UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

ARTÍCULO CIENTÍFICO

TEMA:

METODOLOGÍA DEL SGSI SEGÚN LA NORMA ISO/IEC 27001 PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE URCUQUÍ.

AUTOR: HENRY GEOVANNY VALENCIA FERNÁNDEZ

DIRECTOR: ING. EDGAR MAYA

Ibarra – Ecuador

2016

Metodología del SGSI según la norma ISO/IEC 27001 para el Gobierno Autónomo Descentralizado de San Miguel de Urcuquí.

Autores – Henry Geovanny VALENCIA FERNÁNDEZ, Ing. Edgar Alberto MAYA OLALLA

Facultad de Ingeniería en Ciencias Aplicadas, Universidad Técnica del Norte, Avenida 17 de Julio 5-21 y José María Córdova, Ibarra, Imbabura

hgvalencia@utn.edu.ec, eamaya@utn.edu.ec

Resumen. *El GAD Municipal de Urcuquí es una institución al servicio de la ciudadanía del mismo cantón, ofrece diversos servicios a personas civiles y otras instituciones gubernamentales, la red de datos debe ofrecer disponibilidad, integridad y confidencialidad en cuanto a seguridad.*

El presente trabajo tiene la finalidad diseñar e implementar un sistema de seguridad para la red de datos del GADMU, siguiendo las especificaciones del administrador de la red, se implementó un modelo de seguridad para proteger los servidores de bases de datos y registro de la propiedad, haciendo uso de un firewall cisco y basado en la Metodología del SGSI según la normas ISO/IEC 27001.

Este proyecto se llevó a cabo con los equipos tecnológicos la misma institución sin la necesidad de adquirir un equipo adicional, así se cuenta con el hardware y software necesario para diseñar e implementar este modelo de seguridad.

Palabras Claves

Disponibilidad, Integridad, Confidencialidad, Modelo y equipos de seguridad, ISO 27001, GADMU.

Abstract. *The "Gobierno Autónomo Descentralizado" from Urcuquí is an institution for the citizenship of this canton. They offer different services to civilians and other government institutions, the data network should provide availability, integrity and confidentiality in regards to security.*

This paper aims to desing and implement a security system for the data network of "Gobierno Autónomo Descentralizado" from "San Miguel de Urcuquí", following the specifications established by the network administrator, a security model was implemented to protect servers databases and property registration, using cisco-based firewall Methodology ISMS according to ISO/IEC 27001.

This Project was carried out with the technological equipment of the same institution, without the need to purchase additional equipment, so it has the necessary hardware and software to desing and implement this security model.

Keywords

Availability, Integrity, Confidentiality, Security model and equipment, ISO 27001, GADMU.

1. Introducción

El presente proyecto propone diseñar e implementar un sistema de seguridad para la red de datos del GADMU, minimizando amenazas que pueden darse tanto dentro como fuera de la red, este sistema se enfoca en brindar integridad, disponibilidad y confidencialidad. En el inicio del proyecto revisa los fundamentos teóricos en seguridad en redes y sobre la Metodología del SGSI basado en la norma ISO/IEC 27001, esta norma describe el procedimiento para diseñar e implementar un sistema de seguridad de red que es el PDCA.

En el segundo capítulo se procede a realizar el estudio y levantamiento de información sobre la situación actual de la red de datos del GADMU, tanto física como lógicamente, determinando así cuales son los puntos más de la red más vulnerables, y los riesgos presentes. Con la información recogida acerca del estado actual de la red de datos se procede a diseñar el modelo de seguridad de red usando el proceso que nos indica la norma, con la tecnología indicada y las políticas establecidas para los activos y empleados

Al concluir la implementación se realizaron las pruebas de verificación de funcionamiento del sistema y las indicaciones para mejorar el SGSI, al final se generaron recomendaciones para el mejoramiento del sistema de seguridad y las debidas conclusiones que se presentaron a lo largo de la ejecución del proyecto.

2. Norma ISO/IEC 27001

El estándar ISO/IEC 27001 se publica el 15 de Octubre del año 2005 por ISO e IEC que conforman una metodología para la estandarización universal. La norma principal de la

serie ISO 27000 contiene requisitos para la implementación del sistema de gestión de seguridad de la información.

El estándar proporciona un modelo que permite establecer, implementar, monitorear, revisar y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). El diseño e implementación del SGSI en una organización es influenciado por las necesidades, objetivos y requerimientos de seguridad, los procesos empleados, el tamaño y estructura de la organización. Este sistema se enfoca en los siguientes términos. [1]

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

2.1 Metodología SGSI

El Sistema de Gestión de Seguridad de la Información o SGSI es un proceso continuó, sistemático, documentado y conocido por toda la organización; aunque proporcionar un sistema completamente seguro es imposible, el propósito del SGSI es que los riesgos sean conocidos, asumidos, gestionados y minimizados por la misma organización.

El SGSI establece un ciclo continuó conocido por si siglas PDCA (Plan, Do, Check, Act), que es tradicional en los sistemas de gestión de calidad, este proceso mejora continuamente para que el sistema tenga un largo ciclo de vida. Como se indica en la figura 1. [1]

Figura 1. Modelo PDCA
Fuente: Norma ISO/IEC 27001. (2011). Obtenido de: *http://www.iso27000.es/download/doc_iso27000_all.pdf*

- ✓ ***PLAN*** **(planificar)** La planificación establece el alcance, políticas, objetivos, procesos y procedimientos del SGSI en términos de la organización, sus activos, tipo de tecnología a utilizar, se identifican los riesgos, amenazas y vulnerabilidades a los que se exponen los activos, y la asignación del propietario del SGSI.
- ✓ ***DO*** **(hacer)** Esta parte ejecuta el plan de tratamiento de riesgos para alcanzar los objetivos planteados, aquí se gestionan los recursos asignados al SGSI para el mantenimiento de la seguridad de la información implementando procedimientos y controles que permitan una detección y respuesta a los incidentes de seguridad.
- ✓ ***CHECK*** **(verificar)** La verificación se ejecuta para detectar a tiempo errores, identificar brechas, detectar incidentes, además de verificar si el alcance definido sigue siendo el adecuado y si las mejoras son evidentes, actualizando los planes de seguridad en base de las conclusiones generadas durante las actividades de revisión, es importante registrar las acciones y eventos que pudieran presentarse sobre la efectividad del SGSI.
- ✓ ***ACT*** **(actuar)** Realizar acciones preventivas y correctivas de acuerdo a las lecciones aprendidas de las experiencias propias y de otras organizaciones, comunicando las mismas a todas las partes implicadas en el SGSI, y plantear mejoras que alcancen los objetivos previstos. [1]

2.2 Seguridad en Profundidad.

La seguridad en profundidad son medidas de prevención que se aplican a diferentes capas del sistema de seguridad estas capas son las que se muestran a continuación en la figura 2 y se hacen referencia a las siete capas del modelo OSI. [2]

Figura 2. Modelo de Seguridad en Profundidad
Fuente: Norma ISO/IEC 27001. (2011). Obtenido de: *https://guardnet.files.wordpress.com/2011/06/capas-acciones.jpg*

3. Análisis y Evaluación de Riesgos.

El objetivo de realizar el análisis y evaluación de riesgos es determinar a los mismos con valores representativos para que sean tratados por la institución, esto permite identificar los activos más importantes y se indique el impacto del riesgo. [3]

3.1 Gestión de Riesgo de la seguridad de la información ISO/IEC 27005.

La ISO 27005 proporciona pautas para gestionar los riesgos en la seguridad de la información en una entidad, además de dar soporte al SGSI de la ISO 27001 así este sistema podrá ser implantado con satisfacción orientándose al análisis de gestión de riesgos, los componentes de esta norma se indican en la tabla 1. [1]

Propone	**El enfoque del proceso de gestión de riesgos de seguridad de la información.**
Evaluación	Valorar los riesgos mediante: ➢ Análisis del riesgo. ➢ Evaluación del riesgo.
Tratamiento	➢ Tratamiento del riesgo. ➢ Aceptación del riesgo.
Componentes adicionales	➢ Monitorización y revisión del riesgo. ➢ Comunicación del riesgo.

Tabla 2. Componentes de las Gestión de riesgos.
Fuente:http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

Esta sección evalúa los riesgos reconociendo los controles existentes en la organización, además se identifican, estiman y evalúan los activos, las amenazas y vulnerabilidades en el GADMU.

3.3 Metodología para el análisis de riesgos.

Metodología Cualitativa:

Es más usada en la toma de decisiones ya que es apoyada por su experiencia, dinamismo e intuición, la forma de clasificación de impactos es: Bajo, Moderado, Alto, y Crítico.En esta metodología cualitativa interaccionan 4 elementos que son: amenazas, vulnerabilidades, impactos y controles su ventaja es la compresión de lo que se está realizando. [4]

Metodología Cuantitativa:

Es una recolección de datos, realiza cálculos y usa técnicas de modelamiento que dan como resultado información difícil de estimar, además de hacer uso de escalas de valoración numérica. Para el análisis de riesgos en el GADMU se realizara uso de ambas metodologías, ya que por un lado se clasifican los atributos como indica el método cualitativo y junto con ello se lo valora numéricamente para representarlos con mayor exactitud. [4]

Valoración de Activos

La valoración de activos se realiza de acuerdo a los impactos tanto dentro como fuera de la red de datos y dependencias de estos hacia otros activos, para la evaluación de activos se usa los criterios de cualificación, se indica en la tabla 2, la norma ISO 27005 indica una valoración en el rango de 1-4 para describir el valor de cada activo. [4]

Valor	**Criterio**	**Descripción**	**Efecto**
1	Bajo	Inecesarios	Muy limitado en tecnología
2	Moderado	Poco necesario	Cierta capacidad tecnológica.
3	Alto	Necesario	Tiene capacidad tecnológica.
4	Crítico	Muy necesario	Capacidad tecnológica de última generación.

