Organización interna	
Compromiso encaminado a la Dirección	NO CUMPLE
Coordinación	NO CUMPLE
Asignación de responsabilidades relativas al seguimiento	SI CUMPLE

Proceso de autorización de recursos para tratar la información	SI CUMPLE
Acuerdos de confidencialidad	SI CUMPLE
Ordenadores portátiles y teletrabajo	
Ordenadores portátiles y comunicaciones móviles	SI CUMPLE
Teletrabajo	NO CUMPLE
CONTROL 7 DOMINIO 3: "GESTIÓN DE ACTIVOS"	
Responsabilidad sobre los activos.	
Inventario de activos.	SI CUMPLE
Pertenencia de los activos.	SI CUMPLE
Uso tolerable de los activos.	SI CUMPLE
Categorización de la información.	
Directrices de clasificación.	SI CUMPLE
Etiquetado y manipulación de la información.	NO CUMPLE
Control 9 Dominio 5: "CONTROL DE ACCESO"	
Requisitos de negocio	
Política de control	NO CUMPLE
Gestión de acceso	
Registro de nuevos usuarios.	SI CUMPLE
Gestión y asignación de roles o privilegios.	SI CUMPLE
Gestión de contraseñas.	SI CUMPLE
Responsabilidades de usuario.	
Uso de contraseñas.	SI CUMPLE
Equipo de usuarios sin atención	SI CUMPLE
Política de escritorio despejado y pantalla limpia.	SI CUMPLE
Acceso controlado al sistema operativo y aplicaciones	
Seguridad al iniciar sesión	SI CUMPLE
Autenticación de usuario.	SI CUMPLE
Uso de los recursos del sistema.	SI CUMPLE
Desconexión automática	NO CUMPLE
Limitación del tiempo de conexión.	NO CUMPLE
Restricción del acceso	SI CUMPLE

Reclusión de sistemas sensibles.	SI CUMPLE
CONTROL 11 DOMINIO 7: “SEGURIDAD FÍSICA Y DEL ENTORNO”	
Espacios seguros	
Perímetro de “seguridad "física”	NO CUMPLE
Controles “físicos de entrada”	NO CUMPLE
Seguridad de instalaciones.	NO CUMPLE
Protección contra amenazas	NO CUMPLE
Seguridad del hardware	
Instalación y protección del hardware	NO CUMPLE
Seguridad del cableado.	NO CUMPLE
Mantenimiento de los equipos.	SI CUMPLE
CONTROL 16 DOMINIO 12: “GESTIÓN DE INCIDENTES”	
Mejoras de la seguridad	
Notificación de eventos	NO CUMPLE
Notificación de puntos débiles	NO CUMPLE
Responsabilidades y procedimientos.	SI CUMPLE

Tabla 4 Verificación de cumplimiento de los controles ISO/IEC 27002-2013

Fuente: http://www.criptored.upm.es/descarga/NuevasVersionesISO27001eISO27002.pdf

Después de un breve análisis a los literales propios de cada control se logra comprenden a simple vista que no se esta protegiendo debidamente a el activo de la información. El principal factor es el acceso sin restricción ya que el área no es segura y todos los esfuerzos por proteger el acceso a la red o los sistemas estarían quebrantados por la facilidad en la que un atacante podría acceder a los equipos. Según (Estelella, 2018) “Desde el punto de vista de la seguridad, "Es difícil, o imposible, saber dónde hay copias de los datos (“adiós a los secretos”) o qué copia es la buena (“adiós a la integridad”)”.

Se aplica gran parte de las directrices del octavo control el cual trata la gestión de activos sin embargo seria una buena practica realizar un etiquetado en modalidad de alerta (“peligro”, “no tocar”, etc.), que sirva de información a quien acceda al departamento además con esto se cumpliría a la totalidad de este control.

