ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

EVALUACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA ELÉCTRICA QUITO UTILIZANDO LA NORMA ISO 27002

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

AUTOR:

ECHEVERRÍA RODRÍGUEZ SARA VIVIANA

sara_echeverria@hotmail.es

DIRECTOR:

ING. CARLOS MONTENEGRO, MSC.

carlos.montenegro@epn.edu.ec

QUITO, noviembre 2015

DECLARACIÓN

Yo, Sara Viviana Echeverría Rodríguez declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

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

Echeverría Rodríguez Sara Viviana

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Echeverría Rodríguez Sara Viviana, bajo mi supervisión.

Msc. Ing. Carlos Montenegro
DIRECTOR DE PROYECTO

DEDICATORIA

Este trabajo está dedicado especialmente a mis padres ya que gracias a ellos pude hacer este sueño realidad.

A mi madre Norma, que me enseñó que para obtener lo que uno quiere hay que luchar con todas las fuerzas que se tiene y que nunca debemos darnos por vencidos.

A mi padre Víctor, por demostrarme que la vida, por más dura que sea, siempre tiene un lado bueno. Por enseñarme que no es necesario tener mucho para ser feliz y menos aún para ayudar a la gente que realmente necesita. Por nunca perder la esperanza y ser fuerte a pesar de las duras pruebas que nos ha puesto la vida.

A ti Luis Sánchez N., por ayudarme a cumplir esta meta. Por darme siempre la mano en los momentos difíciles y reír conmigo en los momentos buenos. Por ayudarme a levantar cuando siento que he caído, por ser mis fuerzas cuando más lo he necesitado y por ese apoyo incondicional, no solo conmigo sino también con mi familia. Te amo muchísimo y todos los días le agradezco a Dios por haberte puesto en mi camino.

A mis sobrinos Damián, Didier, Matías, Milan, Thiago y Gabriel por darle alegría a mi vida con sus ocurrencias y sus muestras de cariño.

A mis hermanos Gabriel, Darwin y Belén por el apoyo y las fuerzas brindadas.

A toda mi familia y a todas las personas que han hecho posible la culminación de esta meta.

Sara.

AGRADECIMIENTO

Agradezco a Dios por haberme dado la oportunidad de culminar la mayor de mis metas a pesar de todas las dificultades que se me han presentado en la vida y por darme las fuerzas necesarias para salir con la cabeza en alto de esas dificultades.

Agradezco a mis padres, por el enorme esfuerzo que han hecho todo este tiempo por darme a mí y a mis hermanos la oportunidad de ser personas de bien, por el apoyo brindado y por las enseñanzas de vida que me han dado y han permitido que culmine esta meta.

Agradezco a mis hermanos que han sido mi soporte en los momentos difíciles y por estar siempre en las buenas y malas.

Agradezco a Luis Sánchez por el amor y el apoyo que me ha brindado y por convertirse en mi persona especial para toda la vida.

Agradezco a mi familia por el apoyo incondicional y por los consejos brindados a lo largo de mi vida.

Agradezco al MSc. Ing. Carlos Montenegro, por las enseñanzas como mi profesor y tutor de este proyecto de titulación. Por la confianza brindada y sobre todo por la amistad que me ha brindado durante este tiempo.

Agradezco al Ing. Eduardo Alvear, Oficial de Seguridad de la Información de la Empresa Eléctrica Quito S.A., por todo el apoyo brindado para la realización de este proyecto de titulación.

Agradezco a mis profesores, compañeros y amigos que hicieron muy ameno este paso por la universidad.

Contenido

1. CAPÍTULO 1. PLANTEAMIENTO DEL PROBLEMA 15

1.1. RECONOCIMIENTO DE LA E.E.Q. S.A 15

1.1.1. DATOS DE LA EMPRESA 15

1.1.2. RESEÑA HISTÓRICA Y CONSTITUCIÓN 16

1.1.3. PRINCIPAL ACTIVIDAD 17

1.1.4. INFRAESTRUCTURA 19

1.1.5. PLANES 19

1.1.6. LINEAMIENTOS EMPRESARIALES 20

1.2. SITUACIÓN ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN EN LA E.E.Q. 24

1.2.1. ANTECEDENTES 24

1.2.2. SITUACIÓN ACTUAL 25

1.3. ESPECIFICACIÓN DE LOS DOMINIOS DE LA NORMA ISO 27002 A UTILIZAR PARA LA EVALUACIÓN 31

1.3.1. NORMA ISO 27002 31

1.3.2 ESPECIFICACIÓN DE DOMINIOS DE LA ISO 27002, DIRECTRICES DEL EGSI Y CONTROLES DE CSC A UTILIZAR PARA LA EVALUACIÓN 33

2. CAPÍTULO 2. EVALUACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE LA E.E.Q. S.A. 41

2.1. APLICACIÓN DE LOS DOMINIOS DE LA NORMA ISO 27002 SELECCIONADOS AL S.G.S.I. DE LA E.E.Q. 41

2.1.1. RECOLECCIÓN DE INFORMACIÓN 41

2.2. ANÁLISIS DE RESULTADOS 60

2.2.1. RESULTADOS FINALES 94

2.3. ELABORACIÓN DEL INFORME EJECUTIVO 115

2.4. ELABORACIÓN DEL INFORME TÉCNICO 115

3. CAPÍTULO 3. CONCLUSIONES Y RECOMENDACIONES 116

3.1. CONCLUSIONES 116

3.2. RECOMENDACIONES 117

BIBLIOGRAFÍA 119

ANEXOS 122

INDICE DE TABLAS

Tabla 1.1 Área de concesión de la EEQ [1] 19

Tabla 1.2 Valores Institucionales y Compromisos 21

Tabla 1.3. Cuadro de Integración de Capital de la EEQ. 26

Tabla 1.4 Marco de evaluación para el proyecto de titulación 40

Tabla 2.1 Tabla de recolección de información – Inventario de activos (Parte 1) 43

Tabla 2.2 Tabla de recolección de información – Inventario de activos (Parte 2) 44

Tabla 2.3 Tabla de recolección de información – Inventario de activos (Parte 3) 45

Tabla 2.4 Tabla de recolección de información – Inventario de activos (Parte 4) 46

Tabla 2.5 Tabla de recolección de información – Inventario de activos (Parte 5) 47

Tabla 2.6 Tabla de recolección de información – Inventario de activos (Parte 6) 48

Tabla 2.7 Tabla de recolección de información –Responsable de los activos (Parte 1) 49

Tabla 2.8 Tabla de recolección de información – Responsable de los activos (Parte 2) / Uso aceptable de los activos (Parte 1) 50

Tabla 2.9 Tabla de recolección de información – Uso aceptable de los activos (Parte 2) 51

Tabla 2.10 Tabla de recolección de información – Uso aceptable de los activos (Parte 3) 52

Tabla 2.11 Tabla de recolección de información – Uso aceptable de los activos (Parte 4) 53

Tabla 2.12 Tabla de recolección de información – Uso aceptable de los activos (Parte 5) 54

Tabla 2.13 Tabla de recolección de información – Uso aceptable de los activos (Parte 6) 55

Tabla 2.14 Tabla de recolección de información – Uso aceptable de los activos (Parte 7) 56

Tabla 2.15 Tabla de recolección de información – Uso aceptable de los activos (Parte 8) 57

Tabla 2.16 Tabla de recolección de información – Directrices de clasificación 58

Tabla 2.17 Tabla de recolección de información – Etiquetado y manipulado de la información 59

Tabla 2.18 Tabla de recolección de información – Totales 60

Tabla 2.19 Estructura del documento Equipos Activos de la Empresa eléctrica. 62

Tabla 2.20 Características funcionales de los servidores. 64

Tabla 2.21 Características de las aplicaciones instaladas en cada servidor. ... 65

Tabla 2.22 Características físicas de los servidores. 66

Tabla 2.23 Características a añadir en un inventario de activos de hardware según SANS 20. 73

Tabla 2.24 Características a añadir en un inventario de activos de software según SANS 20. 76

Tabla 2.25 Comparación entre NTE-ISO/IEC 27002:2009 y EGSI, para el dominio 7. Gestión de Activos (Objetivo de control 7.1.1 Inventario de activos). 95

Tabla 2.26 Comparación entre NTE-ISO/IEC 27002:2009 y EGSI, para el dominio 7. Gestión de Activos (Objetivo de control 7.1.2 Responsable de los activos). 96

Tabla 2.27 Comparación entre NTE-ISO/IEC 27002:2009 y EGSI, para el dominio 7. Gestión de Activos (Objetivo de control 7.1.3 Uso aceptable de los activos). 97

Tabla 2.28 Comparación entre NTE-ISO/IEC 27002:2009 y EGSI, para el dominio 7. Gestión de Activos (Objetivo de control 7.2.1 Directrices de Clasificación). 98

Tabla 2.29 Comparación entre NTE-ISO/IEC 27002:2009 y EGSI, para el dominio 7. Gestión de Activos (Objetivo de control 7.2.2 Etiquetado y manipulado de la información). 99

Tabla 2.30 Tabla de criterios de evaluación. 101

Tabla 2.31 Matriz de criterios de evaluación. 101

Tabla 2.32 Medición de cumplimiento – 7.1.1. Inventario de activos 103

Tabla 2.33 Medición de la seguridad de la información - 7.1.2. Responsable de los activos..... 105

Tabla 2.34 Medición de la Seguridad de la Información – 7.1.3. Uso aceptable de los activos..... 107

Tabla 2.35 Medición de la seguridad de la información – 7.2.1. Directrices de clasificación 109

Tabla 2.36 Medición de seguridad de la información – 7.2.2. Etiquetado y manipulado de la información..... 111

Tabla 2.37 Niveles de cumplimiento en base a los criterios de evaluación. .. 113

INDICE DE FIGURAS

Figura 1.1 Orgánico Funcional EEQ. 23

RESUMEN

El siguiente proyecto de titulación “EVALUACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA ELÉCTRICA QUITO UTILIZANDO LA NORMA ISO 27002” fue elaborado como producto de la necesidad de evaluación de la aplicación de los controles de la Norma ISO/IEC 27002 para la Seguridad de la Información en la Empresa Eléctrica Quito S.A.

Fue desarrollado con la finalidad de servir como ayuda al personal de la Empresa Eléctrica Quito S.A., para la identificación de los niveles de cumplimiento en la aplicación de los controles de la norma ISO/IEC 27002, así como también de la aplicación de las directrices del Esquema Gubernamental de Seguridad de la Información (EGSI) establecido por la Secretaría Nacional de la Administración Pública.

Para la realización de este proyecto de titulación, se utilizó una propuesta metodológica de evaluación desarrollada en base al criterio de la autora, la misma que utiliza una tabla de mapeo o relación entre el dominio seleccionado de la norma ISO 27002, las directrices del EGSI y los Controles Críticos de Seguridad (CSC) de SANS INSTITUTE a utilizar para medir el nivel de cumplimiento de la implementación de dicha norma en la EEQ.

La propuesta metodológica antes mencionada consiste en revisar cada una de las directrices del EGSI, compararlas con los controles correspondientes de la ISO 27002 y en base a los resultados obtenidos en la revisión y comparación, obtener los niveles de cumplimiento de cada control y objetivo de control de la norma ISO 27002. Además, mediante el uso de los CSCs de SANS INSTITUTE, se propuso mejoras en el proceso de gestión de activos.

Los resultados obtenidos en la evaluación demostraron que los niveles de cumplimiento a nivel procedural, en la implementación del SGSI en la Empresa Eléctrica Quito a nivel de la Gestión de Activos, son parciales y van acorde a su plan de mejora continua.

INTRODUCCIÓN

El presente proyecto de titulación está compuesto por tres capítulos, y anexos, los cuales tienen por objetivo dar a conocer los resultados de la evaluación que se llevó a cabo en la Empresa Eléctrica Quito S.A., utilizando como base de la evaluación a la norma ISO/IEC 27002.

En el Capítulo 1 se realiza el Planteamiento del Problema, para lo cual se realizó una descripción de la Empresa Eléctrica Quito S.A. a nivel organizacional. Se presenta también, un análisis de la situación actual de la seguridad de la información, la misma que sirvió de base para la evaluación de este proyecto de titulación. Además, se presenta la especificación de los dominios de la ISO 27002, las directrices del EGSI y los controles de CSC a utilizar para la evaluación antes mencionada.

En el Capítulo 2 se realiza la evaluación del sistema de gestión de la seguridad de la información de la Empresa Eléctrica Quito S.A., para lo cual se aplica el dominio, las directrices y los controles seleccionados para la evaluación en el capítulo 1. Se muestra además una tabla de recolección de la información, y en base a esta, se presenta el análisis de los resultados obtenidos en la evaluación. Finalmente en este capítulo, se describe la elaboración de los informes técnico y ejecutivo.

En el Capítulo 3 se presentan las conclusiones y recomendaciones.

PRESENTACIÓN

La Evaluación es una herramienta de auditoría que puede ser utilizada por el personal de una organización para medir el éxito de sus sistemas internos y tomar medidas correctivas cuando sea necesario, con la finalidad de mejorar su rendimiento.

En este proyecto de titulación se realizó una evaluación de la situación actual de la Seguridad de la Información en la Empresa Eléctrica Quito, considerando que aún no se tiene implementado formalmente un Sistema de Gestión de Seguridad de la Información.