Tabla 2. Valoración de Activos.
Fuente:http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

Valoración de importancia activos

El producto de los valores obtenidos de cada parámetro identificados en la tabla 2 determinan la valoración de activos, que a su vez pertenecerán a un nivel de importancia, como indica la tabla 3, la norma ISO 27005 indica un rango valores para determinar la importancia de los activos en la organización. [4]

Ítem	**Rango de Valores**	**Criterio**	**Descripción**
1	1-8	Poco probable	Baja importancia
2	9-26	Importante	Importantes
3	27-64	Crítico	Muy importantes.
Valor del Activo = Dependencia * Funcionalidad * (Confidencialidad, Integridad, Disponibilidad)			

Tabla 3. Valoración de importancia de Activos.
Fuente:http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

Ocurrencia de Amenaza

Son valores numéricos calificativos utilizados para valorar la probabilidad de amenazas, como indica el estándar ISO 27005, la tabla 4 indica el rango de probabilidades de ocurrencia de amenazas en cuatro posibilidades. [4]

Valor	**Rango**	**Criterio**	**Descripción**

1	(0-25)%	Poco Probable	Muy baja probabilidad
2	(26-50)%	Medianamente Probable	Probabilidad baja
3	(51-75)%	Probable	Alta probabilidad.
4	(76-100)%	Muy Probable	Muy alta probabilidad

Tabla 4. Ocurrencia de Amenazas.
Fuente:http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

Valoración de impactos

Según la norma ISO 27005 la valoración de impactos mide la consecuencia de la materialización de un riesgo, además de ser el valor promedio entre los impactos de integridad, confidencialidad y disponibilidad, siendo así un punto muy importante al momento de tomar una decisión sobre los controles a utilizar, como muestra la tabla 5. [4]

Valor	Criterio	Descripción
1	Bajo	El impacto es mínimo.
2	Medio	El impacto es medio.
3	Alto	El impacto es alto.

Tabla 5. Valoración de Impactos.
Fuente:http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

Evaluación del riesgo

El producto entre la probabilidad de ocurrencia de una amenaza que indica la tabla 4 y la valoración de impactos de la tabla 3 da como resultado el nivel de valoración para la evaluación del riesgo, como se indica en la tabla 6. [4]

Rango de valores	Criterio	Descripción
1-2	Bajo	El riesgo del activo es bajo
3-4	Moderado	El riesgo del activo es moderado
5-8	Alto	El riesgo del activo es alto
9-12	Crítico	El riesgo del activo es crítico
Nivel de riesgo = Probabilidad * Impacto		

Tabla 6. Evaluación del riesgo.
Fuente:http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

Tratamiento de riesgos

Es la toma de decisiones frente a los diferentes riesgos, son la estrategia de la organización**,** la norma ISO 27005 nos presenta las siguientes opciones:

- **Reducir:** Consiste en elegir controles de conexión, eliminación, prevención, mitigación del impacto.
- **Aceptar:** No se implantan controles adicionales ya que la organización asume los daños.
- **Evitar:** O eliminar el riesgo, que no suele ser la mejor opción ya que en la mayoría de casos suele ser complejo costoso.
- **Transferir:** A un tercero de forma que se asegure el activo o subcontratarlo. [4]

Basado en las políticas actuales del GADMU (GADMU, 2016) las decisiones que se ejecutan son solo dos: Reducirlo o Aceptarlo, debido al costo que implica las otras dos opciones. Los riesgos serán aceptados cuando estos no afecten a las actividades de los funcionarios y en el caso contrario serán reducidos, como indica la tabla 7.

Criterio	Tratamiento
Bajo	ACEPTAR EL RIESGO
Moderado	
Alto	REDUCIR EL RIESGO
Crítico	

Tabla 7. Tratamiento del riesgo.
Fuente:http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

Prioridad en aplicación de controles

Basado en el estándar ISO 27005 El cálculo de la prioridad controles se realiza mediante el producto del valor de la importancia de activos en la tabla 3 y el rango de valores de la evaluación de riesgos en la tabla 6, aquí se determinan el rango de prioridad de aplicación de controles, como indica la tabla 8. [4]

Rango de Valores	Criterio	Descripción
1-13	Baja	Pueden esperar a ser implantados luego de los de media y alta prioridad.
14-23	Media	Pueden esperar a ser implantados luego de los de alta prioridad.
24-36	Alta	Deben ser implantados inmediatamente.
Prioridad en la aplicación de controles = Nivel de importancia * Nivel de riesgo		

Tabla 8. Prioridad de aplicación de controles.
Fuente:http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

Análisis de Riesgos

Es la identificación de los activos que dan valor a la institución, las amenazas que afecta al diario funcionamiento y el impacto que provoca la ocurrencia de alguna de ellas, en el análisis de riesgos los activos se clasifican en : Primarios y Soporte o Apoyo. [4]

Valoración de activos

Para la valoración de activos se hace uso de la tabla 2 "Valoración de activos" para calificar al activo en valores de dependencia, funcionalidad, confidencialidad, integridad y disponibilidad en donde el producto de estos valores da como resultado el valor del activo, este valor lo relaciona con la tabla 9 "Prioridad de aplicación de controles" para la aplicación de controles, tal como indica la norma ISO 27005. Un ejemplo de calificación de activos es la tabla 9, donde (C-I-D) es: confidencialidad, integridad y disponibilidad. [4]

Activo	Dependencia	Funcionalidad	C-I-D	Valor del activo
Servidor HP ProLiant DL380	4	3	3	36

Tabla 9. Ejemplo de calificación de activos.
Fuente:http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

Identificación de Vulnerabilidades y Amenazas.

En base a estudios de la norma ISO 27001 las vulnerabilidades son el principio para la formación de amenazas, esta identificación permite establecer una relación entre estas dos, dando conocer el origen de las amenazas y si estas se materializan que riesgos son los que se producen.

Las vulnerabilidades se relacionan directamente con las amenazas. La identificación de vulnerabilidades a consecuencia de las amenazas, naturales, físicas, humanas y organizacionales se realizaron mediante visitas técnicas a las instalaciones y entrevistas con el administrador de la red, la tabla 10 indica un ejemplo de identificación de vulnerabilidad y amenaza. [4]

Vulnerabilidad	Amenaza
No posee un plan de contingencia de recuperación de información en caso de desastres	Fenómenos Naturales

Tabla 10. Ejemplo de identificación de vulnerabilidades y amenazas.
Fuente:http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

Estimación del Riesgo

En la estimación del riesgo se asignan valores a las posibilidades y a las consecuencias de un riesgo, en este proceso se utiliza la valoración de la tabla 5 de "Valoración de impactos", determinando así la importancia en cuanto a confidencialidad, integridad y disponibilidad, como indica la tabla 11. Donde C (confidencialidad), I (integridad), D (disponibilidad). [4]

Amenaza	Vulnerabilidad	C	I	D	Impacto
Amenazas Naturales o Ambiental	No existe plan de recuperación	1	1	3	2

Tabla 11. Ejemplo de estimación del riesgo.
Fuente:http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

Valoración de incidentes

Para la valoración de incidentes se utiliza los criterios de la tabla 4 "Ocurrencia de amenazas" como indica el ejemplo de la tabla 12. [4]

Tipo de Amenazas	Vulnerabilidad	Amenaza	Probabilidad
Amenazas Naturales o Ambientales	No existe plan de recuperación	Fenómenos Naturales	2

Tabla 12. Ejemplo de valoración de incidentes.
Fuente:http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

Evaluación de riesgos.

Para la evaluación de riesgos se identifican los activos críticos, con sus vulnerabilidades y se los califica en valores de confidencialidad, integridad y disponibilidad haciendo uso de la tabla 5 "Valoración de impactos", luego el promedio de estos tres valores nos arroja el valor del impacto, a partir de ese punto se califica la probabilidad de ocurrencia de amenazas hacia el activo según la tabla 4 "Ocurrencia de amenazas", al final el nivel del riesgos es el producto entre el valor del impacto y la probabilidad de amenazas como indica la tabla 6 "Evaluación del riesgo", determinando así el tratamiento a seguir, según la tabla 7 "Tratamiento del riesgo". La tabla 13 indica a continuación un ejemplo para este proceso. Donde C (confidencialidad), I (integridad), D (disponibilidad) [4]

Tipo de Amenaza	Amenazas Naturales o Ambientales

Vulnerabilidad	No posee plan de contingencia de recuperación de información en caso de desastres
C	1
I	1
D	3
Impacto	2
Probabilidad	2
Nivel de Riesgo	4
Tratamiento	Aceptar

Tabla 13. Ejemplo de evaluación de riesgos existentes

Fuente: Información extraída del GADMU.