El jefe del departamento de TIC es quien administra los equipos tecnológicos, gestiona el acceso lógico de los usuarios como su creación o asignación de privilegios y responsabilidades del mismo. Para realizar las configuraciones o agregar nuevos valores debe ser mediante la manipulación los datos a través del SGBD.

Mediante la entrevista se conoció que han existido reclamos de usuarios que han realizado sus pagos sin embargo no constan en la base de datos, aunque estos inconvenientes han sido solucionados, el origen de tal hecho no es registrado ni proporciona notificaciones debido a las falencias del software catastral, evitando tener datos historias de las actualizaciones o errores del mismo.

Para realizar las configuraciones necesarias el acceso solicitado fue el de **interactuar con el SGBD** “Sistema gestor de base de datos”, esta interacción es directa hacia el servidor aplicando correctamente el control de acceso al SO mediante los procedimientos seguros para iniciar sesión e identificar y autentificar al usuario.

Al considerar la capacidad del software de sistema de ambos servidores se estima que tan solo un servidor es factible para una administración confiable sería la de “Windows server 2012”, el cual cuenta con una licencia original y no es activado mediante un parche, es así que al no existir riesgos o vulnerabilidades causados por un parche este brinda confiabilidad.

La elección de sistema operativo de ambos servidores no estuvo a la elección del jefe del departamento TIC por el hecho de que el software de catastro urbano y catastro rural fueron adquiridos mediante distintas empresas dedicadas al desarrollo de software, cada uno en desarrollado bajo la dirección de distintas administraciones.

Para acceder al sistema operativo de ambos servidores debe utilizarse un monitor, muse y teclados individuales, por lo que la utilización innecesaria de hardware reduce espacio de trabajo del jefe del departamento de TIC, debido a que no se aplica la gestión de despejar el puesto de trabajo, esto si bien es cierto, no es un inconveniente perjudicial sin embargo podría mejorar su práctica laboral accediendo de manera remota al SO.

Los controles son extensos y aplicarlos es complicado observando la situación actual del departamento de TIC, sin embargo, existen medidas como la seguridad activa o pasiva que pueden ser aplicadas para contrarrestar un parte de los inconvenientes. Aunque ya se hayan aplicado ciertas medidas tanto en el hardware y el software deben seguirse ciertas reglas no solo para protegerlos si no para tener mayor facilidad laboral

La seguridad activa básicamente trata de prevenir y evitar daños a “sistemas informáticos” sean estos hardware, software o de red, los primeros mecanismos aplicados son los del controlar el acceso al espacio en donde se sitúen los equipos. Además (Javier, 2018) afirma que “el uso de contraseñas seguras, asimismo es recomendable encriptar la información para que terceras personas no puedan tener acceso a ella”.

Posterior a las implementaciones de una o varias medidas dedicadas a la protección física es necesario poner a consideración que existe una fuerte referencia hacia las instalaciones seguras. “Los locales en donde se ubiquen los ordenadores que contienen o acceden a los ficheros o datos más prescindibles de la organización deben ser tener una “protección especial” cualquiera que sea su contenido” (Vieltes, 2014).

Si bien es cierto la seguridad pasiva, aunque en principio es conocida como un complemento de la activa. Según (Javier, 2018) "ayuda a "minimizar" el impacto de un daño informático provocado por un usuario o un accidente", un ejemplo de ejecutarla es la de realizar copias seguras para preservar, proteger y evita perder datos que se modificaron por un usuario y desee recuperarse en un futuro.

El análisis de los controles proporciono información necesaria para conocer que el acceso de los empleados a los departamentos no está sometidos a un control o normativa, es decir pueden acceder empleados sin restricción alguna, lo cual se evidencio mediante se ejecutaba la entrevista y se logró observar que varios trabajadores accedían al área libremente.

Cualquier institución, ya sea de índole público o privado podría exponer sus sistemas de información, además de su infraestructura tecnológico, estas amenazas pueden causar una variante a la información o daños hacia su infraestructura.