Para llevar a cabo la evaluación, se seleccionó al dominio 7. Gestión de Activos, de la norma ISO 27002, y se utilizó además las directrices establecidas en el Esquema Gubernamental de Seguridad de la Información elaborado por la SNAP en base a la NTE ISO / IEC 27002, que rige a las empresas que forman parte de la Administración Pública, siendo la Empresa Eléctrica Quito S.A. una de éstas.

Esta evaluación permitió conocer algunas de las fortalezas de la organización así como sus debilidades, basándose en las directrices establecidas en el Esquema Gubernamental de Seguridad de la Información, publicado por la Secretaría Nacional de Administración Pública.

En base a la evaluación, se hace la entrega de un conjunto de conclusiones y recomendaciones que servirán de ayuda al personal de la Empresa Eléctrica Quito en su proceso de mejora continua.

1. CAPÍTULO 1. PLANTEAMIENTO DEL PROBLEMA

En este capítulo se realizará una descripción general de la Empresa Eléctrica Quito S.A. (EEQ en adelante), así como también, una descripción de la situación actual de la misma en base a las normativas establecidas en la Constitución de la República del Ecuador, referentes a los sectores estratégicos, de decisión y control exclusivo del Estado Ecuatoriano.

A continuación, se presentará un resumen de la norma ISO 27002, la misma que servirá como guía en la evaluación del Sistema de Gestión de Seguridad de la Información (SGSI en adelante)[1] que se llevará a cabo en la EEQ. Además, se resumirán también, el Esquema Gubernamental de la Seguridad de la Información (EGSI en adelante), que rige a las empresas de control exclusivo del Estado Ecuatoriano y que fue establecido por la Secretaría Nacional de Administración Pública (SNAP en adelante)[2] ; así como también, los Controles Críticos de Seguridad (CSC en adelante)[3] de SANS Institute, que serán utilizados como apoyo para la evaluación antes mencionada.

1.1. RECONOCIMIENTO DE LA E.E.Q. S.A

1.1.1. DATOS DE LA EMPRESA

A continuación se muestran datos generales de la empresa, los mismos que fueron tomados de la página web de la EEQ. [1]

Nombre: EMPRESA ELÉCTICA QUITO S.A. (E.E.Q. S.A.)

Dirección: Avenida 10 de Agosto y las Casas

Teléfono: (593) (02) 3964 - 700

[1] El SGSI es un conjunto de políticas para una correcta y adecuada gestión de la información.
[2] La SNAP establece herramientas para el mejoramiento de la eficiencia en la administración de las empresas de control del Estado Ecuatoriano.
[3] Los CSCs son una serie de 20 controles enfocados en la seguridad de la información.

1.1.2. RESEÑA HISTÓRICA Y CONSTITUCIÓN

La Empresa Eléctrica Quito S.A., o EEQ como se la llamará en adelante, tiene en la actualidad 120 años de existencia. A continuación, se presenta una parte de la reseña histórica contenida en el Plan Estratégico 2012-2015 [2] de la EEQ:

En el año de 1895, Don Manuel Jijón Larrea importa un pequeño motor con sus accesorios para proporcionar luz eléctrica a su casa y a la Botica Norteamericana de su propiedad. Posteriormente, dotó de luz eléctrica a la Plaza de la Independencia, en la que se instalaron los cuatro primeros focos de arco voltaico.

A partir de 1895 y 1896, los señores Víctor Gangotena, Manuel Jijón y Julio Urrutia fundaron una empresa denominada “La Eléctrica”, cuyo propósito era dotar a la capital de un alumbrado moderno, sencillo y económico y obtener un lucro legítimo.

En 1987, nació la empresa quiteña “La Eléctrica” con una planta cerca de Chimbacalle, la misma que producía 200 kilovatios, y suministró alumbrado público a la ciudad con la instalación de 60 lámparas de arco voltaico de corriente continua y más tarde con 500 lámparas incandecente4s de 16 bujías.

El 6 de Octubre de 1937, el I. Concejo Municipal de Quito dictó la ordenanza No. 479 por la cual se crea la Empresa Municipal como Empresa Técnica Comercial, dependiente del Concejo. Esta Ordenanza fue dictada en virtud del Decreto Supremo del 9 de agosto de 1937, publicado en el Registro Oficial No. 9 de 20 de agosto de 1937 y estableció un Sistema para la Organización y Administración de las plantas eléctricas municipales como particulares.

Esta nueva Empresa contaba con la generación de la Central de Guangopolo, con una potencia de 3.400 KW, destinada a servir a 9.498 abonados. Progresivamente aumentó su capacidad instalada a 9.400 KW y, consecuentemente, fue ampliando sus sistemas de Sub-transmisión y distribución.

En 1945 la Empresa Eléctrica Municipal solicita la concesión de un préstamo al Banco Internacional de Reconstrucción y Fomento, con la finalidad de instalar una nueva Central Hidroeléctrica de unos 20.000 KW de potencia; y el banco otorga dicho préstamo previo la condición de que la empresa se transformara en una entidad independiente del gobierno central y del gobierno de la ciudad y es así como la Empresa Eléctrica Municipal se convierte en una compañía autónoma, formada por acciones, con el nombre de **Empresa Eléctrica Quito S.A.** según consta en la escritura pública, suscrita el 29 de septiembre de 1955 y teniendo como accionistas al Ilustre Municipio de Quito, a la Caja del Seguro y a la Caja de Pensiones.

1.1.3. PRINCIPAL ACTIVIDAD

De acuerdo al Modelo de Gestión y a la Matriz de Competencias del Sector Eléctrico [2], la actividad principal de la EEQ, está enmarcada la generación, sub-transmisión, distribución, comercialización y eficiencia energética, con la facultad de gestión, y las siguientes atribuciones:

- “Proponer plan de expansión y mejora, programación plurianual y anual de la política pública.
- Ejecutar planes y proyectos para generación, sub-transmisión, distribución, comercialización y eficiencia energética.
- Asegurar la disponibilidad de la infraestructura eléctrica para garantizar la continuidad del servicio.
- Gestionar la disponibilidad de recursos para garantizar la calidad del servicio.
- Promover la participación ciudadana en toda la gestión de la organización.
- Programar, coordinar, ejecutar, controlar y evaluar la operación.

El rol que cumple la organización consta en el Contrato de Concesión de prestación del servicio eléctrico, celebrado entre el Consejo Nacional de

Electricidad (CONELEC) y la EEQ, actualizado el 4 de septiembre de 2007, según el cual a la EEQ le corresponde cumplir lo siguiente:

- Ejecutar el servicio público de distribución y comercialización bajo el régimen de exclusividad regulada, a todos los usuarios finales ubicados en el área geográfica de concesión (detallada la Tabla 1.1); garantizando a los consumidores actuales y futuros, el suministro continuo y eficiente de toda la potencia y energía requerida, conforme a los parámetros técnicos y a las normas que regulen el régimen de calidad y suministro de servicios.
- Efectuar las inversiones necesarias que permitan conservar y dar mantenimiento predictivo, preventivo y correctivo a sus obras e instalaciones, con el fin de asegurar su eficiente operación y calidad del servicio.
- Adoptar las medidas necesarias para asegurar la provisión y disponibilidad de electricidad, a fin de satisfacer toda la demanda en el área de concesión, en tiempo oportuno, debiendo a tales efectos, asegurar las fuentes de aprovisionamiento.
- Suministrar el servicio de electricidad al alumbrado público en avenidas, calles, caminos públicos y plazas públicas, de conformidad con los niveles de iluminación y los parámetros de calidad que establecen las regulaciones vigentes.
- Realizar el adecuado mantenimiento de las instalaciones de alumbrado público, de tal manera que el sistema de iluminación pública funcione dentro de los parámetros técnicos establecidos por la normativa."

La Tabla 1.1 contiene el detalle del área geográfica de concesión de la EEQ, así como también el número de clientes regulados facturados en contadores (medidores) de energía, población electrificada en habitantes y el porcentaje de cobertura dentro del área de concesión:

Área de concesión de la EEQ SA	
Área de concesión:	**14.971 Km2**, cubriendo las siguientes provincias y cantones: **Pichincha**: Quito, Rumiñahui, Mejía, Pedro Vicente Maldonado, San Miguel de los Bancos y parte de Puerto Quito y Cayambe. **Napo**: Quijos y El Chaco.
Clientes regulados facturados:	**965.442 contadores** de energía.
Población electrificada:	**2.776.807 de habitantes**.
Cobertura:	**99,54%**

Tabla 1.1 Área de concesión de la EEQ [1]

1.1.4. INFRAESTRUCTURA

Como se observa en la Tabla 1.1, la EEQ opera en diferentes ciudades del Ecuador, teniendo su edificio matriz en la ciudad de Quito, y sus sucursales en ciudades como Rumiñahui, Mejía, Pedro Vicente Maldonado, San Miguel de los Bancos, parte de Puerto Quito, Cayambe Quijos y El Chaco.

Todas las oficinas, centros de operación y demás estaciones de trabajo cuentan con la tecnología necesaria para la correcta ejecución de sus tareas para llevar a cabo la actividad principal de la EEQ.

1.1.5. PLANES

Plan Estratégico

La EEQ cuenta con un plan estratégico denominado Plan Estratégico 2012 – 2015 [2], definido de la siguiente manera:

“La EEQ asume una misión que privilegia el compromiso de contribuir con la sociedad y el ambiente, con una visión que compromete su aporte al desarrollo sostenible de la ciudadanía, forjando así, su posicionamiento como referente de gestión del servicio público de electricidad, con políticas y valores que constituyen la plataforma ética, legal y de comportamiento, definidos en concordancia con las expectativas de los grupos de actores.”

Plan de Expansión

El Plan de Expansión se encuentra contenido en el plan estratégico antes mencionado [2].

“El Plan de Expansión de la EEQ se lo formula a 10 años y se lo actualiza anualmente. Está conformado por varios programas: el Programa de Mejoramiento de la Distribución (PMD), el Plan de Reducción de Pérdidas Eléctricas (PLANREP), el Fondo de Electrificación Rural y Urbano Marginal (FERUM), El Plan de Mejoramiento y Expansión del Alumbrado Público, el Fondo de la Calidad y el Sistema Integrado para la Gestión de la Distribución Eléctrica (SIGDE).”

1.1.6. LINEAMIENTOS EMPRESARIALES

Los lineamientos empresariales mostrados a continuación, fueron tomados del Plan Estratégico 2012-2015 [2]:

Misión

“Proveer a Quito y al área de concesión, el servicio público de electricidad de calidad, con eficiencia, solidaridad y responsabilidad socio ambiental, contribuyendo al desarrollo del sector eléctrico y la construcción del buen vivir.”

Visión

“Ser referente en el contexto nacional y regional, por la calidad y eficiencia en la prestación del servicio público de electricidad y por su aporte al desarrollo sostenible de la comunidad.”

Valores Institucionales y Compromisos

La Tabla 1.2 mostrada a continuación presenta los valores y comportamientos que se han establecido en la EEQ, los cuales le permiten ejecutar su actividad principal, de una forma adecuada:

VALOR	COMPORTAMIENTOS
Honestidad	Veracidad en la rendición de cuentas y actos
	Participar siempre en actividades lícitas
	Ser sincero con uno mismo y con los demás
	Actuar con transparencia
Lealtad	Obrar en beneficio a los intereses de la institución
	Ser confiable para la institución y sus compañeros
	Cumplir acuerdos tácitos y explícitos
	Mantener el compromiso con el cumplimiento de las actividades asignadas por la Empresa
Respeto	Valorar los intereses y necesidades de los clientes
	Aceptar y comprender la forma de ser de los clientes
	Ser tolerante a lo posición y las opiniones diferentes
	Permitir la participación de todo el personal en actividades de la Empresa
Actitud de servicio	Atender al cliente con calidez, calidad, eficiencia y empatía
	Compromiso de llegar al consumidor con servicios de energía en forma eficiente
	Registrar y solucionar efectivamente las quejas y reclamos de los clientes
	Iniciativa y creatividad para solución de requerimientos
	Impulsar proyectos de mejora continua a fin de mejorar la calidad del servicio
	Brindar al usuario criterios para el uso eficiente de energía
Compromiso Institucional	Trabajar con el orgullo de ser parte de la Empresa
	Identificarse y apropiarse con la misión, visión, objetivos y metas de la Empresa
	Dar un valor agregado a cada actividad
	Cumplir con los compromisos adquiridos
Responsabilidad social y ambiental	Cumplir con las leyes, instituciones y organismos de control
	Cumplir con los planes de manejo ambiental en la gestión de sus actividades
	Apoyar el desarrollo de un ambiente laboral favorable para toda la organización
	Cumplir los acuerdos con los grupos de actores
Solidaridad	Colaborar en las actividades de los demás cuando éstos lo requieran
	Impulsar el trabajo y el crecimiento de su equipo
	Compartir los conocimientos
	Equidad en el trato a los trabajadores

Tabla 1.2 Valores Institucionales y Compromisos

Orgánico Funcional

En la Figura 1.1 se presenta el Orgánico Funcional de la EEQ [2], el cual está distribuido en función de los procesos que se desarrollan en la EEQ.

Como se observa, la EEQ posee una estructura jerárquica, cuyo grado de decisión es directo y en forma vertical.

Para este proyecto de titulación, se procede con el análisis de las áreas involucradas en la evaluación con el fin de identificar las capacidades de cada una de ellas.