4. Diseño e Implemetación Del SGSI

El diseño e implementación del SGSI consta en la elaboración de los objetivos de control que indica la norma ISO 27001 para establecer politica y procedimientos de seguridad, que se enfocan en los intereses de la institución.

4.1 Objetivos de Control.

Los objetivos de control son una guía que permiten determinar un proceso para prevenir, proteger y manejar los riesgos debido a diferentes daños, en esta parte nos da la flexibilidad en elegir los objetivos que se acoplen al alcance del sistema, a continuación se lista los controles y objetivos de control. [1]

Politica de Seguridad

Es el objetivo de control que engloba a los demás, este se presenta como una guía para salvaguardar la información de la organización además de abarcar el cumplimiento de los demás objetivos de control, describiendo que se puede hacer o no dentro del GADMU [1]

Gestión de Activos

La gestión de activos abarca artículos sobre la asignación de responsables para cada activo, los cuales deben realizar acciones de almacenamiento, respaldo y controles continuos sobre estos activos, además de notificar novedades o problemas a los responsables del sistema de seguridad. [1]

Seguridad de Recursos Humanos

La seguridad de recursos humanos se enfoca en la capacitación de trabajadores que van a integrarse a las labores dentro del GADMU con el fin de que sean capaces de desarrollar su trabajo junto con el SGSI. [1]

Seguridad Física y Ambiental

La seguridad física y ambiental se refiere a las instalaciones y condiciones del ambiente dentro del edificio del GADMU, como lo son: puestos de trabajo, equipos del data center, y la seguridad física como: puertas cerradas, cámaras de vigilancia y personal de seguridad. [1]

Gestión de Comunicaciones y Operaciones

La gestión de comunicaciones y operaciones son los procesos a seguir para la adquisición de nuevos equipos tecnológicos para el GADMU, designando a los responsables de autorizar y realizar este proceso. [1]

Control de Acceso

El control de acceso se enfoca al acceso de todos los trabajadores hacia los activos de la organización, ya sea mediante un usuario o contraseña u otro método de autenticación, además de los privilegio de acceso a ciertos equipos de telecomunicaciones. [1]

Gestión de Incidentes en la Seguridad de la Información

La gestión de incidentes en la seguridad de la información se enfoca a la verificación y corrección a tiempo de los equipos o sistemas que presenten problemas y reporte de estas al personal designado. [1]

Cumplimiento

Es la comunicación del SGSI a todos los funcionarios del GADMU, con el fin de evitar que alguno de ellos incumplan con las políticas de seguridad establecidas. [1]

4.2 Alcance del SGSI.

Este sistema tiene su alcance definido en la protección de los activos más valiosos de la institución, los cuales son los servidores de bases de datos y de registro, por medio de un equipo firewall cisco RV130, para cumplir el alcance la norma SGSI. Mediante la creación de mapas de redes y sistemas, se definen ubicaciones físicas de los elementos además de realizar diagramas organizativos como se india en la figura 4 y 5 respectivamente. [1]

Diagrama del alcance de redes y sistemas.

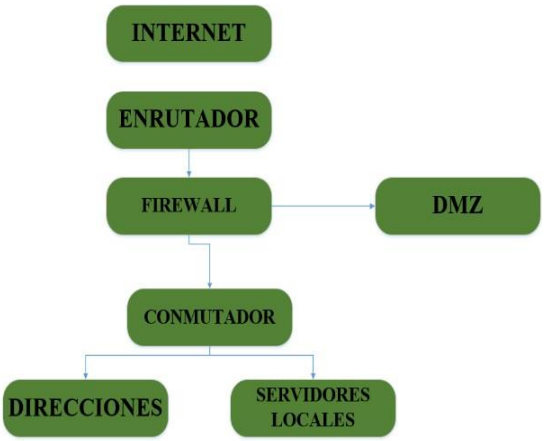


Figura 3. Alcance de rede y sistemas del SGSI
Fuente: GADMU. (2016). Elaborado por Autor

Diagrama del alcance Organizacional

Figura 4. Diagrama del alcance oranizacional del SGSI
Fuente: GADMU (2016)). Elaborado por Autor

4.3 Descripción Técnica del Sistema de Seguridad.

En la tabla 14 se indica de manera general el funcionamiento del sistema de seguridad para la red de datos del GADMU y las acciones que toma el sistema para filtrar tráfico a ciertas direcciones. [5]

Dirección IP	Descripción	Acción
172.16.0.12/16	La IP del administrador es la única que puede ingresar a realizar tareas de configuración en los servidores de Gestión Documental y Registro de la Propiedad por el puerto SSH que esta re direccionado al puerto 22016.	Aceptar
172.16.0.0 /16	Cualquier usuario de la red de datos del GADMU puede ingresar a los servidores de Gestión Documental y Registro de la Propiedad por el puerto 80 (HTTP) para realizar tareas de consulta.	Aceptar
172.16.0.0/16	Si algún usuario quiere ingresar a los servidores de Gestión Documental y Registro de la Propiedad por otro puerto para configurar no lo puede hacer, excepto la ip de Administrador.	Denegar
172.16.0.0/16	Los usuarios no tiene restricciones para navegar en internet desde la red local, en cuanto a bloqueo de puertos	Aceptar
IP pública	Las restricciones desde el internet o desde una ip publican cualquier hacia la red local del GADMU; solo pueden ingresar a los servidores para realizar tareas de consulta como usuarios por el puerto 80 (HTTP).	Aceptar
IP pública	Si desde una IP pública o desde internet quieren ingresar a los servidores de Gestión Documental y Registro de la Propiedad por algún otro puerto no lo pueden hacer.	Denegar
IP pública	Solo el administrador puede ingresar a los servidores de Gestión Documental y Registro de la Propiedad para configurarlos mediante el puerto SSH re direccionado al 22016.	Aceptar

Tabla 14. Funcionamiento general del SGSI.

Fuente: Información extraída del GADMU

4.4 Estructura de Red Implantada en el GADMU.

La implementación consta de un firewall Cisco RV130 el cual contiene todas las herramientas que se determina en el alcance, como son: VLAN, DMZ, y ACL para la protección de los servidores de bases de datos y registro de la propiedad, como se indica en la figura 5. [5]

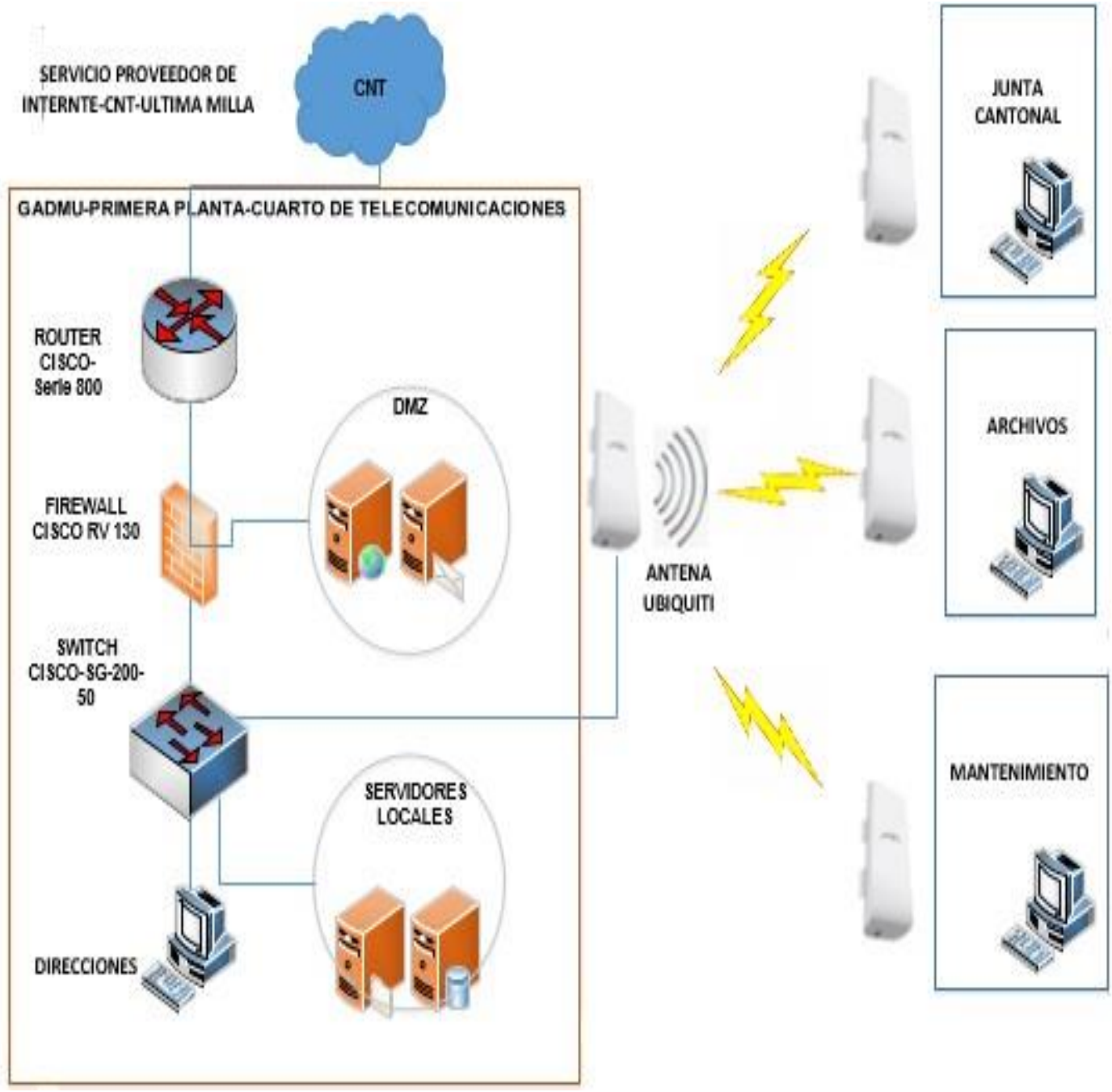


Figura 5. Estructura de red de datos implantada en el GADMU

Fuente: GADMU (2016)). Elaborado por Autor

4.5 Descripción de Herramientas Utilizadas.

Listas de Acceso.