Existen diferentes conceptualizaciones para el termino riesgo, mientras que en informática se describe como riesgo es igual a vulnerabilidades por amenazas, por otra parte, al no existir "amenaza" o "vulnerabilidad" no hay riesgos". Sin embargo, las amenazas están en auge y al tener información rápidamente accesible y aprender a vulnerar medios digitales brindando herramientas que hacen el trabajo más fácil para el o los atacantes.

Los estándares se seguridad son un proceso en el cual interfieren personas. Así lo afirma (Smaldone, 2017) "la seguridad no es un producto, sino un proceso, no basta la adquisición de equipamiento (hardware) y de programas (software), ni siquiera la correcta implantación de éstos en el ámbito organizacional". Es necesario concientizar desde el personal administrativo hasta los de servicio de su importancia.

La verificación del cumplimiento de uno o varios estándares permite conocer el estado actual de la institución, iniciando por su manera de administrar sus recursos tanto físicos como lógicos, de modo que al llegar conocer que el activo de la información es esencial para la organización este debe protegerse y administrarse de una manera correcta, siguiendo las reglas que proporcionan los estándares ya que especifican el cómo utilizar estos medios posteriormente el como protegerlos y con ello a su información.

Es necesario que todo empleado de la empresa conozca las limitaciones de acceso a ciertas áreas. Así lo afirma (Vieltes, 2014) “las personas representan el eslabón más débil de la “seguridad informática”, a diferencia de los ordenadores, las personas pueden no seguir las instrucciones del modo en el que fueron dictadas”.

Aquellas medidas dedicadas a la seguridad que requieren el cumplimiento de ciertos estándares como ha sido analizado en el presente estudio se logró conocer una peculiaridad, y es que las amenazas que someten a los medios físico y digitales se ha encontrado que el único atacante es **el ser humano**.

Conclusiones

Como conclusión del análisis realizado en el departamento de TIC del GAD municipal del cantón Ventanas se obtiene lo siguiente:

- El nivel de amenazas externas o de origen ambiental se ven incrementadas al no cumplir con los requerimientos exigidos por los controles de seguridad física y del entorno.

- Se han implementado ciertas medidas para efectuar los requerimientos de los controles que preceden al nivel lógico como gestión de incidentes o controles de acceso protegiendo de cierta manera los datos que gestionan.

- Existe una clara desventaja al utilizar el servidor torre, debido a la escasez de características propias de un servidor, impidiendo un adecuado mantenimiento, además, los respaldos deben hacerse de forma manual, situación que no ocurre en el servidor en rack.

- Aunque la dificultad de proteger el medio físico es alta, existe la posibilidad reducir el riesgo mediante Data Center protegido con un gabinete con puertas y cerradura, su implementación no tendría costos elevados ya que se posee una parte del hardware necesario.

Bibliografía

Carrera, A. (02 de 16 de 2018). *Comprar Hosting*. Obtenido de Mejor sistema operativo para servidores: https://www.comparahosting.com/p/mejor-so-para-servidores/

Estelella, A. (13 de agosto de 2018). *El pais*. Obtenido de La máquina que nos cambió la vida: https://elpais.com/diario/2006/08/06/domingo/1154836353_850215.html

Garcia Teodoro, P., Diaz Verdejo, J. E., & Lopez Soler, J. M. (2014). *Transmision de datos y redes de computadoras.* Madrid: Pearson Educacion, S.A.