Una de las áreas involucradas en la evaluación es la Dirección de Tecnologías de la Información y Comunicación (DTIC en adelante), la misma que se encuentra al en un nivel inferior a la Gerencia General, al mismo nivel de la Asesoría Jurídica y por encima de las áreas operativas. Esta posición en la organización, le da a la DTIC, la autonomía para tomar decisiones junto con la Gerencia General y además de asesorar a las áreas operativas sobre el uso de tecnología. Además, es el área responsable del asesoramiento, soporte y conducción del desarrollo informático de la empresa de acuerdo a su planificación estratégica y su sistema de control de calidad.

Otra de las áreas involucradas es la Dirección de Administración de Activos y Bienes, la cual forma parte de la Gerencia Administrativa y Financiera, y se encuentra en el último nivel considerada como un proceso adjetivo para la EEQ.

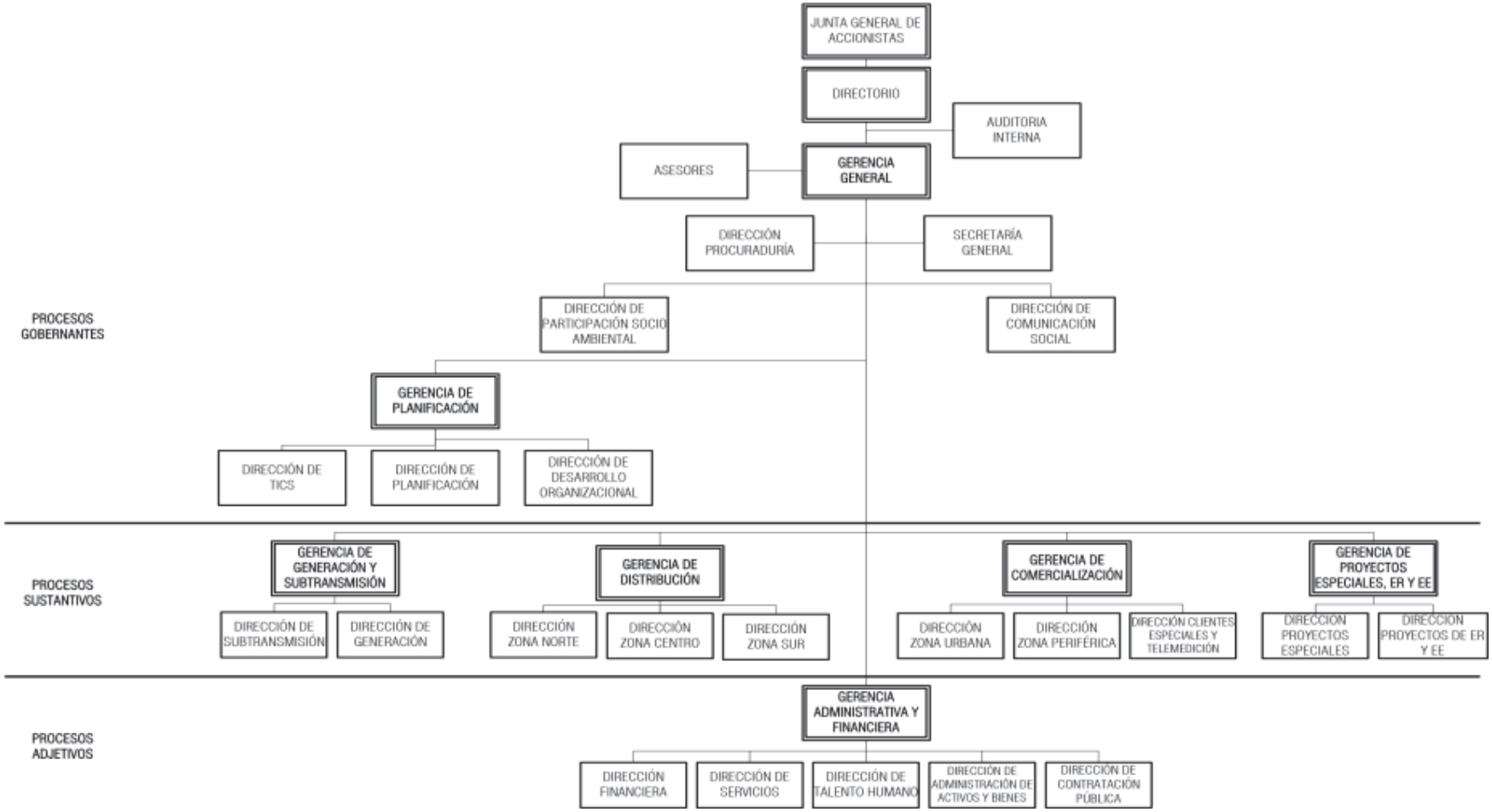

Figura 1.1 Orgánico Funcional EEQ.

1.2. SITUACIÓN ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN EN LA E.E.Q.

1.2.1. ANTECEDENTES

Actualmente, la información es considerada como uno de sus activos más valiosos, por esta razón las organizaciones se han visto en la necesidad de proteger dicho activo ante las constantes amenazas que surgen día tras día.

Una forma de proteger la información, es establecer estándares para el uso adecuado no solo de la información, sino también de los equipos que la contienen o la procesan dentro de las organizaciones.

La ISO/IEC 27000 es conjunto de estándares que permite a todo tipo de organización, el desarrollo e implementación de un Sistema de Gestión de la Seguridad de la Información.

Debido a esta necesidad, la EEQ decide establecer un Sistema de Gestión de Seguridad de la Información, para lo cual en el año 2013 se llevó a cabo una consultoría aplicada al proceso de comercialización. A continuación, se muestra un extracto de la consultoría mencionada:

RESUMEN DE LA CONSULTORÍA LLEVADA A CABO EN LA EEQ EN EL AÑO 2013 COMO PARTE INICIAL A LA IMPLEMETACIÓN DEL SGSI

La EEQ, según Sumario Ejecutivo del **Informe Final V1.0, "SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN"** [3], solicita a la empresa Information Security del Ecuador Inc. (I-SEC), la asesoría en el desarrollo del "SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN".

El objetivo general de la consultoría fue el de realizar el acompañamiento para la implementación del Sistema de Gestión de Seguridad de la Información únicamente para el proceso de comercialización, para lo cual se realizó un análisis de los riesgos de seguridad de la información y se plantearon controles y recomendaciones para la mitigación de las amenazas encontradas.

1.2.2. SITUACIÓN ACTUAL

La Constitución de la República del Ecuador establece que los sectores estratégicos, de decisión y control exclusivo del Estado, son aquellos que por su trascendencia y magnitud tienen decisiva influencia económica, social, política o ambiental, y deberán orientarse al pleno desarrollo de los derechos y al interés social [2].

El Plan Nacional del Buen Vivir, que busca garantizar el bienestar de toda la sociedad ecuatoriana, establece las capacidades estatales de planificación del desarrollo, de regulación y control de los sectores estratégicos de la economía, y de distribución y redistribución de la riqueza social.

En relación a esto, se considera que el acceso a la energía eléctrica es un componente estratégico para el desarrollo, por ser un factor esencial para el cumplimiento y mejoramiento de actividades como la salud, la educación, la cultura, la industria, el comercio, las comunicaciones y la provisión de otros servicios públicos.

Los artículos 15, 313, 314, 315 y 413 de la Constitución de la República del Ecuador, determinan los principios y orientaciones para la gestión de los sectores estratégicos, y en el caso del sector eléctrico, para garantizar la provisión y el servicio eficiente de electricidad a la población.

Por tal razón, la EEQ pasa a ser parte de la Administración Pública del Estado Ecuatoriano, siendo competencia del Ministerio de Coordinación de los Sectores Estratégicos – MICSE, del Ministerio de Electricidad y Energía Renovable –MEER; y debe obedecer a las normas y/o leyes que se establezcan y que permitan garantizar el buen vivir de nosotros los ecuatorianos.

Cabe mencionar que la EEQ es propiedad de los gobiernos descentralizados de: Municipio del Distrito Metropolitano de Quito –MDMQ, y el Gobierno de la Provincia de Pichincha de acuerdo a la Tabla 3, los cuales buscan de igual manera, mejorar la situación actual de los ecuatorianos.

El capital de la EEQ, de acuerdo a la Aprobación Superintendencia de Compañías No. oo.Q.1739 del 6 de Julio del 2000 [4], está integrado de la siguiente manera:

ACCIONISTA	Acciones Ordinarias	Acciones Preferidas	Total	%
Fondo de Solidaridad	23 844 120		23 844 120	52.47
I. Municipio del Distrito Metropolitano de Quito	14 982 044	618 076	15 600 120	34.33
Industriales y Comerciales	766 440		766 440	1.69
Consejo Provincial de Pichincha	5 166 080		5 166 080	11.37
Consejo Provincial del Napo	70 040		70 040	0.15
TOTAL:	44 828 724	618 076	45´466.800	100

Tabla 1.3. Cuadro de Integración de Capital de la EEQ.

En base a los artículos 15, 313, 314, 315 y 413 de la Constitución de la República del Ecuador, la EEQ debe regirse entre otros, al siguiente acuerdo:

Acuerdo No. 166 de la Secretaría Nacional de la Administración Pública

"El miércoles 25 de septiembre de 2013, la Secretaría Nacional de la Administración Pública, mediante Acuerdo No. 166 [5] dispone:

166 Dispónese a las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información.

De acuerdo a dicha disposición, se acuerdan los siguientes artículos:

Artículo 1.- Disponer a las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información.

Artículo 2.- Las entidades de la Administración Pública implementarán en un plazo de dieciocho (18) meses el Esquema Gubernamental de Seguridad de la Información (EGSI), que se adjunta a este acuerdo como Anexo 1, a excepción

de las disposiciones o normas marcadas como prioritarias en dicho esquema, las cuales se implementarán en seis (6) meses desde la emisión del presente Acuerdo.

La implementación del EGSI se realizará en cada institución de acuerdo al ámbito de acción, estructura orgánica, recursos y nivel de madurez en gestión de Seguridad de la Información.

Artículo 3.- Las entidades designarán, al interior de su institución, un Comité de Seguridad de la Información liderado con un Oficial de Seguridad de la Información, conforme lo establece el EGSI y cuya designación deberá ser comunicada a la Secretaría Nacional de la Administración Pública, en el transcurso de treinta (30) días posteriores a la emisión del presente Acuerdo.

Artículo 7.- Las entidades realizarán una evaluación de riesgos y diseñarán e implementarán el plan de manejo de riesgos de su institución, en base a la norma INEN ISO/IEC 27005 “Gestión del Riesgo en la Seguridad de la Información”.

En base a los acuerdos detallados en los artículos anteriormente mencionados, se dispone de manera general que el EGSI podrá ser revisado periódicamente en base a las observaciones o sugerencias de las entidades de la Administración Pública Central, Institucional o que dependan de la Función Ejecutiva; Además, cualquier propuesta de inclusión de controles o directrices adicionales, deberán ser comunicadas a la Secretaría Nacional de la Administración Pública previo a su aplicación, de igual manera en el caso de existir alguna excepción institucional, deberá ser justificada técnicamente y comunicada a dicho organismo.

Se dispone también, que los Oficiales de Seguridad de la Información de los Comités de Gestión de Seguridad de la Información actuarán como contrapartes de la Secretaría Nacional de la Administración Pública en la implementación del EGSI y en la gestión de incidentes en la seguridad de la información.

Como disposiciones transitorias, la Secretaría Nacional de la Administración Pública en un plazo de quince (15) días creará un proyecto en el sistema GPR

para homogenizar los hitos a cumplir las instituciones que implementen el EGSI, además emitirá en el plazo de sesenta (60) días desde la emisión del Acuerdo los lineamientos específicos para el registro y documentación del proceso de implementación del EGSI; y en un plazo de noventa (90) días, las metodologías o procedimientos para actualización, implementación, seguimiento y control del EGSI."

RESOLUCIÓN DE LA EEQ PARA LA IMPLEMENTACIÓN DEL EGSI

Como respuesta al Acuerdo No. 166, el Gerente General Encargado, de la EEQ, Ing. Iván Velasteguí R., el 16 de Abril de 2014, emite la Resolución de Gerencia General No. GCG-2884-2014 [6], en la que resuelve, entre otras cosas:

- Disponer la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI) en la Empresa Eléctrica Quito S.A.
- Definir y difundir la política de seguridad de la información en toda la organización.
- Crear el Comité de Gestión de la Seguridad de la Información de la Empresa Eléctrica Quito S.A., el cual se encargará de la supervisión de dicha implementación.
- La especificación de las atribuciones y responsabilidades del Comité de Gestión de la Seguridad de la Información.
- La definición de los miembros del Comité de Gestión de la Seguridad de la Información de la Empresa Eléctrica Quito S.A.
- La definición de las responsabilidades del Oficial de Seguridad de la Información, de la Dirección de Tecnologías de la Información y Comunicaciones.

Posteriormente, el 04 de Septiembre de 2014, se emite una Reforma a la Resolución de Gerencia General No. GEG-2884-2014 del 16 de Abril de 2014 [7], en la que resuelve, modificar el Art 2 de dicha Resolución para mejorar alcance de la implementación.

ESQUEMA GUBERNAMENTAL DE LA SEGURIDAD DE LA INFORMACIÓN (EGSI)

A continuación se muestra un resumen del Esquema Gubernamental de Seguridad de la Información, el mismo que se encuentra como Anexo 1 del Acuerdo No. 166 del 19 de Septiembre de 2013.