Mediante ACL's se procede a permitir o denegar el acceso a los activos de la institución, ya que vamos a gestionar servicios se hiso uso de las ACL extendidas ya que con ellas gestionamos, puertos de comunicación, tipo de protocolo y direcciones IP ya son parámetros para filtrar el tráfico que circula tanto desde la red interna como desde la externa.

Las listas de acceso van de acuerdo con la política de seguridad para cumplir el proyecto, la estrategia principal para la protección de estos servidores es, que los trabajadores de la entidad solo puedan realizar actividades de consulta desde cualquier parte, y que solo el administrador tenga acceso total a estos servidores desde la WAN. [2]

Redes Virtuales VLAN.

Una LAN Virtual o VLAN, es un conjunto de dispositivos terminales que pertenecen a una red o subred lógica formando un solo dominio de broadcast independiente de su ubicación física en la red, no es importante que todos los equipos estén conectados al mismo switch o que los diferentes enlaces pertenezca a la misma VLAN. Las VLAN no pueden comunicarse entre sí ya que están separadas lógicamente aun que se encuentren conectadas en la misma red, ofreciendo un nivel de seguridad básico a lugares de la red que son restringidos

Las redes virtuales configuran para segmentar la red, por defecto el firewall cisco RV130 viene con 1 vlan para la red local, esta vlan se asigna interfaz física del dispositivo (fa0/1), al crear otra vlan para la DMZ esta se asigna a otra interfaz (fa0/2) como se muestra en la figura 6. [2]

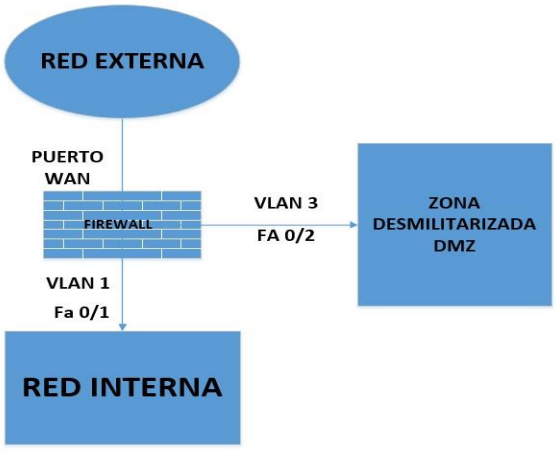
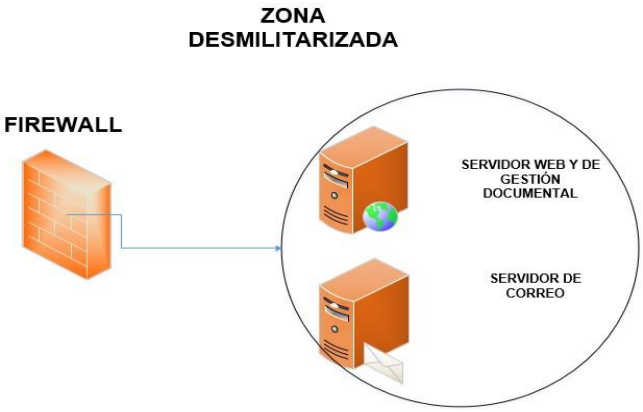


Figura 6. Esquema de distribución de red mediante Vlan's.
Fuente: GADMU (2016)). Elaborado por Autor

Zona Desmilitarizada.

La DMZ es el área destinada para los servidores de acceso público, es una subred detrás de un firewall en cual se pueden gestionar puertos para el acceso ya sea desde la LAN o la WAN. En la figura 7 se indica como ubicar la DMZ para los servidores. [2]

Figura 7. Representación de ubicación de la DMZ



Fuente: *https://norbertomn.files.wordpress.com/2014/02/curso-seguridad-en-informacion.pdf*

SSH

El protocolo SSH es un medio de comunicación seguro entre un cliente y un servidor ya que la información se encripta durante la transmisión, el protocolo SSH utiliza el puerto 22 para comunicarse, este protocolo ofrece confidencialidad e integridad, a continuación se indican algunas características. [2]

- ✓ **Integridad:** La información no es alterada por otras personas.
- ✓ **Autenticación:** Que los que participan en la comunicación son quienes dicen ser.
- ✓ **Confidencialidad:** Personas ajenas a la comunicación no puede leer la misma.
- ✓ **No repudio:** Si se envía un mensaje, este no debe rechazarse.
- ✓ **Rechazo de duplicados:** No deja enviar el mensaje si este se repite.

Firewall CISCO RV 130

El firewall CISCO RV 130 es un dispositivo que permite filtrar tráfico en una red de datos, este dispositivo contiene todas las características para implantar las herramientas que se mencionaron anteriormente.

Ademas de que es capaz de llevar una administración de servicios para toda la red en el sentido que se elija, este dispositivo fue facilitado por GADMU para llevar a cabo este proceso, en la figura 8 se indica el dispositivo. [6]

Figura 7. Firewall Cisco RV 130
Fuente:http://www.cisco.com/c/dam/en/us/td/docs/routers/csbr/rv130w/admin_guide/es/rv130w_admin_es.pdf

5. Resultados Obtenidos

Para apreciar de mejor manera los resultados obtenidos con este proyecto se procede a elaborar un cuadro sobre los impactos que se produjeron luego de la implantación de este sistema de seguridad, para ellos se realizó el análisis de la situación en la que se encontró a la red de datos, con la que se encuentra funcionando actualmente, como se indica en la tabla 15. [5]

SITUACIÓN ANTERIOR	**SITUACIÓN ACTUAL**
Políticas de seguridad desactualizadas, desconocidas y obsoletas debido a la falta de comunicación de las mismas a todo el personal.	La existencia de un manual de políticas de seguridad que se acoplan a las necesidades del GADMU, y que son conocidas por todos los trabajadores de la entidad.
Falta de organización de todos los implicados en la seguridad de la red para comunicar cambios en los sistemas de la misma.	Un diagrama organizacional que compromete a todos los implicados en comunicar cambios o mejoras en los sistemas de la red y en la toma de decisiones frente a los problemas que exista en la misma.
Desorganización y desconocimiento en los procesos que se lleva a cabo para la solución de problema de hardware o software por parte de los usuarios de los equipos terminales.	Proceso organizado y conocido por los trabajadores para brindar una solución eficaz a los problemas de hardware o software.
Falta de concienciación sobre la seguridad de la información para los nuevos trabajadores con los activos que manejaran durante sus labores.	Compromiso inicial de los trabajadores con la institución sobre las responsabilidades de cuidar los activos con los que trabajará.
Una red totalmente desprotegida a nivel lógico y deficiencias en su estructura con lo que se producen varios riesgos y vulnerabilidad en el sistema.	Una red más protegida y segmentada la cual filtra el trafico limitando el acceso a ciertos servicios disminuyendo riesgos y eliminando vulnerabilidades
La topología física de la red se encontraba con deficiencias en sus conexiones debido a la falta de conocimiento sobre seguridad en redes.	Una topología física más robusta y ordenada que distribuye de mejor manera los servicios a todos los usuarios.
Ninguna iniciativa sobre la implantación de algún sistema de seguridad, aún con el registro de un ataque de DoS sobre esta red.	Un sistema de seguridad basado en una norma internacional como los es la ISO 27001 la cual tiene un ciclo de vida continuo (PDCA) que mejora de acuerdo a las necesidades de la entidad.

Tabla 15. Impactos del SGSI en el GADMU.

Fuente: Información extraída del GADMU.

6. Conclusiones

- ✓ Mediante la norma ISO 27005 para el análisis y gestión de riesgos se determinaron los activos más importantes con altos niveles de riesgos que deben ser reducidos, dando como resultado el cumplimiento obligatorio de las políticas y procesos de seguridad de la información para efectuar esta acción.
- ✓ Las políticas y procesos de seguridad de la información van a cambiar con el transcurso del tiempo debido a las mejorar continua que la norma ISO 27001 para cumplan con los objetivos de la organización.
- ✓ Aunque las políticas y controles de seguridad de la información que se encontró en el GADMU no estaban totalmente documentadas sirvieron de base para establecer los nuevos controles de seguridad.
- ✓ Por medio de la metodología del análisis y gestión de riesgos ISO 27005 se establecieron los controles para reducir los riesgos existentes, que fueron arrojados en el análisis de estos, asegurando el funcionamiento del SGSI.
- ✓ En el análisis de riesgos se identifican el valor de los activos más importantes a ser protegidos, debido a que se encuentran propensos a sufrir algún daño, calificándolos en valores de dependencia,

función, confidencialidad, integridad y disponibilidad.