Gonzales, A. F. (8 de 12 de 2015). *Deusto, Facultad de ingenieria* . Obtenido de La informacion en las empresas: https://blogs.deusto.es/master-informatica/la-informacion-en-las-empresas/

Javier, G. R. (diciembre de 2018). *Universidad estatal del sur de Manabi.* Obtenido de Diseño de un plan estrategico de seguridad informatica: http://repositorio.unesum.edu.ec/handle/53000/1474

López, J. F. (2014). *Universidad Politecnica de Valencia.* Obtenido de Administracion de sistemas corporaticos basados en windows server : https://riunet.upv.es/bitstream/handle/10251/48152/CERD%C3%81N%20-%20Administraci%C3%B3n%20de%20Sistemas%20Corporativos%20basados%20en%20Windows%202012.%20Server%3A%20Protocolos%20de%20R....pdf?sequence=2

Lopez, J. T. (2014). *Repositorio Institucional Digital UNAP.* Obtenido de http://repositorio.unapiquitos.edu.pe/bitstream/handle/UNAP/4504/Jenny_Tesis_Titulo_2014.pdf?sequence=1&isAllowed=y

Mullins, M. (1 de 11 de 2017). *Fluke networks*. Obtenido de Estándares y pautas del centro de datos: https://es.flukenetworks.com/blog/cabling-chronicles/data-center-standards-and-guidelines

Narváez, D. N. (25 de noviembre de 2016). *Universidad San francisco de Quito.* Obtenido de Biblioteca Repositorio Digital: http://repositorio.usfq.edu.ec/bitstream/23000/6259/1/128452.pdf

P.Laudon, k. C. (2016). *Sistemas de informacion gerencial.* Mexico: Pearson Educacion de Mexico, S.A. de C.V.

Ramos, P. C. (22 de 04 de 2017). *ISSUU*. Obtenido de Informe ieee estándar tia 942 final : https://issuu.com/paulocesaralvisramos/docs/informe_ieee_est__ndar_tia_942-fina

Revuelta, M. G. (2016). *Doc Player*. Obtenido de TIA-942 Infrastructure Standard for Data Centers: https://docplayer.es/1257815-Tia-942-infrastructure-standard-for-data-centers.html

Rico, E. (5 de marzo de 2015). *Pasos para construir un data center*. Obtenido de https://otroespacioblog.wordpress.com/2015/03/05/pasos-para-construir-un-data-center/

Sampieri, R. H. (2014). *Metodologia de la investigacion* . México D.F.: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V.

Smaldone, J. (5 de 07 de 2017). *La seguridad no es un producto, sino un proceso*. Obtenido de Ambito.com: https://www.ambito.com/la-seguridad-no-es-un-producto-sino-un-proceso-n3988862

Torres, A. (2 de 9 de 2017). *Comprar hosting*. Obtenido de ¿Qué es un servidor y que tipos hay?: https://www.comparahosting.com/p/que-es-un-servidor/

Vieltes, A. G. (2014). *Enciclopedia de la Seguridad Informática. 2ª Edición.* Mexico, D.F.: Alfa Omega Grupo Editor, SA. de C.V.

Villarubia, C. (16 de 08 de 2017). *TIA actualiza su estándar de cableado para data center*. Obtenido de DcD Media: https://www.dcd.media/noticias/tia-actualiza-su-est%C3%A1ndar-de-cableado-para-data-center/

Anexos

Anexo 1. Guía de observación(ficha)

GUIA DE OBSERVACION

FICHA PARA GUÍA DE OBSERVACIÓN

Observador: Ernesto Israel Jimenez Vergara

Ubicación: GAD Municipal del Cantón Ventanas

Situación observada y contexto: Oficina del departamento TICS

Tiempo de observación: Observación de campo

1. INICIO DE LA ACTIVIDAD

	SIEMPRE	A VECES	CASI NUNCA	NO APLICA
¿Aplica controles de acceso?				x
¿Existe división de áreas?				x
¿Puesto laboral limpio o despejado?				x

2. DESARROLLO DE LA ACTIVIDAD

N.º	DESCRIPCIÓN	INTERPRETACIÓN
1	Acceso al departamento sin restricción	Se puede acceder al departamento sin restricción alguna además de no contar con una sala de espera aislada de todo equipo informático.
2	Limpiar el escritorio para poder colocar ordenador	El puesto de trabajo contaba con documentos como manual de usuarios solicitudes al departamento etc., además de tener a un costado equipo informático; un servidor rack. Dos monitores, 2 teclados2 dos mouses.
3	Ausencia de etiquetado de información	La sala no contiene etiquetado de información (carteles de peligro no tocar o documentos en los que se evidencia la palabra Confidencial).