Introducción

El Esquema Gubernamental de Seguridad de la Información, nació como respuesta a los avances en las Tecnologías de la Información y Comunicaciones (TIC), y a su vez, la necesidad de los gobiernos de salvaguardar sus activos de información de la ciudadanía manejados en sus instituciones y minimizar los riesgos que puedan existir.

"La Secretaría Nacional de Administración Pública, considerando que las TIC son herramientas imprescindibles para el desempeño institucional e inter-institucional, y como respuesta a la necesidad gestionar de forma eficiente y eficaz la seguridad de la formación en las entidades públicas, emitió los Acuerdos Ministeriales No. 804 y No. 837, de 29 de julio y 19 de agosto de 2011 respectivamente, mediante los cuales creó la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación. [8]"

El EGSI, está basado en la norma técnica ecuatoriana NTE-INEN ISO/IEC 27000:2009 para la Gestión de la Seguridad de la Información y está dirigido para las Instituciones de la Administración Pública Central, Dependiente e Institucional.

Se establece una serie de directrices o controles para la Gestión de la Seguridad de la Información, basado en la mejora continua en las instituciones en las que será aplicado. Cabe mencionar que el EGSI no reemplaza a la norma NTE-INEN ISO/IEC 27002:2009, sino que está diseñado en base a dicha norma.

El objetivo principal de la implementación del EGSI es incrementar la seguridad de la información en las entidades públicas, así como también, incrementar la

confianza de los ciudadanos que hacen uso de los servicios de dichas entidades.

Está conformado por:

1. Política de Seguridad de la Información
2. Organización de la Seguridad de la Información
3. Gestión de los Activos
4. Seguridad de los Recursos Humanos
5. Seguridad Física y del Entorno
6. Gestión de Comunicaciones y Operaciones
7. Control de Acceso
8. Adquisición, desarrollo y Mantenimiento de Sistemas de Información
9. Gestión de los Incidentes de la Seguridad de la Información
10. Gestión de la Continuidad del Negocio
11. Cumplimiento

Glosario de Términos.

1.3. ESPECIFICACIÓN DE LOS DOMINIOS DE LA NORMA ISO 27002 A UTILIZAR PARA LA EVALUACIÓN.

En base a la situación actual de la EEQ, mostrada en las secciones 1.1 y 1.2 de este documento, en esta sección se procede con la especificación de los dominios de la norma ISO 27002 a utilizar para la evaluación, pero se considera necesario presentar una breve descripción de la norma ISO 270002, así como también, de los CSCs de SANS Institute que servirán de apoyo en la evaluación.

Es necesario indicar que se utiliza a la norma ISO 27002 como base para la evaluación desarrollada en este proyecto de titulación, ya que la necesidad de la EEQ radicó en la evaluación de los niveles de cumplimiento en la implementación de las directrices del EGSI, mismo documento que está basado en la ISO 27002 y que al momento de la evaluación, la EEQ se encontraba en proceso de reestructuración del SGSI y aplicación del mismo a nivel organizacional, más no solo al proceso de comercialización como se había pensado originalmente.

No se considera la ISO 27004 para dicha evaluación ya que la misma incluye el uso de medidas y mediciones para evaluar la eficacia de un SGSI que está implementado en su totalidad en una organización.

1.3.1. NORMA ISO 27002

La Norma ISO 27002, o también ISO/IEC 27002, fue publicada por primera vez por la ISO (International Organization for Standardization) y la IEC (International Electrothecnical Comission) en el año 2005 con el nombre de ISO/IEC 17799:2000, bajo el título *Information technology - Security techniques - Code of practice for information security management*.

Esta norma, forma parte de la familia de normas SGSI (Sistema de Gestión de la Seguridad de la Información), INEN-ISO/IEC 27000, la cual tiene por objetivo común, la correcta creación y gestión del SGSI en una organización.

La norma ISO/IEC 27002, es un conjunto de recomendaciones de buenas prácticas enfocadas a una adecuada gestión de la seguridad de la información. Esta norma contiene varios dominios, objetivos de control y controles, dependiendo de la edición, que sirven de guía al personal de una organización, para iniciar, implantar y mantener SGSIs.

Objetivo de la norma ISO 27002

Según la página web iso27002.es [9], el objetivo de la norma ISO 27002 contempla:

- "Servir de punto de información de la serie de normas ISO 27000 y de la gestión de seguridad de la información mediante la aplicación de controles óptimos a las necesidades de las organizaciones en cada momento;
- Realizar la libre difusión de información en español en base a las investigaciones, conocimientos y búsquedas de los editores de la web;
- Responder a todas las consultas recibidas en relación a las normas de la serie ISO 27000, independientemente de su origen (empresas grandes, Pymes, organismos públicos, estudiantes, etc.;
- Establecer contactos con todo tipo de organizaciones, desarrolladores y personas relacionadas con la norma, con el objetivo de intercambiar informaciones, opiniones, experiencias o conocimientos, e impulsar la colaboración en actividades de fomento y promoción de las buenas prácticas para la aplicación de controles para la seguridad de la información."

Conformación de la norma ISO 27002

La norma ISO/IEC 27002:2005 está formada por 11 dominios, 39 Objetivos de control y 133 controles, los cuales están orientados la correcta gestión de la seguridad de la información.

Norma ISO 27002 en Ecuador

Esta norma se ha publicado en diferentes países, y en países como el nuestro se ha publicado bajo el nombre de Norma Técnica Ecuatoriana (NTE) ISO/IEC 27002.

Para éste proyecto de titulación, se utilizará la norma ISO/IEC 27002:2005, que corresponde a la versión en español lanzada en el 2005.

1.3.2 ESPECIFICACIÓN DE DOMINIOS DE LA ISO 27002, DIRECTRICES DEL EGSI Y CONTROLES DE CSC A UTILIZAR PARA LA EVALUACIÓN

Debido a la necesidad de evaluación y análisis de la situación actual de la EEQ, se ha decidido conjuntamente con el Oficial de Seguridad de la misma que se considerará al dominio **7. Gestión de Activos** de la norma ISO/IEC 27002:2005 como el control a evaluar en el presente proyecto de titulación.

Esta decisión se debe a que en la EEQ se mantiene un alto grado de confidencialidad con respecto a la entrega de información a personas ajenas a la organización. Además, se consideró que el dominio seleccionado para la evaluación, es uno de los más importantes de implementación.

Adicionalmente como complemento a la evaluación, se utilizaron varios de los controles establecidos por SANS Institute los mismos que servirán como referencia para aplicación de los controles de la ISO 27002.

Dominio 7. Gestión de Activos

El dominio 7. Gestión de Activos de la ISO/IEC 27002:2005, se enfoca en la identificación de los activos de la organización y a través de dicha identificación, la elaboración y control de inventarios para una mejor gestión de los mismos.

A continuación, se muestran los objetivos de control y controles del dominio especificado para la evaluación según la información publicada en el Anexo de ISO 27001 en español [9]:

Objetivo de control 7.1. Responsabilidad sobre los activos: Este objetivo de control indica que todos los activos de la organización deberían ser justificados y tener asignado un propietario. Los controles son los siguientes:

Control 7.1.1. Inventario de activos.

"Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes."

Control 7.1.2. Propiedad de los activos.

"Toda la información y activos asociados a los recursos para el tratamiento de la información deberían pertenecer a una parte designada de la Organización."

Control 7.1.3. Uso aceptable de los activos.

"Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información."

Objetivo de control 7.2. Clasificación de la información: Este objetivo de control indica que se debería clasificar la información para indicar la necesidad, prioridades y nivel de protección previsto para su tratamiento. Los controles son los siguientes:

Control 7.2.1. Directrices de clasificación.

"La información debería clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización".

Control 7.2.2. Etiquetado y manipulado de la información.

"Se debería desarrollar e implantar un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la Organización".

Además, como complemento para la evaluación, se utilizan los Controles Críticos de Seguridad de SANS, con el fin de dar a conocer las tareas que se deben realizar y la forma de realizar dichas tareas, para mitigar las amenazas más críticas en cuanto a la Seguridad de la Información.

Critical Security Controls de SANS Institute

El SANS Institute (SysAdmin Audit, Networking and Security Institute) [10], es una institución con ánimo de lucro fundada en el año de 1989 como una organización de búsqueda corporativa y de educación. Está conformada por más de 165.000 profesionales de la seguridad de la información alrededor del mundo, entre analistas, consultores, administradores de red, universitarios, agencias gubernamentales, entre otros.

SANS es la mayor y la más confiable de las fuentes en cuanto a formación y certificación en seguridad de la información en todo el mundo. Desarrolla, mantiene y pone a disposición, sin costo alguno, la mayor colección de documentos de investigación sobre diversos aspectos de la seguridad de la información.

Critical Security Controls (Controles Críticos de Seguridad)

Como parte de la información publicada por SANS Institute, los Critical Security Controls (CSCs) son una serie de 20 controles de seguridad que se centran en dar prioridad a las funciones eficaces de seguridad de la información, contra las últimas Amenazas Avanzadas Dirigidas, con énfasis en “What Works” (“Lo que funciona”), es decir, en controles de seguridad, donde los procesos, arquitecturas y servicios hayan demostrado eficacia en el uso del mundo real [11].

A continuación, se presenta una breve descripción de los objetivos de cada uno de los controles CSC [11]:

CSC 1. Inventario de dispositivos autorizados y no autorizados: Gestionar activamente (inventariar, rastrear y corregir) todos los dispositivos de hardware en la red para que sólo los dispositivos autorizados tengan acceso y los

dispositivos no autorizados y no administrados sean detectados y se les impida el acceso.

CSC 2. Inventario de software autorizado y no autorizado: Gestionar activamente (inventariar, rastrear y corregir) todo el software en la red, de forma que sólo el software autorizado está instalado y se pueda ejecutar, y que el software no autorizado y no administrado sea detectado y se le impida la instalación o ejecución.

CSC 3. Configuraciones de Seguridad para Hardware y Software en dispositivos móviles, laptops, estaciones de trabajo, y servidores: Establecer, implementar y gestionar activamente (rastrear, informar, corregir) la configuración de seguridad de las computadoras portátiles, servidores y estaciones de trabajo mediante la gestión de la configuración y un riguroso proceso de control de cambios, con el fin de evitar que los atacantes exploten servicios y ambientes vulnerables.

CSC 4. Evaluación de la vulnerabilidad continua y remediación: Adquirir, evaluar y tomar decisiones continuamente sobre la nueva información con el fin de identificar las vulnerabilidades, remediar, y minimizar las ventanas de oportunidad para los atacantes.

CSC 5. Defensa de malware: Controlar la instalación, difusión y ejecución de código malicioso en múltiples puntos de la empresa, al mismo tiempo que se optimiza el uso de la automatización para permitir una rápida actualización de la defensa, la recopilación de datos, y acción correctiva.

CSC 6. Seguridad en aplicaciones de software: Gestionar el ciclo de vida de seguridad de todo el software de desarrollo propio y adquirido con el fin de prevenir, detectar y corregir las debilidades en la seguridad.

CSC 7. Control de Acceso a Wireless: Utilizar procesos y herramientas para realizar un seguimiento, control, prevención y corrección del uso de seguridad de las redes inalámbricas de área local (LAN), puntos de acceso y sistemas inalámbricos de los clientes.

CSC 8. Capacidad de recuperación de datos: Utilizar procesos y herramientas para realizar copias de seguridad de la información crítica con una metodología probada para la recuperación oportuna de la misma

CSC 9. Evaluación de las habilidades de Seguridad y entrenamiento adecuado para llenar los vacíos: Para todas las funciones en la organización (priorizando las de misión crítica para el negocio y su seguridad), identificar los conocimientos específicos, destrezas y habilidades necesarias para apoyar la defensa de la empresa; desarrollar y ejecutar un plan integrado para evaluar, identificar las brechas, y remediar a través de programas de concienciación política, planificación de la organización, y formación.

CSC 10. Configuraciones Seguras para los dispositivos de red tales como firewalls, routers y switches: Establecer, implementar y gestionar activamente (rastrear, informar, corregir) la configuración de seguridad de los dispositivos de infraestructura de red utilizando una rigurosa gestión de la configuración y cambiar el proceso de control con el fin de evitar que los atacantes exploten servicios y ambientes vulnerables.

CSC 11. Limitación y control de los puertos, protocolos y servicios de red: Gestionar (rastrear, controlar y corregir) la utilización de los puertos, protocolos y servicios en los dispositivos conectados a la red, con el fin de minimizar las ventanas de vulnerabilidad disponibles para los atacantes.

CSC 12. Uso controlado de privilegios administrativos: Utilizar procesos y herramientas para realizar un seguimiento, control, prevención y corrección del uso, asignación y configuración de privilegios de administrador en los ordenadores, redes y aplicaciones.

CSC 13. Límites de Defensa: Detectar, prevenir y corregir el flujo de información en la transferencia de las redes, en los diferentes niveles de confianza con un enfoque en la seguridad de los datos que se dañan.

CSC 14. Mantenimiento, Monitoreo y Análisis de los registros de auditoría: Recoger, gestionar y analizar los registros de auditoría de eventos que podrían ayudar a detectar, comprender, o recuperarse de un ataque.