- ✓ Las mejoras en el SGSI van en concordancia con las actualizaciones del análisis de riesgos, identificando nuevas amenazas, vulnerabilidades y si los controles aún son efectivos para cumplir los objetivos de la organización.
- ✓ El beneficio de contar con un firewall cisco rv130 es, que el equipo tiene las propiedades necesarias para realizar las configuraciones de seguridad de la red de datos a nivel lógico.

Agradecimientos

Se extienda un especial agradecimiento al Gobierno Autónomo Descentralizado de San Miguel de Urcuquí por el apoyo brindado sobre este proyecto, especialmente al Ing. Mario Farinango encargado del Departamento de Sistemas quien facilito los recursos necesarios para la culminación de este trabajo.

Referencias

[1] ISO/IEC, «ISO/IEC 27005,» 30 Junio 2008. [En línea].Available:http://www.pqmonline.com/assets/files/lib/std/iso_iec_27005-2008.pdf.

[2] Cursos en Seguridad de la Información.,«Seguridad de sistemas delainformación,» 2010. [Enlínea].Available:https://norbertomn.files.wordpress.cm/2014/02/curso-seguridad-en-sistemasdeinformacion.pdf. [Último acceso: 1 Marzo 2016].

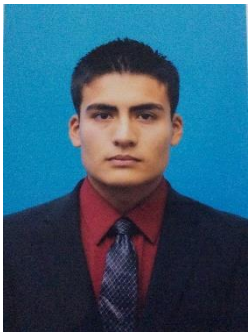
[3] ISO 27000, «ISO 27005-2008,» 30 Junio 2008. [En línea]. Available: http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf. [Último acceso: 1 Abril 2016].

[4] iso 27000, «Gestión de Riesgos tecnológicos basada en ISO 27005 para la continuidad de negocio,» 2011. [En línea]. Available: file:///C:/Users/HENRY/Downloads/Dialnet-GestionDeRiesgosTecnologicosBasadaEnISO31000EISO27-4797252%20(3).pdf. [Último acceso: 1 Abril 2016].

[5] I. M. Farinango, Interviewee, *Estado de la red de datos.* [Entrevista]. 1 Junio 2016.

[6] CISCO, «CISCO RV 130,» 2015. [En línea]. Available: http://www.cisco.com/c/dam/en/us/td/docs/routers/csbr/rv130w/admin_guide/es/rv130w_admin_es.pdf. [Último acceso: 1 Abril 2016].

Autores



Henry G. VALENCIA FERNÁNDEZ. Nació en Ibarra el 27 de Agosto de 1992 Realizó sus estudios primarios en la Escuela "28 de Septiembre" Los estudios secundarios los realizó en la Unidad Educativa Experimental "Teodoro Gomez de la Torre" donde finalizó en el año 2010, obteniendo el título de Bachiller en Ciencias Especialización Físico Matemático. Actualmente, está realizando su proceso de titulación en Ingeniería en Electrónica y Redes de Comunicación, Universidad Técnica del Norte – Ecuador.

Edgar A. MAYA OLALLA. Nació en Ibarra – Ecuador el 22 de Abril del año 1980. Ingeniero en Sistemas Computacionales en la Univerdad Técnica del Norte en el año 2006. Actualmente es docente de la Carrera de Ingeniería en Electrónica y Redes de Comunicación en la Universidad Técnica del Norte, Obtiene su Maestría en Redes de Comunicación en la Pontificia Universidad Católica del Ecuador en el año 2014 Quito- Ecuador.

Methodology of the ISMS according to ISO / IEC 27001 for the Decentralized Autonomous Government of San Miguel de Urcuquí.

Authors – Henry Geovanny VALENCIA FERNÁNDEZ, Ing. Edgar Alberto MAYA OLALLA

Facultad de Ingeniería en Ciencias Aplicadas, Universidad Técnica del Norte, Avenida 17 de Julio 5-21 y José María Córdova, Ibarra, Imbabura

hgvalencia@utn.edu.ec, eamaya@utn.edu.ec

Abstract. *The "Gobierno Autónomo Descentralizado" from Urcuquí is an institution for the citizenship of this canton. They offer different services to civilians and other government institutions, the data network should provide availability, integrity and confidentiality in regards to security.*

This paper aims to desing and implement a security system for the data network of "Gobierno Autónomo Descentralizado" from "San Miguel de Urcuquí", following the specifications established by the network administrator, a security model was implemented to protect servers databases and property registration, using cisco-based firewall Methodology ISMS according to ISO/IEC 27001.

This Project was carried out with the technological equipment of the same institution, without the need to purchase additional equipment, so it has the necessary hardware and software to desing and implement this security model.

Keywords

Availability, Integrity, Confidentiality, Security model and equipment, ISO 27001, GADMU.

1. Introduction

The present project proposes to design and implement a security system for the GADMU data network, minimizing threats that can occur both inside and outside the network, this system focuses on providing integrity, availability and confidentiality. At the beginning of the project, it reviews the theoretical foundations of network security and the ISMS Methodology based on ISO / IEC 27001, this standard describes the procedure for designing and implementing a network security system, which is the PDCA.

In the second chapter we proceed to study and collect information on the current situation of the GADMU data network, both physically and logically, thus determining which are the most vulnerable points of the network, and the present risks. With the information gathered about the current state of the data network, we proceed to design the network security model using the process indicated by the standard, with the indicated technology and policies established for the assets and employees

At the conclusion of the implementation, the system performance verification tests and the indications to improve the ISMS were carried out. In the end, recommendations were made for the improvement of the safety system and the necessary conclusions that were presented during the execution of the project.

2. ISO/IEC 27001 Standard

The ISO / IEC 27001 standard is published on October 15, 2005 by ISO and IEC that conform a methodology for universal standardization. The main standard of the ISO 27000 series contains requirements for the implementation of the information security management system.

The standard provides a model for establishing, implementing, monitoring, reviewing and improving an Information Security Management System (ISMS). The design and implementation of the ISMS in an organization is influenced by the needs, objectives and safety requirements, the processes employed, the size and structure of the organization. This system is focused on the following terms.[1]

- ✓ **Confidentiality:** Information is not made available or disclosed to unauthorized individuals, entities or processes.
- ✓ **Integrity:** accurate and complete maintenance of the information and its processing methods.

- ✓ **Availability:** access and use of the information and the systems of treatment of the same by the authorized individuals, entities or processes when they require it

2.1 SGSI Methodology

The Information Security Management System or ISMS is a continuous process, systematic, documented and known throughout the organization; Although providing a completely secure system is impossible, the purpose of the ISMS is for the risks to be known, assumed, managed and minimized by the same organization.

The ISMS establishes a continuous cycle known as PDCA (Plan, Do, Check, Act), which is traditional in quality management systems, this process continuously improves for the system to have a long life cycle. As indicated in figure 1. [1]

Figure 3. PDCA Model
Source: Standard ISO/IEC 27001. (2011). Obtained from: *http://www.iso27000.es/download/doc_iso27000_all.pdf*

- ✓ ***PLAN***.- The planning establishes the scope, policies, objectives, processes and procedures of the ISMS in terms of the organization, its assets, the type of technology to be used, the risks, threats and vulnerabilities to which the assets are exposed, and the allocation Of the owner of the ISMS.

- ✓ ***DO.-*** This part executes the risk management plan to reach the objectives set, here the resources assigned to the ISMS are managed for the maintenance of information security by implementing procedures and controls that allow detection and response to security incidents.

- ✓ ***CHECK.-*** Verification is executed to detect errors in a timely manner, identify gaps, detect incidents, and verify if the defined scope remains adequate and if improvements are evident, updating security plans based on the conclusions generated during the activities. Review, it is important to record the actions and events that could be presented on the effectiveness of the ISMS.

- ✓ ***ACT.-*** To carry out preventive and corrective actions according to the lessons learned from the own experiences and of other organizations, communicating them to all the parties involved in the ISMS, and to propose improvements that reach the objectives. [1]

2.2 Security in Depth

Security in depth are prevention measures that are applied to different layers of the security system. These layers are shown below in figure 2 and reference is made to the seven layers of the OSI model. [2]

Figure 2. Modelo de Seguridad en Profundidad
Source: Standard ISO/IEC 27001. (2011). Obtained from: *https://guardnet.files.wordpress.com/2011/06/capas-acciones.jpg*

3. Analysis and Evaluation of Risks.

The objective of the risk analysis and evaluation is to determine them with representative values to be treated by the institution, this allows to identify the most important assets and indicate the impact of the risk. [3]

3.1 Information Security Risk Management ISO / IEC 27005.

ISO 27005 provides guidelines for managing the risks of information security in an entity, in addition to supporting the ISO 27001 ISMS, so that this system can be implemented with satisfaction by orienting itself to risk management analysis, the components of this standard Are shown in Table 1. [1]

Proposes	**The approach of the information security risk management process.**
Evaluation	Assess risks through: ➢ Risk analysis. ➢ Risk assessment.
Treatment	➢ Risk management. ➢ Acceptance of risk.