4	Empelados del GAD Acceden para solicitar mantenimiento de uno de sus equipos	Un empleado de otra oficina accede al departamento para solicitar el mantenimiento de un ordenador, la solicitud es entregada y colocada a un costado del escritorio.
5	Observación detallada del área: - el área de mantenimiento podría ser cualquier espacio libre de la oficina - el almacenamiento material (tintas, hojas, herramientas), podría ser cualquier lugar en el que se pueda colocar. - fluido de agua proveniente de un espacio ocasionado por la ubicación de escaleras. - Una estructura de madera se encarga de ocultar o en teoría proteger al cableado estructurado. - Armario lleno de documentos cuyo responsables son el personal de talento humano (se comparte oficina para ese fin).	La división de áreas es inexistente, por lo que cualquier espacio desocupado podría servir para colocar herramientas o algún material, estos en ocasiones deben ser removidos para poder acceder al cableado estructurado el cual se encuentra dentro de una estructura de madera en la que a un costado existe una apertura cubierta con una puerta por la cual existe el goteo de fluidos de agua productos de los aires acondicionados del edificio, por ultimo se conoce que se comparte la oficina con otro departamento.
6	Ejecución del mantenimiento	El mantenimiento del ordenador solicitado anteriormente es realizado en un escritorio desocupado al costado de la puerta de la oficina.
7	En el trascurso de la entrevista se observan nuevos aspectos, control de acceso lógico y pantalla limpia)	Se aplica cierta protección al servidor de base de datos mediante autentificación de contraseña además de implementar control de pantalla limpia.
8	Luego de obtener información por medio de la entrevista se observa un ordenador oculto bajo el escritorio	El ordenador oculto resulta ser un servidor de torre el cual fue trasladado de la oficina de catastro a la oficina de TIC

Anexo 2. Entrevista

Entrevista realizada por estudiante de la universidad técnica de Babahoyo, técnica de recolección de datos que brindara información necesaria para estudio de caso como proyecto de fin de carrea.

Tiempo estimado de la entrevista: 30 minutos

Datos preliminares	
Investigador:	Ernesto Israel Jimenez Vergara
Entrevistado:	Ing. Cesar Varas Beltrán
Puesto:	Jefe departamental del área de Tecnologías de la información y comunicación TICS
Antigüedad en el puesto:	2 años
Lugar de la entrevista:	Oficina del departamento TIC, del GAD Municipal del Cantón Ventanas
Permisos:	Se me permitió tomar fotografías del departamento, pero no a realizar un video de la entrevista, por autorización del jefe del departamento.
Preguntas:	

1. **¿Existen políticas de control de acceso?**

   No existe una documentación en donde se hayan plasmado una política para ello, pero se trata de cubrir sus puntos mediante la creación de usuarios y asignación respectivas de privilegios para que accedan a los servicios del servidor.

2. **¿El servidor que se puede apreciar en el escritorio es el único en él departamento?**

   Es el único servidor Slim o en rack, pero existe otro que fue trasladado de la oficina de catastro y actualmente se encuentra bajo el escritorio debido al poco espacio con el que cuenta la oficina.

3. **¿Existe la probabilidad de que se utilice solo el Servidor Rack como único servidor de base de datos?**

   La visión original era aquella, pero debido a inconvenientes con el nuevo software implementado para los cobros catastrales no se ha realizado el cambio definitivo.

4. **¿La información que se genera o administra en el servidor ha sido vulnerada alguna vez?**

   No vulnerada mas bien al no tener el diagrama de la base de datos no se ha podido conocer que datos tomar o utilizar para el nuevo software catastral ocasionando inconvenientes con los usuarios que deseen realizar sus pagos, ya que no contaban en ocasiones en el sistema o los valores no eran coherentes.