CSC 15. Acceso controlado en base a la necesidad de conocer: Utilizar procesos y herramientas para realizar un seguimiento, control, prevención y acceso seguro correcto para activos críticos (por ejemplo, información, recursos, sistemas), de acuerdo a la determinación formal de las personas, los equipos y las aplicaciones que tienen la necesidad y el derecho a acceder a estos activos críticos, basada en una clasificación aprobada previamente.

CSC 16. Monitoreo y Control de Cuenta: Gestionar activamente el ciclo de vida del sistema y de las cuentas de aplicaciones - su creación, el uso, la inactividad, la eliminación - con el fin de reducir al mínimo las oportunidades para los atacantes.

CSC 17. Protección de datos: Utilizar procesos y herramientas para evitar la exfiltración de datos, mitigar los efectos de los datos exfiltrados, y garantizar la privacidad e integridad de la información sensible.

CSC 18. Respuesta y Manejo de Incidentes: Proteger la información de la organización, así como su reputación, mediante el desarrollo e implementación de una infraestructura de respuesta a incidentes (por ejemplo, planes, roles definidos, capacitación, comunicaciones, de control de gestión) para descubrir rápidamente un ataque y luego efectivamente contener los daños, la erradicación de la presencia del atacante, y la restauración de la integridad de la red y sistemas.

CSC 19. Ingeniería de Seguridad de Redes: Hacer de la seguridad un atributo inherente de la empresa por la especificación, diseño y características del edificio en las que se permiten las operaciones de los sistemas de alta confianza al tiempo que niega o minimiza las oportunidades para los atacantes.

CSC 20. Pruebas de Penetración y Ejercicios Team Red: Poner a prueba la fortaleza general de las defensas de una organización (la tecnología, los procesos y las personas) mediante la simulación de los objetivos y acciones de un atacante.

Propuesta metodológica de evaluación.

La evaluación en este proyecto de titulación se basa en una propuesta metodológica desarrollada en base al criterio de la autora, la misma que se fundamenta en la revisión de la aplicación de las directrices del Esquema Gubernamental de la Seguridad de la Información (EGSI), tomando en cuenta los controles y objetivos de control establecidos en la norma ISO 27002. Además, se utilizan como propuesta de mejora, los Controles Críticos de Seguridad (CSCs) de SANS INSTITUTE.

Para llevar a cabo la evaluación, se elaboró la tabla 1.4 que muestra un mapeo o correlación entre el dominio seleccionado de la norma ISO 27002 para la evaluación, las directrices del EGSI y los controles de SANS INSTITUTE. Esta correlación, permitió la revisión de los niveles de cumplimiento a nivel de documentación, y de implementación de cada una de las directrices establecidas en el EGSI, las mismas que fueron elaboradas en base a la norma ISO 27002, por lo que también permitió la revisión de los niveles de cumplimiento de controles y objetivos de control de dicha norma.

Como complemento, se realizó también una revisión de los CSCs, y se propuso actividades de mejora para el proceso de implementación.

ISO/IEC 27002:2005			EGSI	SANS 20
Dominios	**Objetivos de Control**	**Controles**	**Controles a evaluar según EGSI**	**System Experts[4]**
7. Gestión de Activos	**7.1. Responsabilidad sobre los activos**	7.1.1. Inventario de activos	3.1.1. Inventario de activos primarios en formatos físicos y/o electrónicos 3.1.2. Inventario de activos de soporte de Hardware 3.1.3. Inventario de activos de soporte de Software 3.1.4. Inventario de activos de soporte de Redes	**CSC 1** **CSC 2**
		7.1.2. Responsable de los activos	3.2.1. Asignación de Responsables de los Activos 3.2.2. Consolidación inventarios de activos con sus responsables	**CSC 1** **CSC 2**
		7.1.3. Uso aceptable de los activos.	3.3.1. Reglamentar el uso de correo electrónico institucional 3.3.2. Reglamentar el acceso y uso de la Internet y sus aplicaciones/servicios 3.3.3. Reglamentar el uso de los sistemas de video – conferencia	**CSC 13**
	7.2. Clasificación de la información	7.2.1. Directrices de clasificación	3.4.1. Clasificar la información como pública o confidencial 3.4.2. Elaborar y aprobar un catálogo de clasificación de la información	**CSC 15**
		7.2.2. Etiquetado y manipulado de la información	3.5.1. Procedimientos de etiquetado de la información 3.5.2. Procedimientos para verificación de cumplimiento del proceso de etiquetado de información	**CSC 15** **CSC 17**

Tabla 1.4 Marco de evaluación para el proyecto de titulación[5]

[4] System Experts es un proveedor líder en servicios de consultoría de cumplimientos de TI y seguridad (http://systemexperts.com).
[5] Elaborado por la autora.

2. CAPÍTULO 2. EVALUACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE LA E.E.Q. S.A.

En este capítulo se realiza la evaluación del SGSI en la EEQ, conforme a la información recopilada en las secciones 1.1 y 1.2, tomando en cuenta el dominio de evaluación establecido en la sección 1.3 de este documento.

2.1. APLICACIÓN DE LOS DOMINIOS DE LA NORMA ISO 27002 SELECCIONADOS AL S.G.S.I. DE LA E.E.Q.

eD acuerdo a lo indicado en la sección 1.3.2, en este proyecto de titulación se evaluará únicamente el dominio 7 de la norma ISO/IEC 27002, el cual corresponde a la **Gestión de Activos.**

Además, debido a las normativas establecidas en la Constitución de la República del Ecuador, toda empresa que pertenezca a los sectores estratégicos, de decisión y control exclusivo del Estado Ecuatoriano, deberán implementar el SGSI en base a las directrices establecidas en el EGSI publicado por la SNAP.

2.1.1. RECOLECCIÓN DE INFORMACIÓN

Debido a las normativas internas, no toda la información de la EEQ puede ser entregada en su totalidad a entes externos a la misma, por ésta razón, el proceso de recolección de información se llevó a cabo mediante entrevistas personales, así como también mediante el uso del correo electrónico y la consulta de la información publicada en la página web de la EEQ, la misma que es de carácter público.

Las entrevistas personales fueron sobre temas puntuales y se llevaron a cabo en las instalaciones de la EEQ, con el Oficial de Seguridad de la Información, y

en una ocasión con el Asesor de Gerencia, con la finalidad de dar a conocer el alcance de este proyecto de titulación, y de recabar la información necesaria para llevar a cabo el análisis objetivo de dicho proyecto de titulación. En las reuniones se convino evaluar únicamente el Dominio 7. Gestión de Activos, en base a necesidades propias de la organización.

Para la recolección de información se elaboraron las tablas de cumplimiento de la 2.1 a la 2.17 que incluyen una correlación entre el dominio a evaluar de la ISO/IEC 27002, es decir, el dominio 7.Gestión de Activos, y los controles de evaluación del EGSI relacionados a dicho dominio:

(ISO/IEC 27002:2005) 7. GESTIÓN DE ACTIVOS		EGSI		DOCUMENTACIÓN				IMPLEMENTACIÓN			
Objetivo de control	Control	EGSI	Aspectos a Evaluar	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento
7.1. Responsabilidad sobre los activos	7.1.1. Inventario de activos	3.1.1. Inventario de activos primarios en formatos físicos y/o electrónicos	3.1.1.1. Los procesos estratégicos, claves y de apoyo de la institución.	x			Existe documentación al respecto y está contenida en el listado de Activos de Información, y en la documentación publicada en la página w eb de la EEQ (PLAN ESTRATÉGICO 2012-2015).		x		Se cuenta con la información publicada y documentada pero no se ha elaborado un Inventario de Activos Primarios en donde conste dicha información.
			3.1.1.2. Las normas y reglamentos que son la razón de ser de la institución.	x			Existe documentación al respecto y está contenida en el listado de Activos de Información, y en la documentación publicada en la página w eb de la EEQ (PLAN ESTRATÉGICO 2012-2015).		x		Se cuenta con la información publicada pero no se ha elaborado un Inventario de Activos Primarios en donde conste dicha información.
			3.1.1.3. Planes estratégicos y operativos de la institución y áreas específicas.	x			Existe documentación al respecto y está contenida en el listado de Activos de Información, y en la documentación publicada en la página w eb de la EEQ (PLAN ESTRATÉGICO 2012-2015).		x		Se cuenta con la información publicada pero no se ha elaborado un Inventario de Activos Primarios en donde conste dicha información.
			3.1.1.4. Los archivos generados por los servidores públicos, tanto de manera física como electrónica, razón de ser de la función que desempeñan en la institución.	x			La información generada por los funcionarios y trabajadores se encuentra disponible en el sistema QUIPUX.		x		Se cuenta con la información publicada pero no se ha elaborado un Inventario de Activos Primarios en donde conste dicha información.
			3.1.1.5. Los manuales e instructivos de sistemas informáticos: instalación, guía de usuario, operación, administración, mantenimiento, entre otros.	x			Existe documentación al respecto y es gestionada por la Dirección de Tecnología de la Información y Comunicaciones	x			Información contenida en un Inventario gestionado por la DTIC, el cual no fue provisto para su respectiva evaluación.

Tabla 2.1 Tabla de recolección de información – Inventario de activos (Parte 1)[6]

[6] Elaborado por la autora

(ISO/IEC 27002:2005) 7. GESTIÓN DE ACTIVOS		EGSI		DOCUMENTACIÓN				IMPLEMENTACIÓN			
Objetivo de control	Control	EGSI	Aspectos a Evaluar	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento
7.1. Responsabilidad sobre los activos	7.1.1. Inventario de activos	3.1.1. Inventario de activos primarios en formatos físicos y/o electrónicos	3.1.1.6. De la operación de los aplicativos informáticos de los servicios informáticos: datos y meta-datos asociados, archivos de configuración, código fuente, respaldos, versiones, etc.	x			Existe documentación al respecto y es gestionada por la Dirección de Tecnología de la Información y Comunicaciones	x			Información contenida en un Inventario gestionado por la DTIC, el cual no fue provisto para su respectiva evaluación.
			3.1.1.7. Del desarrollo de aplicativos de los servicios informáticos: actas de levantamiento de requerimientos, documento de análisis de requerimientos, modelos entidad - relación, diseño de componentes, casos de uso, diagramas de uso, diagramas de flujo y estado, casos de prueba, etc.	x			Existe documentación al respecto y es gestionada por la Dirección de Tecnología de la Información y Comunicaciones	x			Información contenida en un Inventario gestionado por la DTIC, el cual no fue provisto para su respectiva evaluación.
			3.1.1.8. Del soporte de aplicativos de los servicios informáticos: tickets de soporte, reportes físicos y electrónicos, evaluaciones y encuestas, libros de trabajo para capacitación, etc.	x			Existe documentación al respecto y es gestionada por la Dirección de Tecnología de la Información y Comunicaciones.	x			Información contenida en un Inventario gestionado por la DTIC, el cual no fue provisto para su respectiva evaluación.
			3.1.1.9.De la imagen corporativa de la institución: manual corporativo (que incluye manual de marca y fuentes en formato electrónico de logos), archivos multimedia, tarjetas de presentación, volantes, banners, trípticos, etc.	x			Existe documentación al respecto y es gestionada por la Dirección de Comunicación Social.		x		La información es gestionada por la Dirección de Comunicación Social pero no se ha elaborado un Inventario de Activos Primarios en donde conste dicha información.

Tabla 2.2 Tabla de recolección de información – Inventario de activos (Parte 2)[7]

[7] Elaborado por la autora

(ISO/IEC 27002:2005) 7. GESTIÓN DE ACTIVOS		EGSI		DOCUMENTACIÓN				IMPLEMENTACIÓN			
Objetivo de control	Control	EGSI	Aspectos a Evaluar	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento
7.1. Responsabilidad sobre los activos	7.1.1. Inventario de activos	3.1.2. Inventario de activos de soporte de Hardware	3.1.2.1. Equipos móviles: teléfono inteligente (smartphone), teléfono celular, tableta, computador portátil, asistente digital personal (PDA), etc.			x	Información en el Inventario de Equipos Activos en la Empresa Eléctrica. Está pendiente añadir a dicho inventario la información sobre teléfonos celulares y teléfonos celulares inteligentes.			x	Información contenida en un inventario denominado Equipos Activos en la Empresa Eléctrica, en el cual no costa la información de teléfonos celulares y teléfonos celulares inteligentes (pendiente de inclusión).
			3.1.2.2. Equipos fijos: servidor de torre, servidor de cuchilla, servidor de rack, computador de escritorio, computadoras portátiles, etc.	x			Información en el Inventario de Equipos Activos en la Empresa Eléctrica. Información de servidores contenida en el Inventario de Activos de Plataforma.	x			Información contenida en un inventario denominado Equipos Activos en la Empresa Eléctrica, en el cual constan más de 5000 registros.
			3.1.2.3. Periféricos de entrada: teclado, ratón, micrófono, escáner plano, escáner de mano, cámara digital, cámara w eb, lápiz óptico, pantalla de toque, etc.	x			Información contenida en el Inventario de Equipos Activos en la Empresa Eléctrica (Contiene código del bien, descripción, fecha de adquisición, número de rol y nombre de la persona responsable del activo).	x			Información contenida en un inventario denominado Equipos Activos en la Empresa Eléctrica, en el cual constan más de 5000 registros.
			3.1.2.4. Periféricos de salida: monitor, proyector, audífonos, parlantes, impresora láser, impresora de inyección de tinta, impresora matricial, impresora térmica, plotter, máquina de fax, etc.	x			Información en el Inventario de Equipos Activos en la Empresa Eléctrica (Contiene código del bien, descripción, fecha de adquisición, número de rol y nombre de la persona responsable del activo).	x			Información contenida en un inventario denominado Equipos Activos en la Empresa Eléctrica, en el cual constan más de 5000 registros.