Additional components	➢ Monitoring and review of risk. ➢ Communication of risk.

Table 4. Components of Risk Management.
Source:http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

This section assesses risks by recognizing existing controls in the organization, identifying, estimating, and evaluating assets, threats, and vulnerabilities in GADMU.

3.1 Methodology for risk analysis.

Qualitative Methodology:

It is more used in decision making because it is supported by its experience, dynamism and intuition, the form of classification of impacts is: Low, Moderate, High, and Critical.In this qualitative methodology interact 4 elements that are: threats, vulnerabilities, Impacts and controls their advantage is the compression of what is being done. [4]

Quantitative Methodology:

It is a collection of data, perform calculations and uses modeling techniques that result in information difficult to estimate, in addition to making use of numerical scales. For the analysis of risks in the GADMU, both methodologies will be used, since on the one hand attributes are classified as indicated by the qualitative method and together with this it is valued numerically to represent them with greater accuracy. [4]

Asset Valuation

The valuation of assets is done according to the impacts both inside and outside the data network and dependencies of these towards other assets, for the evaluation of assets the qualification criteria are used, indicated in table 2, ISO 27005 indicates a rating in the range of 1-4 to describe the value of each asset. [4]

Value	Criterion	Description	Effect
1	Low	Unnecessary	Very limited in technology
2	Moderate	Little Needed	Some technological capability.
3	High	Necessary	It has technological capability.
4	Crítical	Very Necessary	State-of-the-art technological capability

Table 2. Asset Valuation.
Source:http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

Valuation of active importance

The product of the values obtained from each parameter identified in Table 2 determine the valuation of assets, which in turn will belong to a level of importance, as indicated in Table 3, ISO 27005 indicates a range values to determine the importance of The assets in the organization. [4]

Item	Values Range	Criterion	Description
1	1-8	Unlikely	Low Importance
2	9-26	Important	Important
3	27-64	Crítical	Very important.
Value of Asset = Dependency * Functionality * (Confidentiality, Integrity, Availability)			

Table 3. Valuation of Importance of Assets.
Source:http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

Threat Occurrence

They are numerical qualifying values used to evaluate the probability of threats, as indicated by the ISO 27005 standard, Table 4 indicates the range of probability of occurrence of threats in four possibilities. [4]

Value	Range	Criterion	Description
1	(0-25)%	Unlikely	Very low probability
2	(26-50)%	Moderately Likely	Low probability
3	(51-75)%	Probable	High probability.
4	(76-100)%	Very likely	Very high probability

Table 4. Threat Occurrence.
Source:http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

Impact assessment

According to ISO 27005, the impact assessment measures the consequence of the materialization of a risk, in addition to being the average value between the impacts of integrity, confidentiality and availability, being thus a very important point when making a decision on the controls To use, as shown in Table 5. [4]

Value	Criterion	Description
1	Low	The impact is minimal.
2	Medium	The impact is medium
3	High	The impact is high.

Table 5. Impact Assessment.
Source:http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

Risk assessment

The product between the probability of occurrence of a threat indicated in Table 4 and the assessment of impacts in Table 3 results in the assessment level for the risk assessment, as indicated in Table 6. [4]

Range of values	Criterion	Description
1-2	Low	Asset risk is low
3-4	Moderate	Asset risk is moderate
5-8	High	Asset risk is high
9-12	Crítical	Asset risk is critical
Risk level = Probability * Impact		

Table 6. Risk Assessment.
Source:http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

Treatment of risks

It is the decision-making against the different risks, they are the strategy of the organization, the standard ISO 27005 presents the following options:

- **Reduce:** Consists of choosing connection controls, elimination, prevention, mitigation of impact.
- **Accept:** No additional controls are implemented as the organization assumes damage.
- **Avoid:** Or eliminate risk, which is usually not the best option since in most cases it is usually expensive complex.
- **Transfer:** To a third party in order to secure the asset or subcontract it. [4]

Based on current GADMU policies (GADMU, 2016), the decisions that are implemented are only two: Reduce or Accept it, due to the cost of the other two options. The risks will be accepted when these do not affect the activities of the officials and in the opposite case they will be reduced, as indicated in table 7.

Criterio	Treatment
Low	ACCEPT THE RISK
Moderate	
High	REDUCE RISK
Crítical	

Table 7. Treatment of Risk.
Source:http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

Priority in applying controls

Based on the ISO 27005 standard The calculation of the priority controls is done by the product of the value of the importance of assets in Table 3 and the range of values of the risk assessment in Table 6, here we determine the priority range Of application of controls, as indicated in Table 8. [4]

Values Range	Criterion	Description
1-13	Low	They can expect to be implanted after the medium and high priority.
14-23	Half	They can expect to be implanted after the high priority ones.
24-36	High	They must be implanted immediately.
Priority in the application of controls = Level of importance * Risk level		

Table 8. Priority of application of controls.
Source:http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

Risk Analysis

It is the identification of the assets that give value to the institution, the threats that affect the daily operation and the impact that causes the occurrence of any of them, in the risk analysis the assets are classified in: Primary and Support or Support. [4]

Asset Valuation

For valuation of assets, use table 2 "Valuation of assets" to qualify the asset in values of dependency, functionality, confidentiality, integrity and availability where the product of these values results in the value of the asset, this value It relates it to Table 9 "Priority of application of controls" for the application of controls, as indicated by ISO 27005. An example of asset qualification is Table 9, where (CID) is: confidentiality, integrity and availability. [4]

Activo	Dependencia	Funcionalidad	C-I-D	Valor del activo
Servidor HP ProLiant DL380	4	3	3	36

Table 9. Example of asset rating.
Source:http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

Identification of Vulnerabilities and Threats.

Based on studies of the ISO 27001 standard, vulnerabilities are the principle for the formation of threats, this identification allows establishing a relationship between these two, giving knowledge of the origin of the threats and if these materialize that risks are those that occur.

Vulnerabilities are directly related to threats. The identification of vulnerabilities as a consequence of threats, natural, physical, human and organizational were made through technical visits to the facilities and interviews with

the network administrator, table 10 indicates an example of vulnerability and threat identification. [4]

Vulnerability	Threat
It does not have a contingency plan for the recovery of information in case of disasters	Natural Phenomena

Table 10. Example of vulnerability and threat identification.
Source:http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

Risk estimation

In the estimation of risk, values are assigned to the possibilities and consequences of a risk, in this process the valuation of table 5 of "Assessment of impacts" is used, thus determining the importance in terms of confidentiality, integrity and availability, as Indicates table 11. Where C (confidentiality), I (integrity), D (availability). [4]

Threat	Vulnerability	C	I	D	Impact
Natural or Environmental Threats	There is no recovery plan	1	1	3	2

Table 11. Example of risk estimation.
Source:http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

Assessment of incidents

For the evaluation of incidents, the criteria in table 4 "Threat occurrence" are used as indicated by the example in table 12. [4]

Threat Type	Vulnerability	Threat	Probability
Natural or Environmental Threats	There is no recovery plan	Natural Phenomenon	2

Table 12. Example of incident assessment.
Source:http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

Risks evaluation

For the risk assessment, the critical assets with their vulnerabilities are identified and classified in terms of confidentiality, integrity and availability using Table 5 "Impact assessment", then the average of these three values gives us the value of Impact, from that point the probability of occurrence of threats to the asset according to Table 4 "Threat Occurrence" is qualified, in the end the risk level is the product between the value of the impact and the probability of threats as indicated by the Table 6 "Risk assessment", thus determining the treatment to be followed, according to table 7 "Treatment of risk". Table 13 below shows an example for this process. Where C (confidentiality), I (integrity), D (availability)[4]

Type of Threat	Natural or Environmental Threats
Vulnerability	It does not have contingency plan for the recovery of information in case of disasters
C	1
I	1
D	3
Impact	2
Probability	2
Risk level	4
Treatment	Accept

Table 13. Example of existing risk assessment

Source: Information extracted from GADMU.

4. Design and implementation of ISMS

The design and implementation of the ISMS consists of the elaboration of the control objectives indicated by ISO 27001 to establish security policies and procedures that focus on the interests of the institution.