5. **¿Quiénes tienen los permisos para acceder a los servidores?**

   Solo yo (afirma el jefe del departamento TIC), y si se encuentra un error o necesita un mantenimiento en el software y se necesite acceso a la base de datos solo el único administrador realizaría las operaciones.

6. **¿Qué tiempo se tarda en solucionar errores dentro de los sistemas que se administran en el departamento?**

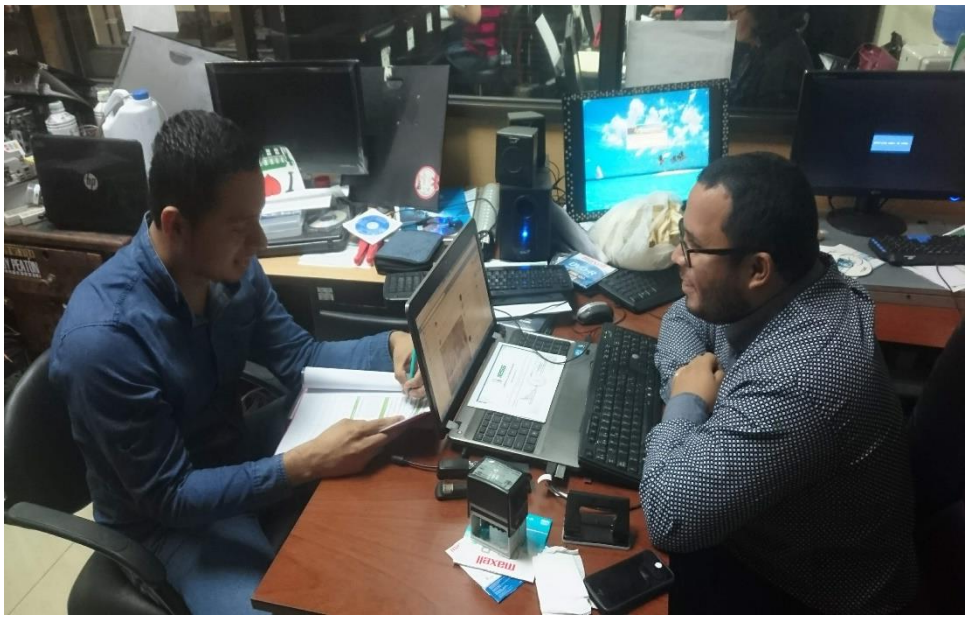
   En ocasiones se requiere de una colaboración externa si los errores dependen del nuevo software que se adquirió, además de que no presenta notificaciones o un historial de eventos, por otra parte, los demás sistemas no están centralizados y toda modificación consulta o actualización se realizan no se puede estimar.