Tabla 2.3 Tabla de recolección de información – Inventario de activos (Parte 3)[8]

[8] Elaborado por la autora

(ISO/IEC 27002:2005) 7. GESTIÓN DE ACTIVOS		EGSI		DOCUMENTACIÓN				IMPLEMENTACIÓN			
Objetivo de control	Control	EGSI	Aspectos a Evaluar	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento
7.1. Responsabilidad sobre los activos	7.1.1. Inventario de activos	3.1.2. Inventario de activos de soporte de Hardware	3.1.2.5. Periféricos y dispositivos de almacenamiento: sistema de almacenamiento (NAS, SAN), librería de cintas, cintas magnéticas, disco duro portátil, disco flexible, grabador de discos (CD, DVD, Blu-ray), CD, DVD, Blu-ray, memoria USB, etc.	x			Información en el Inventario de Equipos Activos en la Empresa Eléctrica (Contiene código del bien, descripción, fecha de adquisición, número de rol y nombre de la persona responsable del activo). Información de SANs, NASs y librerías de cintas, contenida en el Inventario de Activos de Plataforma.	x			Información contenida en un inventario denominado Equipos Activos en la Empresa Eléctrica, en el cual constan más de 5000 registros. La información de SANs, NASs y librerías de cintas está contenida en otro inventario denominado Inventario de Activos de Plataforma.
			3.1.2.6. Periféricos de comunicaciones: tarjeta USB para redes inalámbricas (Wi-Fi, Bluetooth, GPRS, HSDPA), tarjeta PCMCIA para redes inalámbricas (Wi-Fi, Bluetooth, GPRS, HSDPA), tarjeta USB para redes alámbricas/inalámbricas de datos y de telefonía,etc.	x			Información en el Inventario de Equipos Activos en la Empresa Eléctrica (Contiene código del bien, descripción, fecha de adquisición, número de rol y nombre de la persona responsable del activo).	x			Información contenida en un inventario denominado Equipos Activos en la Empresa Eléctrica, en el cual constan más de 5000 registros.
			3.1.2.7. Tableros: de transferencia (bypass) de la unidad ininterrumpible de energía (UPS), de salidas de energía eléctrica, de transferencia automática de energía, etc.	x			Información en el Inventario de Equipos Activos en la Empresa Eléctrica (Contiene código del bien, descripción, fecha de adquisición, número de rol y nombre de la persona responsable del activo).	x			Información contenida en un inventario denominado Equipos Activos en la Empresa Eléctrica, en el cual constan más de 5000 registros.
			3.1.2.8.Sistemas: de control de accesos, de aire acondicionado, automático de extinción de incendios, de circuito cerrado de televisión, etc.	x			Información en el Inventario de Activos de Plataforma. La información de los sistemas de control de accesos se almacena en los centros de datos.	x			Información en inventario denominado Inventario de Activos de Plataforma. No consta la información de los sistemas de control de accesos.

Tabla 2.4 Tabla de recolección de información – Inventario de activos (Parte 4)[9]

[9] Elaborado por la autora

(ISO/IEC 27002:2005) 7. GESTIÓN DE ACTIVOS		EGSI		DOCUMENTACIÓN				IMPLEMENTACIÓN			
Objetivo de control	Control	EGSI	Aspectos a Evaluar	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento
7.1. Responsabilidad sobre los activos	7.1.1. Inventario de activos	3.1.3. Inventario de activos de soporte de Software	3.1.3.1. Sistemas Operativos	x			Información en el Inventario de Equipos Activos en la Empresa Eléctrica. Información en el documento denominado Políticas para el uso y manejo de recursos informáticos (TI-D001), sección 9.1. Anexos - Listado de Software Autorizado. Información en el Inventario de Plataforma.	x			Información contenida en los inventarios Equipos Activos de la Empresa Eléctrica y en el Inventario de Plataforma.
			3.1.3.2. Software de servicio, mantenimiento o administración de: gabinetes de servidores de cuchilla, servidores (estantería/rack, torre, virtuales), sistema de redes de datos, sistemas de almacenamiento (NAS, SAN), telefonía, sistemas (de UPS, grupo de electrógeno, de aire acondicionado, automático de extinción de incendios, de circuito cerrado de televisión), etc.	x			Información en el documento denominado Procedimiento para administración de redes y comunicaciones (TI-GRC-P001). Información en el documento denominado Políticas para el uso y manejo de recursos informáticos (TI-D001), sección 9.1. Anexos - Listado de Software Autorizado. Documentación en el Inventario de Plataforma.			x	Información parcial contenida en el denominado Inventario de Plataforma
			3.1.3.3. Paquetes de software o software base de: suite de ofimática, navegador de Internet, cliente de correo electrónico, mensajería instantánea, edición de imágenes, video conferencia, servidor (proxy, de archivos, de correo electrónico, de impresiones, de mensajería instantánea, de aplicaciones, de base de datos), etc.	x			Información en el documento Inventario de Equipos Activos en la Empresa Eléctrica. Información en el documento Inventario de Activos de Plataforma. Información actualizada en el documento de Políticas para el uso y manejo de recursos informáticos (TI-D001), sección 9.1. Anexos - Listado de Software Autorizado.	x			Información contenida en el denominado Inventario de Plataforma
			3.1.3.4. Aplicativos informáticos del negocio.	x			Información actualizada contenida en el documento de Políticas para el uso y manejo de recursos informáticos (TI-D001), sección 9.1. Anexos - Listado de Software Autorizado (Aplicaciones desarrolladas).		x		Información no contenida en Inventario

Tabla 2.5 Tabla de recolección de información – Inventario de activos (Parte 5)[10]

[10] Elaborado por la autora

(ISO/IEC 27002:2005) 7. GESTIÓN DE ACTIVOS		EGSI		DOCUMENTACIÓN				IMPLEMENTACIÓN			
Objetivo de control	Control	EGSI	Aspectos a Evaluar	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento
7.1. Responsabilidad sobre los activos	7.1.1. Inventario de activos	3.1.4. Inventario de activos de soporte de redes	3.1.4.1. Cables de comunicaciones (interfaces: RJ-45 o RJ-11, SC, ST o MT-RJ, interfaz V35, RS232, USB, SCSI, LTP), panel de conexión (patch panel), tomas o puntos de red, racks (cerrado o abierto, de piso o pared), etc.			x	En el Inventario de Activos de Plataforma y en el Inventario de Equipos Activos de la Empresa Eléctrica, hay información generalizada de los cables de comunicaciones, sin embargo no hay un detalle de cada uno de los cables, ni éstos tienen codificación alguna.			x	Información parcial generalizada contenida en los inventarios Equipos Activos de la Empresa Eléctrica y en el Inventario de Plataforma.
			3.1.4.2. Switches (de centros de datos, de acceso, de borde, de gabinete de servidores, access-point, transceiver, equipo terminal de datos, etc).	x			Información en el Inventario de Equipos Activos en la Empresa Eléctrica (Contiene código del bien, descripción, fecha de adquisición, número de rol y nombre de la persona responsable del activo). Información en los gráficos del Procedimiento para administración de redes y comunicaciones (TI-GRC-P001).	x			Información contenida en el Inventario Equipos Activos de la Empresa Eléctrica
			3.1.4.3. Ruteador (router), cortafuego (firewall), controlador de red inalámbrica, etc.	x			Información contenida en el Inventario de Equipos Activos en la Empresa Eléctrica (Contiene código del bien, descripción, fecha de adquisición, número de rol y nombre de la persona responsable del activo).	x			Información contenida en el Inventario Equipos Activos de la Empresa Eléctrica
			3.1.4.4. Sistema de detección/prevención de intrusos (IDS/IPS), firewall de aplicaciones web, balanceador de carga, switch de contenido, etc.	x			Información en el Inventario de Equipos Activos en la Empresa Eléctrica (Contiene código del bien, descripción, fecha de adquisición, número de rol y nombre de la persona responsable del activo).	x			Información contenida en el Inventario Equipos Activos de la Empresa Eléctrica

Tabla 2.6 Tabla de recolección de información – Inventario de activos (Parte 6)[11]

[11] Elaborado por la autora

(ISO/IEC 27002:2005) 7. GESTIÓN DE ACTIVOS		EGSI		DOCUMENTACIÓN				IMPLEMENTACIÓN			
Objetivo de control	Control	EGSI	Aspectos a Evaluar	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento
7.1. Responsabilidad sobre los activos	7.1.2. Responsable de los activos	3.2.1. Asignación de Responsables de los activos (tareas de cada responsable)	3.2.1.1.Elaborar el inventario de los activos a su cargo y debe mantenerlo actualizado			x	Información en el Inventario de Equipos Activos en la Empresa Eléctrica. Información en el Instructivo para el Control de Bienes, anexo del documento Procedimiento para Control de Bienes (GR-GBB-P003), sección 4. Mantenimiento y control de activos.		x		Cada responsable del activo no realiza un inventario de los activos a su cargo, sin embargo, en el documento inventario de Equipos Activos de la Empresa Eléctrica, se define el nombre del responsable de cada uno de los activos
			3.2.1.2. Delegar de tareas rutinarias, tomando en cuenta que la responsabilidad sigue siendo del responsable			x	Incluido en el documento de Políticas para el uso y manejo de los recursos informáticos de la EEQ, (TI-D001). Información en el Instructivo para el Control de Bienes (GR-GBB-P003), sección 4. Mantenimiento y control de activos.	x			En el documento Políticas para el uso y manejo de recursos informáticos se definen políticas y procedimientos que debe seguir el responsable del activo, para la administración de los activos a su cargo.
			3.2.1.3. Administrar la información dentro de los procesos de la institución a los cuales ha sido asignado.	x			Información en el documento de Políticas para el uso y manejo de recursos informáticos (TI-D001), sección 6. Políticas, Políticas de Seguridad de la Información y Políticas de control de acceso.	x			En el documento Políticas para el uso y manejo de recursos informáticos se definen políticas y procedimientos para la administración de la información a cargo de cada responsable.
			3.2.1.4. Elaborar las reglas para el uso aceptable del mismo e implantarlas previa autorización de la autoridad correspondiente.			x	Incluido en el Instructivo para el Control de Bienes, anexo del documento Procedimiento para Control de Bienes (GR-GBB-P003). Contiene procedimientos para altas, traspasos, bajas y destino final de los bienes de la EEQ y asignación de responsabilidades de mantenimiento y control de bienes. Información en el documento de Políticas para el uso y manejo de recursos informáticos (TI-D001), sección 6. Políticas, Políticas Detalladas.	x			Las reglas para el uso aceptable del activo están definidas en el Instructivo para control de bienes, el cual contiene procedimientos para la administración de los mismos. Además, en el documento Políticas para el uso y manejo de recursos informáticos, constan políticas y procedimientos para el uso aceptable de los activo, en la sección 6.
			3.2.1.5. Clasificar, documentar y mantener actualizada la información y los activos, y definir los permisos de acceso a la información.			x	Información en el Listado de Activos de Información, el cual contiene 251 activos con sus responsables, de éstos, 54 son considerados como activos críticos e incluye un perfil del responsable en donde termina el trato de la información.			x	En el documento, Listado de Activos de Información constan 251 activos clasificados como activos críticos. El resto de información no ha sido completamente clasificada.

Tabla 2.7 Tabla de recolección de información –Responsable de los activos (Parte 1)[12]

[12] Elaborado por la autora

(ISO/IEC 27002:2005) 7. GESTIÓN DE ACTIVOS		EGSI		DOCUMENTACIÓN				IMPLEMENTACIÓN			
Objetivo de control	Control	EGSI	Aspectos a Evaluar	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento
7.1. Responsabilidad sobre los activos	7.1.2. Responsable de los activos	*3.2.2. Consolidación de inventarios de activos con sus responsables*	3.2.2.1. Consolidación de los inventarios de los activos a cargo del Responsable del Activo, por área o unidad organizacional.	x			Información en el Inventario de Equipos Activos en la Empresa Eléctrica (Contiene código del bien, descripción, fecha de adquisición, número de rol y nombre de la persona responsable del activo). Información contenida en el Instructivo de Control de Bienes y en el Procedimiento para Control de Bienes.		x		No se cuenta con documentación de consolidación de inventarios de Responsables y activos a su cargo por área o unidad organizacional. Únicamente se ingresa en el Inventario de Equipos Activos de la Empresa Eléctrica, el nombre y número de rol del responsable de cada activo.
	7.1.3. Uso aceptable de los activos	*3.3.1. Identificar documentar e implementar las reglas sobre el uso aceptable de los activos asociados con los servicios de procesamiento de la información.*	3.3.1.1. Para la elaboración de las reglas, el Responsable del Activo deberá tomar en cuenta las actividades definidas en los controles correspondientes a los ámbitos de "Intercambio de Información" y "Control de Acceso", donde sea aplicable.		x		Información en el Instructivo de Control de Bienes y en el Procedimiento para Control de Bienes. Las reglas son definidas por TI y por Control de Bienes en base a las necesidades globales de la organización.		x		El responsable del activo no es el encargado de la definición de reglas sobre el uso aceptable de los activos. Los responsables de definirlas son las áreas de TI y Control de Bienes.
		3.3.2. El oficial de Seguridad de la Información es el encargado de asegurar los lineamientos para la utilización de los recursos de las Tecnologías de la Información contemplen los requerimientos de seguridad establecida, según la criticidad de la información que procesan.				x	Los lineamientos para la utilización de los recursos de las Tecnologías de Información, antes de la contratación del personal para Oficial de Seguridad, eran gestionados por la DTIC, y se los definían en base a las necesidades de cada área de trabajo.			x	Los lineamientos para la utilización de los recursos de las Tecnologías de Información, antes de la contratación del personal para Oficial de Seguridad, eran gestionados por la DTIC, y se los definían en base a las necesidades de cada área de trabajo.
		3.3.3.La información y documentos generados en la institución y enviados por cualquier medio o herramienta electrónica con propiedad de la información que procesan.		x			Toda la información que es generada y procesada por los funcionarios y trabajadores de la EEQ se almacena y está disponible en el sistema QUIPUX [22].			x	Toda la información que es generada y procesada por los funcionarios y trabajadores de la EEQ se almacena y está disponible en el sistema QUIPUX.