4.1 Control Objectives.

The control objectives are a guide to determine a process to prevent, protect and manage risks due to different damages, in this part gives us the flexibility in choosing the objectives that fit the scope of the system, then the controls are listed And control objectives. [1]

Security policy

It is the control objective that encompasses the others, this one is presented as a guide to safeguard the information of the organization besides covering the fulfillment of the other control objectives, describing that it can be done or not within the GADMU [1]

Asset Management

Asset management includes articles on the assignment of controllers for each asset, which must carry out actions of storage, back-up and continuous controls on these assets, in addition to notifying news or problems to those responsible for the security system. [1]

Human Resources Security

Human resources security focuses on the training of workers who will be integrated into the work within the GADMU in order to be able to carry out their work together with the ISMS. [1]

Physical and Environmental Safety

Physical and environmental security refers to the facilities and environmental conditions within the GADMU building, such as: workstations, data center equipment, and physical security such as closed doors, surveillance cameras and security personnel. [1]

Communications and Operations Management

The management of communications and operations are the processes to be followed for the acquisition of new technological equipment for GADMU, designating those responsible for authorizing and carrying out this process. [1]

Access control

Access control focuses on the access of all workers to the assets of the organization, either through a user or password or another method of authentication, in addition to the privilege of access to certain telecommunications equipment. [1]

Incident Management in Information Security

The management of incidents in the security of the information focuses to the verification and correction in time of the equipment or systems that present problems and report of these to the designated personnel. [1]

Fulfillment

It is the communication of the ISMS to all GADMU officials, in order to prevent any of them from complying with established security policies. [1]

4.2 Scope of the ISMS.

This system has its scope defined in the protection of the most valuable assets of the institution, which are the database servers and registry, through a firewall cisco RV130, to meet the scope of the ISMS standard. By creating maps of networks and systems, physical locations of the elements are defined as well as organizational diagrams as shown in Figure 4 and 5 respectively. [1]

Diagram of the scope of networks and systems.

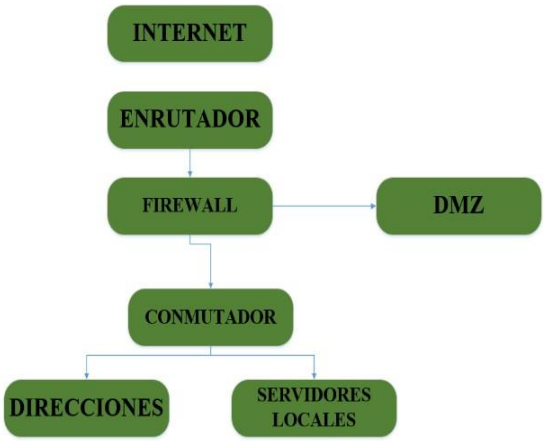


Figure 3. Network scope and ISMS systems
Source: GADMU. (2016). Prepared by Author

Organizational scope diagram

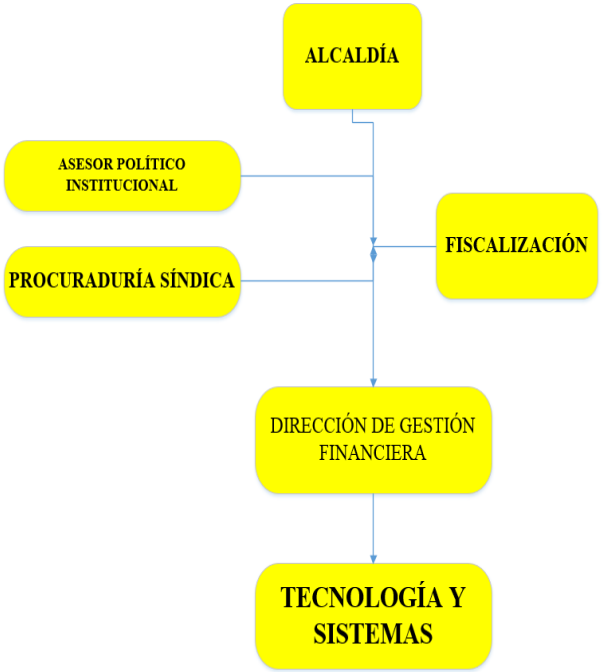


Figure 4. Diagram of the ISMS's oranizational scope
Source: GADMU (2016)). Prepared by Author

4.3 Technical Description of the Security System.

Table 14 generally indicates the operation of the security system for the GADMU data network and the actions taken by the system to filter traffic to certain addresses. [5]

IP Adress	Description	Action
172.16.0.12/16	The IP of the administrator is the only one that can enter to perform configuration tasks in the Document Management and Property Registry servers for the SSH port that is re-directed to port 22016.	ACCEPT
172.16.0.0 /16	Any user of the GADMUR data network can enter the Document Management and Property Registration servers on port 80 (HTTP) to perform query tasks.	ACCEPT
172.16.0.0/16	If any user wants to enter the Document Management and Property Registration servers for another port to configure can not do it, except the Administrator ip.	DENY
172.16.0.0/16	Users have no restrictions to surf the internet from the local network, in terms of port blocking	ACCEPT
Public IP	Restrictions from the internet or from an ip publish any to the local network of the GADMU; They can only enter the servers to perform queries as users on port 80 (HTTP).	ACCEPT
Public IP	If from a public IP or from the internet they want to enter the Document Management and Property Registry servers by some other port they can not do it.	DENY
Public IP	Only the administrator can enter the Document Management and Property Registration servers to configure them through the SSH port re-directed to 22016.	ACCEPT

Table 14. General operation of the ISMS.

Source: Information extracted from GADMU

4.4 Network Structure Implemented in the GADMU.

The implementation consists of a Cisco RV130 firewall which contains all the tools that are determined in the scope, such as: VLAN, DMZ, and ACL for protection of database servers and property registration, as indicated in Figure 5. [5]

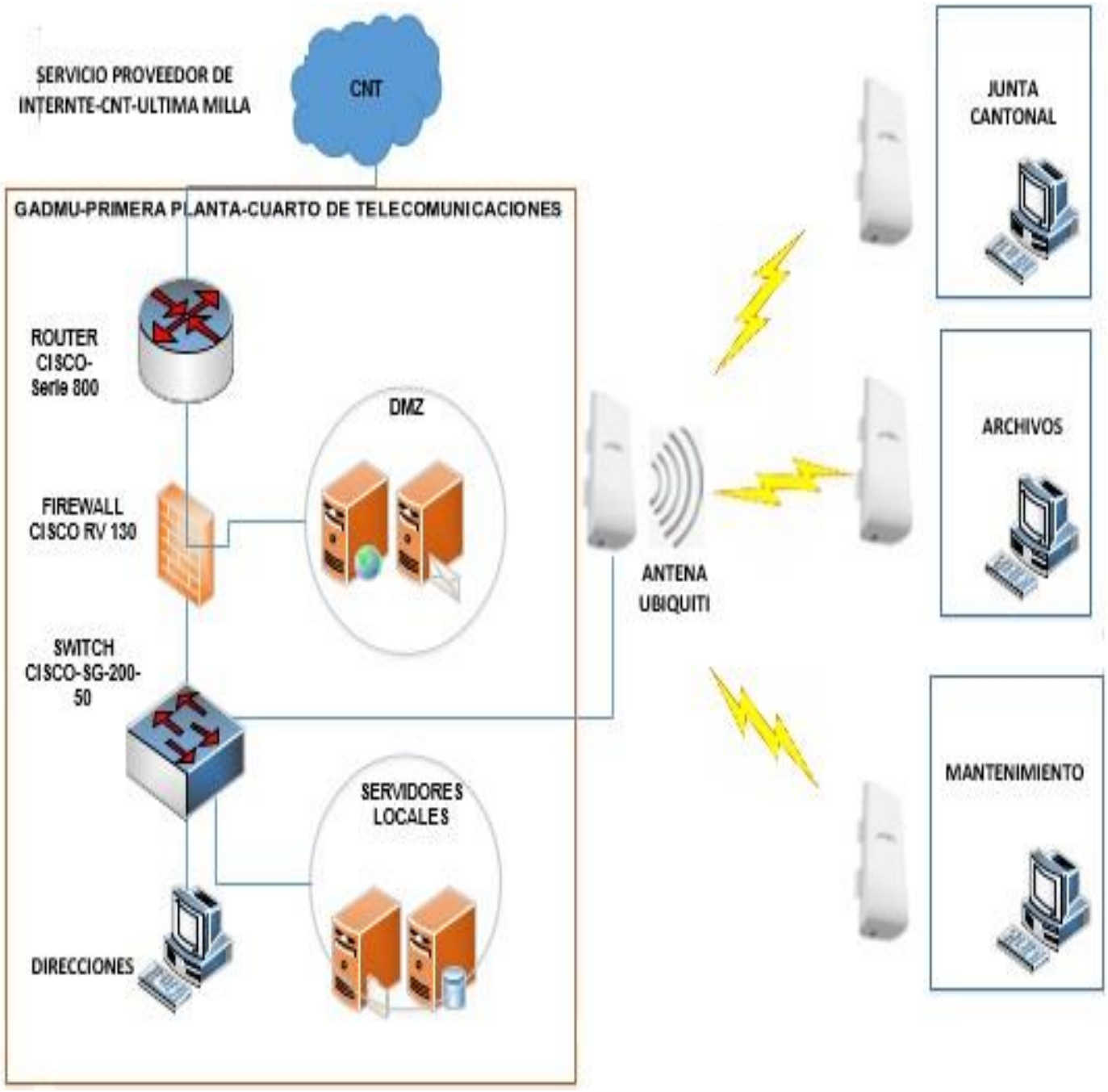


Figure 5. Data network structure implemented in the GADMU

Source: GADMU (2016)). Prepared by Author

4.5 Description of Used Tools.

Access Lists.

Through ACL's we proceed to allow or deny access to the institution's assets, since we will manage services using the extended ACLs because we manage them, communication ports, protocol type and IP addresses are already parameters for Filter the traffic that circulates both from the internal network and from the external network.