7. **¿Con que sistema operativo trabajan los servidores?**

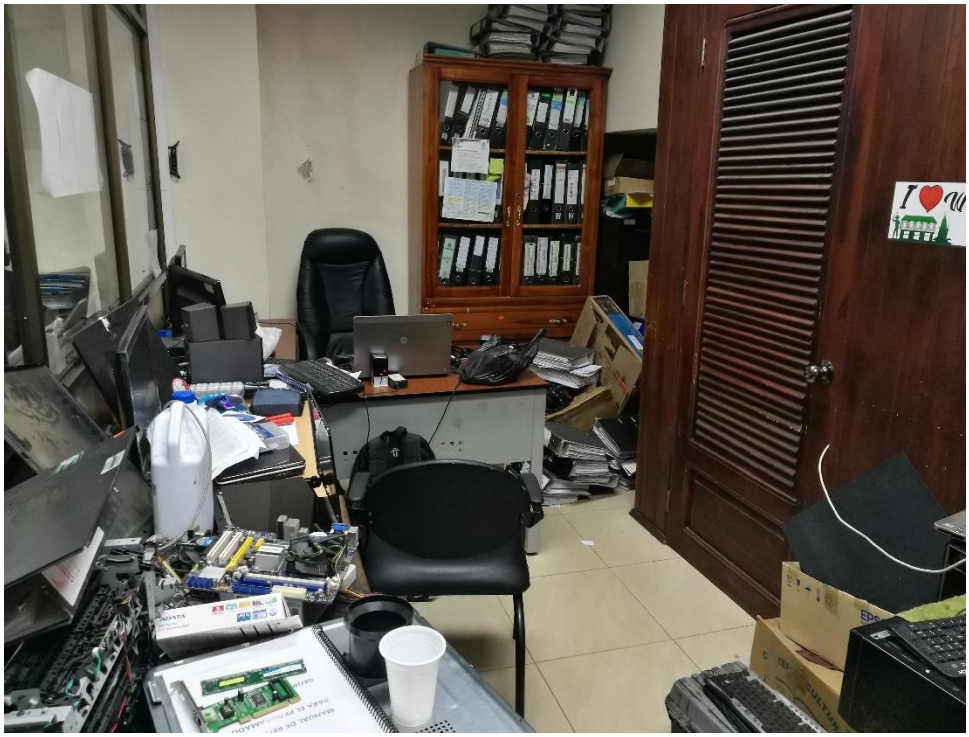
   Trabajan con Windows server, el servidor en rack tiene instalado Windows server 2012 más licencia, fue adquirido con el propósito de almacenar los datos del nuevo sistema catastral mientras que el servidor torre ya tiene mucho tiempo de funcionamiento y tiene instalado Windows server 2003, actualmente funcional, pero sin una licencia original.

   Anotación adicional: La base de datos que se administran en los servidores son manipuladas solo por el jefe del departamento, además la base de datos del biométrico es manipulada en una portátil utilizada solo para ello.

Anexo 3. Fotos del Servidor e infraestructura de red



Entrevista con jefe del departamento de TIC

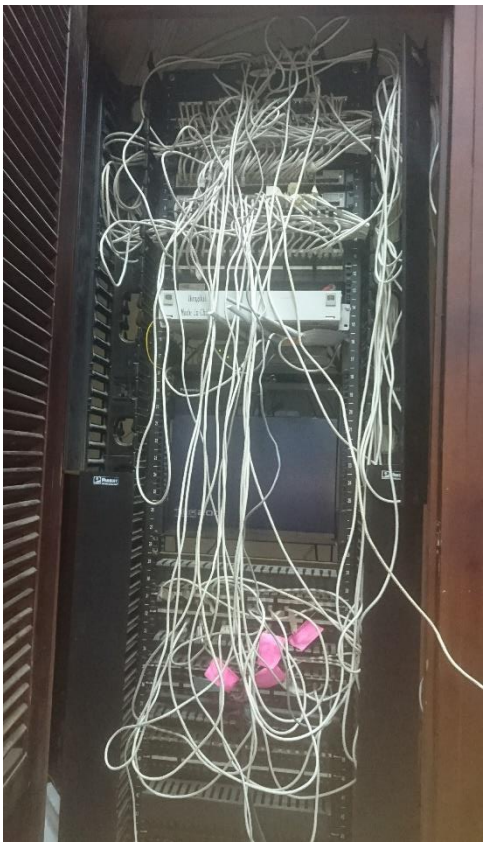


Departamento de TIC del GAD Municipal del cantón Ventanas

Servidor a un costado del escritorio del jefe del departamento de TIC del Gad Municipal del cantón Ventanas

(Izquierda)UPS para el servidor torre y en rack, (derecha) UPS para los equipos del cableado estructurado.

(Izquierda) Armario de madera que oculta el cableado estructurado, (Derecha) puerta de acceso hacia un hueco cuadrado desde el primer piso hasta el tercer piso de la Municipalidad.



Cableado estructurado dentro del gabinete de madera