Tabla 2.8 Tabla de recolección de información – Responsable de los activos (Parte 2) / Uso aceptable de los activos (Parte 1) [13]

[13] Elaborado por la autora

(ISO/IEC 27002:2005) 7. GESTIÓN DE ACTIVOS		EGSI		DOCUMENTACIÓN				IMPLEMENTACIÓN			
Objetivo de control	Control	EGSI	Aspectos a Evaluar	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento
7.1. Responsabilidad sobre los activos	7.1.3. Uso aceptable de los activos	*3.3.4. Reglamentar el uso de correo electrónico institucional*	3.3.4.1. Este servicio debe utilizarse exclusivamente para las tareas propias de las funciones que se desarrollan en la institución y no debe utilizarse para ningún otro fin.	x			Incluido en el Procedimiento Administración de Servicios Internet y Correo, disponible en el Sistema de Gestión de la Calidad. Contiene políticas para creación de usuarios, estructura de contraseñas; procedimientos para solicitudes de acceso a Internet o correo electrónico; procedimiento de creación de usuarios; procedimiento para acceso a Internet en el firewall de la EEQ; Como anexo incluye un acta de compromiso para el buen uso del servicio de Internet de la EEQ.	x			En el documento Procedimiento Administración de Servicios Internet y Correo (TI-GBD-P004), se definen políticas y procedimientos para el uso aceptable de servicios de Internet y Correo Electrónico, en donde se indica que dichos servicios deben ser utilizados únicamente para tareas propias de la organización.
			3.3.4.2. Cada persona es responsable tanto del contenido del mensaje enviado como de cualquier otra información que adjunte.	x			Incluido en el Procedimiento Administración de Servicios Internet y Correo, disponible en el Sistema de Gestión de la Calidad. Contiene políticas para creación de usuarios, estructura de contraseñas; procedimientos para solicitudes de acceso a Internet o correo electrónico; procedimiento de creación de usuarios; procedimiento para acceso a Internet en el firewall de la EEQ; **Como anexo incluye un acta de compromiso para el buen uso del servicio de Internet de la EEQ.**	x			El documento Procedimiento Administración de Servicios Internet y Correo (TI-GBD-P004), contiene como anexo un acta de compromiso para el buen uso del servicio de Internet de la EEQ, en donde se le indica a cada usuario que es responsable del tráfico de información que genere.
			3.3.4.3. Todos los mensajes deben poder ser monitoreados y conservados permanentemente por parte de la institución.		x		No se monitorea la información ni tampoco es almacenada sino en cada equipo en el caso del correo electrónico, en cada bandeja de correo.		x		No se monitorea la información ni tampoco es almacenada sino en cada equipo en el caso del correo electrónico, en cada bandeja de correo.
			3.3.4.4. Toda cuenta de correo electrónico debe estar asociada a una única cuenta de usuario.	x			Incluido en el Procedimiento Administración de Servicios Internet y Correo, disponible en el Sistema de Gestión de la Calidad. Contiene políticas para creación de usuarios, estructura de contraseñas; procedimientos para solicitudes de acceso a Internet o correo electrónico; procedimiento de creación de usuarios; procedimiento para acceso a Internet en el firewall de la EEQ; Como anexo incluye un acta de compromiso para el buen uso del servicio de Internet de la EEQ.	x			Cada cuenta de correo es asociada a una única cuenta de usuario, definida por el número de rol del personal. Esto está establecido en el documento Procedimiento Administración de Servicios Internet y Correo (TI-GBD-P004).

Tabla 2.9 Tabla de recolección de información – Uso aceptable de los activos (Parte 2)[14]

[14] Elaborado por la autora

(ISO/IEC 27002:2005) 7. GESTIÓN DE ACTIVOS		EGSI		DOCUMENTACIÓN				IMPLEMENTACIÓN			
Objetivo de control	Control	EGSI	Aspectos a Evaluar	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento
7.1. Responsabilidad sobre los activos	7.1.3. Uso aceptable de los activos	*3.3.4. Reglamentar el uso de correo electrónico institucional*	3.3.4.5 La conservación de los mensajes se efectuará en carpetas personales, para archivar la información de acceso exclusivo del usuario y que no debe compartirse con otros usuarios. Debe definirse un límite de espacio máximo.		x		Los mensajes son conservados únicamente dentro de los equipos de cada usuario, más no a nivel institucional.		x		Los mensajes son conservados únicamente dentro de los equipos de cada usuario, más no a nivel institucional.
			3.3.4.6. Toda la información debe ser gestionada de forma centralizada y no en las estaciones de trabajo de los usuarios.		x		La información se gestiona en cada equipo.		x		La información es gestionada en cada equipo, más no a nivel centralizado.
			3.3.4.7. Todo sistema debe contar con las facilidades automáticas que notifiquen al usuario cuando un mensaje enviado por él no es recibido correctamente por el destinatario, describiendo detalladamente el motivo del error.		x		No se cuenta con sistemas de notificación cuando el mensaje que se envía no es correctamente recibido por el receptor.		x		No se cuenta con sistemas de notificación cuando el mensaje que se envía no es correctamente recibido por el receptor.
			3.3.4.8. Deben utilizarse programas que monitoreen el accionar de virus informáticos tanto en mensajes como en archivos adjuntos, antes de su ejecución.			x	Se utiliza un software de antivirus de plataforma integral.			x	Únicamente se utiliza el software de plataforma.

Tabla 2.10 Tabla de recolección de información – Uso aceptable de los activos (Parte 3)[15]

[15] Elaborado por la autora

(ISO/IEC 27002:2005) 7. GESTIÓN DE ACTIVOS		EGSI		DOCUMENTACIÓN				IMPLEMENTACIÓN			
Objetivo de control	Control	EGSI	Aspectos a Evaluar	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento
7.1. Responsabilidad sobre los activos	7.1.3. Uso aceptable de los activos	*3.3.4. Reglamentar el uso de correo electrónico institucional*	3.3.4.9. Todo usuario es responsable por la destrucción de los mensajes con origen desconocido, y asume la responsabilidad por las consecuencias que pueda ocasionar la ejecución de los archivos adjuntos. En estos casos, no deben contestar dichos mensajes y deben enviar una copia al Oficial de Seguridad de la Información para que se efectúe el seguimiento y la investigación necesaria.	x			Incluido en el Procedimiento Administración de Servicios Internet y Correo, disponible en el Sistema de Gestión de la Calidad. Contiene políticas para creación de usuarios, estructura de contraseñas; procedimientos para solicitudes de acceso a Internet o correo electrónico; procedimiento de creación de usuarios; procedimiento para acceso a Internet en el firew all de la EEQ; **Como anexo incluye un acta de compromiso para el buen uso del servicio de Internet de la EEQ.**	x			En el documento Procedimiento Administración de Servicios Internet y Correo (TI-GBD-P004), se definen políticas y procedimientos que indican que cada usuario es responsable de los mensajes que genere o reciba y de la ejecución de archivos adjuntos maliciosos. Se incluyen estas definiciones en el acta de compromiso para el buen uso del servicio de Internet de la EEQ.
			3.3.4.10. Para el envío y la conservación de la información, debe implementarse el cifrado (criptografía) de datos.			x	Se hace uso de HTTPS para la transmisión de información.			x	No se encripta la información, pero se hace uso de HTTPS para la transmisión de la misma.
			3.3.4.1.11. Todo usuario es responsable de la cantidad y tamaño de mensajes que envíe. Debe controlarse el envío no autorizado de correos masivos.	x			Incluido en el Procedimiento Administración de Servicios Internet y Correo, disponible en el Sistema de Gestión de la Calidad. Contiene políticas para creación de usuarios, estructura de contraseñas; procedimientos para solicitudes de acceso a Internet o correo electrónico; procedimiento de creación de usuarios; procedimiento para acceso a Internet en el firew all de la EEQ; **Como anexo incluye un acta de compromiso para el buen uso del servicio de Internet de la EEQ.**	x			En el documento Procedimiento Administración de Servicios Internet y Correo (TI-GBD-P004), se definen políticas y procedimientos que indican que cada usuario es responsable de los mensajes que genere o reciba. Se incluyen estas definiciones en el acta de compromiso para el buen uso del servicio de Internet de la EEQ.

Tabla 2.11 Tabla de recolección de información – Uso aceptable de los activos (Parte 4)[16]

[16] Elaborado por la autora

(ISO/IEC 27002:2005) 7. GESTIÓN DE ACTIVOS		EGSI		DOCUMENTACIÓN				IMPLEMENTACIÓN			
Objetivo de control	Control	EGSI	Aspectos a Evaluar	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento
7.1. Responsabilidad sobre los activos	7.1.3. Uso aceptable de los activos	*3.3.5. Reglamentar el acceso y uso de la Internet y sus aplicaciones/servicios*	3.3.5.1. Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en la institución, y no debe utilizarse para ningún otro fin.	x			Incluido en el Procedimiento Administración de Servicios Internet y Correo, disponible en el Sistema de Gestión de la Calidad. Contiene políticas para creación de usuarios, estructura de contraseñas; procedimientos para solicitudes de acceso a Internet o correo electrónico; procedimiento de creación de usuarios; procedimiento para acceso a Internet en el firewall de la EEQ; **Como anexo incluye un acta de compromiso para el buen uso del servicio de Internet de la EEQ.**	x			En el documento Procedimiento Administración de Servicios Internet y Correo (TI-GBD-P004), se definen políticas y procedimientos para el uso adecuado del Internet y Correo Electrónico. Se incluyen estas definiciones en el acta de compromiso para el buen uso del servicio de Internet de la EEQ.
			3.3.5.2. Cada usuario es responsable de la información y contenidos a los que accede y de aquella que copia para conservación en los equipos de la institución.	x			Información en el documento de Políticas para el uso y manejo de recursos informáticos, sección 6. Políticas, Políticas de Seguridad de la Información y Políticas de control de acceso.	x			En el documento Políticas para el uso y manejo de recursos informáticos (T-D001), se indica que cada usuario es responsable de la información a la que accede a través de Internet (Políticas de control de acceso). En el documento Procedimiento Administración de Servicios Internet y Correo (TI-GBD-P004), se definen políticas y procedimientos para el uso adecuado del Internet y Correo Electrónico. Se incluyen estas definiciones en el acta de compromiso para el buen uso del servicio de Internet de la EEQ.
			3.3.5.3. Debe limitarse a los usuarios el acceso a portales, aplicaciones o servicios de la Internet y la Web que pudieren perjudicar los intereses y reputación de la institución. Específicamente, se debe bloquear el acceso por medio de dispositivos físicos y/o móviles a aquellos portales, aplicaciones o servicios de la Internet y la Web sobre pornografía, racismo, violencia, delincuencia o de contenidos ofensivos y contrarios a los intereses, entre otros, y valores de la institución o que impacten negativamente en la productividad y trabajo de la institución.	x			Información contenida en el documento de Políticas para el uso y manejo de recursos informáticos, sección 6. Políticas, Políticas de Seguridad de la Información y Políticas de control de acceso.	x			En el documento Políticas para el uso y manejo de recursos informáticos (T-D001), se indica que cada usuario es responsable de la información a la que accede a través de Internet (Políticas de control de acceso).