The access lists are in accordance with the security policy to comply with the project, the main strategy for the protection of these servers is that workers of the entity can only carry out consultation activities from anywhere, and that only the administrator has Full access to these servers from the WAN. [2]

Virtual Networks VLAN.

A Virtual LAN or VLAN is a set of terminal devices that belong to a logical network or subnet forming a single broadcast domain independent of its physical location on the network, it is not important that all the computers are connected to the same switch or that the Different links belong to the same VLAN. VLANs can not communicate with each other because they are logically separated even though they are connected on the same network, offering a basic level of security to places in the network that are restricted

Virtual networks configure to segment the network, by default the firewall cisco RV130 comes with 1 vlan for the local network, this vlan is assigned physical device interface (fa0 / 1), when creating another vlan for the DMZ this is assigned to another Interface (fa0 / 2) as shown in figure 6. [2]

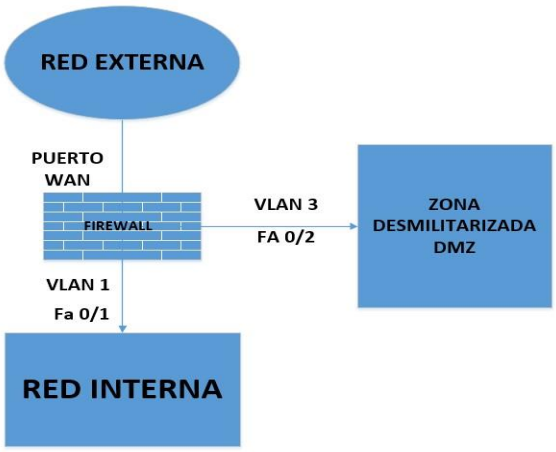


Figure 6. Network distribution scheme using Vlan's.
Source: GADMU (2016)). Prepared by Author

Demilitarized Zone.

The DMZ is the area intended for publicly accessible servers, it is a subnet behind a firewall in which ports can be managed for access either from the LAN or the WAN. Figure 7 shows how to locate the DMZ for the servers. [2]

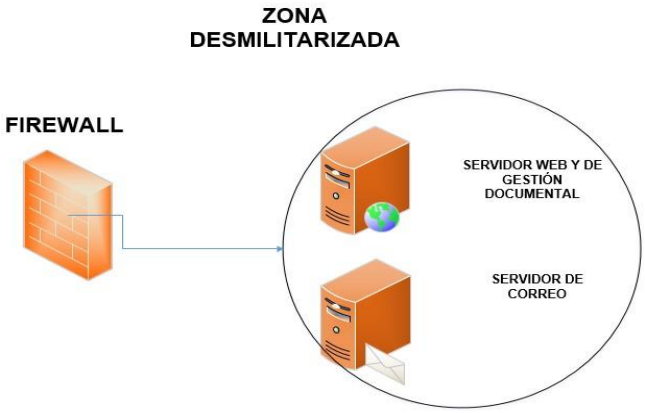


Figure 7. Location representation of the DMZ
Sourcee: https://norbertomn.files.wordpress.com/2014/02/curso-seguridad-en-informacion.pdf

SSH

The SSH protocol is a secure means of communication between a client and a server since the information is encrypted during transmission, the SSH protocol uses port 22 to communicate, this protocol offers confidentiality and integrity, here are some features. [2]

- ✓ **Integrity:** The information is not altered by other people.
- ✓ **Authentication:** That those who participate in communication are who they claim to be.
- ✓ **Confidentiality:** People outside the communication can not read the same.
- ✓ **No repudiation:** If a message is sent, it should not be rejected.
- ✓ **Rejection of duplicates:** It does not stop sending the message if it is repeated.

Firewall CISCO RV 130

The CISCO RV 130 firewall is a device that allows you to filter traffic on a data network, this device contains all the features to implement the tools mentioned above.

In addition to being able to carry out a service management for the whole network in the sense that is chosen, this device was facilitated by GADMU to carry out this process, figure 8 indicates the device. [6]

Figure 7.

Firewall Cisco RV 130
Source:http://www.cisco.com/c/dam/en/us/td/docs/routers/csbr/rv130w/admin_guide/es/rv130w_admin_es.pdf

5. Results Obtained.

In order to better appreciate the results obtained with this project, a table is drawn up on the impacts that occurred after the implementation of this security system, for which an analysis of the situation in which the network was found Of data, with which it is currently operating, as indicated in table 15. [5]

SITUATION PREVIOUS	SITUATION CURRENT
Outdated security policies, unknown and obsolete due to the lack of communication of the same to all personnel.	The existence of a manual of security policies that are coupled to the needs of the GADMU, and that are known by all the workers of the entity.
Lack of organization of all those involved in network security to communicate changes in network systems.	An organizational diagram that commits all those involved in communicating changes or improvements in the systems of the network and in the decision-making in front of the problems that exist in the same.
Disorganization and ignorance in the processes that is carried out for the solution of problem of hardware or software by the users of the terminal equipment.	Process organized and known by the workers to provide an effective solution to the problems of hardware or software.
Lack of awareness about information security for new workers with the assets they manage during their work.	Initial commitment of workers with the institution on the responsibilities of taking care of the assets with which it will work.
A totally unprotected network at the logical level and deficiencies in its structure with which several risks and vulnerability occur in the system.	A more secure and segmented network that filters traffic by limiting access to certain services by reducing risks and eliminating vulnerabilities
The physical topology of the network was deficient in its connections due to a lack of knowledge about network security.	A more robust and orderly physical topology that better distributes services to all users.
No initiative on the implementation of any security system, even with the registry of a DoS attack on this network.	A safety system based on an international standard such as ISO 27001 which has a continuous life cycle (PDCA) that improves according to the needs of the entity.

Table 15. Impacts of ISMS in GADMU.

Source: Information extracted from GADMU.

6. Conclusions

- ✓ By means of ISO 27005 standard for risk analysis and management, the most important assets were determined with high levels of risk that should be reduced, resulting in mandatory compliance with information security policies and processes for this action.
- ✓ Information security policies and processes are going to change over time due to continual improvement of the ISO 27001 standard to meet the objectives of the organization.
- ✓ Although the information security policies and controls found in the GADMU were not fully documented, they served as a basis for establishing new security controls.
- ✓ Through the risk analysis and risk management methodology ISO 27005, controls were established to reduce existing risks, which were included in the analysis of these, ensuring the operation of the ISMS.
- ✓ The risk analysis identifies the value of the most important assets to be protected, because they are prone to suffering damage, qualifying them as values of dependence, function, confidentiality, integrity and availability.
- ✓ Improvements in the ISMS are in line with updates to the risk analysis, identifying new threats, vulnerabilities, and whether controls are still effective in meeting the organization's objectives.
- ✓ The benefit of having a cisco rv130 firewall is that the computer has the necessary properties to perform the security settings of the data network at the logical level.

Aggrement

Special thanks be extended to the Autonomous Government of San Miguel de Urcuquí for the support provided on this project, especially to Engineer Mario Farinango in charge of the Systems Department who provided the necessary resources for the completion of this work.

Bibliographic references

[1] ISO/IEC, «ISO/IEC 27005,» 30 Junio 2008. [En línea].Available: http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf.

[2] Cursos en Seguridad de la Información., «Seguridad de sistemas de la información,» 2010. [En línea]. Available: https://norbertomn.files .wordpress.com/2014/02/curso-seguridad-en-sistemas-de-informacion .pdf. [Último acceso: 1 Marzo 2016].

[3] ISO 27000, «ISO 27005-2008,» 30 Junio 2008. [En línea]. Available: http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf. [Último acceso: 1 Abril 2016].

[4] iso 27000, «Gestión de Riesgos tecnológicos basada en ISO 27005 para la continuidad de negocio,» 2011. [En línea]. Available: file:///C:/Users/HENRY/Downloads/Dialnet-GestionDeRiesgos TecnologicosBasadaEnISO31000EISO27-4797252%20(3).pdf. [Último acceso: 1 Abril 2016].

[5] I. M. Farinango, Interviewee, *Estado de la red de datos.* [Entrevista]. 1 Junio 2016.

[6] CISCO, «CISCO RV 130,» 2015. [En línea]. Available: http://www.cisco.com/c/dam/en/us/td/docs/routers/csbr/rv130 w/admin_guide/es/rv130w_admin_es.pdf. [Último acceso: 1 Abril 2016].

Authors

Henry G. VALENCIA FERNÁNDEZ. Was born in Ibarra on 27 August 1992. He completed his primary education at the Pedagogical Institute “28 de Septiembre”. Secondary studies were conducted at the “Unidad Educativa Experimental Teodoro Gómez de la Torre” College, where he finished in 2010, obtaining the Bachelor of Physical Mathematical Sciences Specialization. Currently he is conducting its process engineering degree in Electronics and Communication Networks, Northen Technical University-Ecuador.

Edgar A. MAYA OLALLA. Was born in Ibarra – Ecuador on April 22, 1980. He is an Engineer in Computer System at Northen Technical University in 2006. He currently teaches Race Engineering in Electronics and Communication Networks at the Technical University North Ibarra-Ecuador, and is a graduate of the Master in Communication Networks at Pontifical Catholic University of Ecuador, Quito, Ecuador.