Tabla 2.12 Tabla de recolección de información – Uso aceptable de los activos (Parte 5)[17]

[17] Elaborado por la autora

(ISO/IEC 27002:2005) 7. GESTIÓN DE ACTIVOS		EGSI		DOCUMENTACIÓN				IMPLEMENTACIÓN			
Objetivo de control	Control	EGSI	Aspectos a Evaluar	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento
7.1. Responsabilidad sobre los activos	7.1.3. Uso aceptable de los activos	*3.3.5. Reglamentar el acceso y uso de la Internet y sus aplicaciones/servicios*	3.3.5.4. El Oficial de Seguridad de la Información debe elaborar, poner en marcha y controlar la aplicación de un procedimiento institucional para acceso y uso de la Internet y la Web por parte de todo funcionario sin excepción, y en el cual se acepten las condiciones aquí especificadas y otras que la institución considere apropiadas..	x			Información contenida en el documento de Políticas para el uso y manejo de recursos informáticos, sección 6. Políticas, Políticas de Seguridad de la Información y Políticas de control de acceso.	x			En el documento Políticas para el uso y manejo de recursos informáticos (T-D001), se indica que cada usuario es responsable de la información a la que accede a través de Internet (Políticas de control de acceso).
			3.3.5.5. Todos los accesos deben ser sujetos de monitoreo y conservación permanente por parte de la institución.			x	No se monitorea los acceso, ni se conserva la información al respecto.		x		No se monitorea los acceso, ni se conserva la información al respecto.
			3.3.5.6. El Oficial de Seguridad de la Información, puede acceder a los contenidos monitoreados, con el fin de asegurar el cumplimiento de las medidas de seguridad.		x		El Jefe de Seguridad de la Información solicita la información bajo demanda y la revisa para solución de requerimientos.		x		El Jefe de Seguridad de la Información solicita la información bajo demanda y la revisa para solución de requerimientos.
			3.3.5.7. La institución podrá en cualquier momento bloquear o limitar el acceso y uso de la Internet a los funcionarios o a terceros que accedan tanto por medio alámbrico como inalámbrico.	x			No hay documentación al respecto pero se hace uso de un PROXY.	x			Se realiza el bloqueo gracias a la utilización de PROXY.

Tabla 2.13 Tabla de recolección de información – Uso aceptable de los activos (Parte 6)[18]

[18] Elaborado por la autora

(ISO/IEC 27002:2005) 7. GESTIÓN DE ACTIVOS		EGSI		DOCUMENTACIÓN				IMPLEMENTACIÓN			
Objetivo de control	Control	EGSI	Aspectos a Evaluar	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento
7.1. Responsabilidad sobre los activos	7.1.3. Uso aceptable de los activos	*3.3.5. Reglamentar el acceso y uso de la Internet y sus aplicaciones/servicios*	3.3.5.8. Se debe bloquear y prohibir el acceso y uso de servicios de correo electrónico de libre uso tales como: Gmail, Hotmail, Yahoo, Facebook, entre otros.		x		Información contenida en el documento de Políticas para el uso y manejo de recursos informáticos, sección 9.2 Páginas de Libre Acceso. El correo institucional es un servicio de correo electrónico de libre uso, GMAIL adquirido en base a el EGSI (todas las disposiciones deben basarse en una gestión de riesgos).			x	Se limita el acceso y uso a servicios de correo gratuitos, a excepción de GMAIL. El correo institucional es un servicio de correo electrónico de libre uso, GMAIL adquirido en base a el EGSI (todas las disposiciones deben basarse en una gestión de riesgos).
			3.3.5.9. Se prohíbe expresamente a las entidades de la Administración Pública, la contratación, acceso y uso de servicios de correo electrónico en la Internet (Nube), para uso institucional o de servidores públicos, como empresas privadas o públicas cuyos centros de datos, redes (salvo la Internet), equipos, softw are base y de gestión de correo electrónico y cualquier elemento tecnológico necesario, se encuentren fuera del territorio nacional; y adicionalmente, si las condiciones de los servicios que tales empresas prestaren no se someten a la Constitución y Leyes Ecuatorianas.		x		Existe un acuerdo de uso de servicios en la nube, basado en el EGSI (todas las disposiciones deben basarse en una gestión de riesgos).		x		Existe un acuerdo de uso de servicios en la nube, basado en el EGSI (todas las disposiciones deben basarse en una gestión de riesgos).

Tabla 2.14 Tabla de recolección de información – Uso aceptable de los activos (Parte 7)[19]

[19] Elaborado por la autora

(ISO/IEC 27002:2005) 7. GESTIÓN DE ACTIVOS		EGSI		DOCUMENTACIÓN				IMPLEMENTACIÓN			
Objetivo de control	Control	EGSI	Aspectos a Evaluar	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento
7.1. Responsabilidad sobre los activos	7.1.3. Uso aceptable de los activos	3.3.6. Reglamentar el uso de los sistemas de video - conferencia	3.3.6.1. Definir un responsable para administrar la video-conferencia		x		La información está pendiente a ser incluída en el documento de Políticas para el uso y manejo de recursos informáticos, hasta Marzo del 2015.		x		No existen responsables para la administración de la video conferencia.
			3.3.6.2. Definir y documentar del procedimiento de acceso a los ambientes de pruebas y producción.			x	No existe ambiente de pruebas, sólo hay ambiente de producción. Información contenida en el Video Instructivo para administración del sistema de video conferencia, el cual está en proceso de revisión y no ha sido publicado formalmente.			x	No existe ambiente de pruebas, sólo hay ambiente de producción. El procedimiento de acceso al ambiente de pruebas está contenido en un Video Instructivo para la administración del sistema de video-conferencia, el cual se encontraba pendiente de publicación a la fecha de consulta.
			3.3.6.3. Elaborar un documento tipo "lista de chequeo" (check-list) que contenga los parámetros de seguridad para el acceso a la red interministerial que soporta el servicio de video-conferencia.	x			Incluido en el video que explica las actividades para la administración del sistema de videoconferencia, el cual está en proceso de revisión.		x		No se cuenta con un documento que contenga los parámetros de seguridad para el acceso a la red interministerial que soporta el servicio de video-conferencia.
			3.3.6.4. Crear contraseñas para el ingreso a la configuración de los equipos y para las salas virtuales de video-conferencia.		x		La información está pendiente a ser incluida en el documento de Políticas para el uso y manejo de recursos informáticos, hasta Marzo del 2015.		x		No se hace uso de contraseñas para el acceso a los sistemas de video-conferencia.
			3.3.6.5. Deshabilitar la respuesta automática de los equipos de video-conferencia.		x		La información está pendiente a ser incluida en el documento de Políticas para el uso y manejo de recursos informáticos, hasta Marzo del 2015.		x		La respuesta automática de los sistemas de video conferencia no está deshabilitada.

Tabla 2.15 Tabla de recolección de información – Uso aceptable de los activos (Parte 8)[20]

[20] Elaborado por la autora

(ISO/IEC 27002:2005) 7. GESTIÓN DE ACTIVOS		EGSI		DOCUMENTACIÓN				IMPLEMENTACIÓN			
Objetivo de control	Control	EGSI	Aspectos a Evaluar	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento
7.2. Clasificación de la información	7.2.1. Directrices de clasificación	*3.4.1. Clasificación de la información como pública o confidencial.*		x			Información en el Listado de Activos de Información, el cual contiene 251 activos con sus responsables, de éstos, 54 son considerados como activos críticos e incluye un perfil del responsable en donde termina el trato de la información (Contiene además, una clasificación de los activos de información, en función de su disponibilidad, confidencialidad e integridad de acuerdo a la LOTAIP).			x	Información parcial contenida en el Listado de Activos de Información, el cual contiene 251 activos con sus responsables, de éstos, 54 son considerados como activos críticos e incluye un perfil del responsable en donde termina el trato de la información (Contiene además, una clasificación de los activos de información, en función de su disponibilidad, confidencialidad e integridad de acuerdo a la LOTAIP).
		3.4.2. Elaborar y aprobar un catálogo de clasificación de la información. Se la deberá clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la institución. El nivel de protección se puede evaluar analizando la confidencialidad, la integridad y la disponibilidad.		x			Se dispone de un procedimiento de Clasificación de Información que se encuentra en revisión para aprobación, en consecuencia no puede ser entregado aún; además, se dispone del listado de activos de información de la EEQ clasificados en función de su disponibilidad, confidencialidad en integridad, el cual no puede ser entregado aún por motivos internos. Sin embargo para este caso en particular, se puede visitar la página Web www.eeq.com.ec, donde se encuentra la información acorde a la LOTAIP.			x	Se dispone de un procedimiento de Clasificación de Información que se encuentra en revisión para aprobación, en consecuencia no puede ser entregado aún; además, se dispone del listado de activos de información de la EEQ clasificados en función de su disponibilidad, confidencialidad en integridad, el cual no puede ser entregado aún por motivos internos. Sin embargo para este caso en particular, se puede visitar la página Web www.eeq.com.ec, donde se encuentra la información acorde a la LOTAIP.

Tabla 2.16 Tabla de recolección de información – Directrices de clasificación[21]

[21] Elaborado por la autora

(ISO/IEC 27002:2005) 7. GESTIÓN DE ACTIVOS		EGSI		DOCUMENTACIÓN				IMPLEMENTACIÓN			
Objetivo de control	Control	EGSI	Aspectos a Evaluar	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento	Cumple	No Cumple	Cumple Parcialmente	Observaciones de cumplimiento
7.2. Clasificación de la información	7.2.2. Etiquetado y manipulado de la información	*3.5.1. Incluir datos mediante abreviaturas, acerca del tipo de activo y su funcionalidad para la generación de etiquetas.*		x			Información contenida en el Listado de activos de información de la EEQ, en el que se etiqueta a cada activo, según el área y un secuencial.	x			Información contenida en el Listado de activos de información de la EEQ, en el que se etiqueta a cada activo, según el área y un secuencial.
		3.5.2. En caso de repetición de la etiqueta del activo, deberá añadirse un número secuencial único al final.			x		Información contenida en el Listado de activos de información de la EEQ, en el que se etiqueta a cada activo, según el área y un secuencial.		x		Información contenida en el Listado de activos de información de la EEQ, en el que se etiqueta a cada activo, según el área y un secuencial.
		3.5.3. En caso de documentos en formato electrónico, la etiqueta deberá asociarse a un metadato único, pudiendo ser éste un código MD5.			x		No se utiliza etiquetas asociadas a metadatos únicos para documentos en formatos electrónicos.		x		No se utiliza etiquetas asociadas a metadatos únicos para documentos en formatos electrónicos.
		3.5.4. Las etiquetas generadas deberán estar incluidas en el inventario, asociadas a su respectivo activo.				x	Información contenida en el Listado de activos de información de la EEQ, en el que se etiqueta a cada activo, según el área y un secuencial.			x	
		3.5.5. Los responsables de los activos deberán supervisar el cumplimiento del proceso de generación de etiquetas y rotulación de los activos.			x		Los responsables de los activos no supervisan el cumplimiento del proceso de generación de etiquetas y rotulación de los activos, lo realiza el área de Control de Bienes mediante la asignación de un código único de barras.		x		Los responsables de los activos no supervisan el cumplimiento del proceso de generación de etiquetas y rotulación de los activos, lo realiza el área de Control de Bienes mediante la asignación de un código único de barras.
		3.5.6. Para el caso de etiquetas físicas, los responsables de los activos verificarán con una periocidad no mayor a 6 meses, que los activos se encuentren rotulados y con etiquetas legibles.			x		Los responsables de los activos no verifican que los activos estén rotulados y con etiquetas legibles, esto lo realiza el área de Control de Bienes.		x		Los responsables de los activos no verifican que los activos estén rotulados y con etiquetas legibles, esto lo realiza el área de Control de Bienes.
		3.5.7. En caso de destrucción de un activo, la etiqueta asociada a éste debe mantenerse en el inventario respectivo con los registros de las acciones realizadas.			x		En los inventarios, no se mantienen las etiquetas de activos destruidos.		x		En los inventarios, no se mantienen las etiquetas de activos destruidos.

Tabla 2.17 Tabla de recolección de información – Etiquetado y manipulado de la información[22]

[22] Elaborado por la autora

De la información obtenida en las tablas de la 2.1 a la 2.17, se evaluaron 68 controles tomados del EGSI, en base a la norma ISO/IEC 27002, de los cuales se tuvieron los siguientes resultados:

ASPECTO DE EVALUACIÓN	NIVEL DE CUMPLIMIENTO	TOTAL
DOCUMENTACIÓN	Cumple	40
	No Cumple	16
	Cumple Parcialmente	12
IMPLEMENTACIÓN	Cumple	30
	No Cumple	25
	Cumple Parcialmente	13

Tabla 2.18 Tabla de recolección de información – Totales[23]

Documentación

La EEQ cumple con un 58.82% de los controles del EGSI a nivel de documentación, es decir, cuenta con documentación formal y publicada referente a cada control. No cumple con un 23,53% de los controles y un 17,65% de dichos controles se cumplen parcialmente.

Implementación

La EEQ cumple con un 44.11% de los controles del EGSI a nivel de la implementación, es decir, tiene implementados 30 controles en las diferentes áreas y se vigila que se cumplan con los mismos. No cumple con un 36.77% de los controles y un 19,11% de dichos controles se cumplen parcialmente.

2.2. ANÁLISIS DE RESULTADOS

La EEQ se encuentra actualmente en un proceso de mejora continua, la finalidad es brindar un servicio de calidad a la ciudadanía ecuatoriana. Dicho proceso de mejora está basado en la implementación de las directrices del EGSI a nivel institucional, cuyo objetivo principal es gestionar eficaz y eficientemente la seguridad de la información en las entidades de administración pública.

[23] Elaborado por la autora

Como se ha mencionado anteriormente, el EGSI está elaborado conforme las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27002 para la Gestión de Seguridad de la Información y contiene una serie de directrices a cumplir, las cuales han sido clasificadas en prioritarias y secundarias de acuerdo a su importancia en la implementación, según la SNAP.

Cabe aclarar que el EGSI no establece la implementación de un Sistema de Seguridad de la Información, sino que busca una correcta Gestión de la Seguridad de la Información mediante la aplicación de las directrices contenidas en éste.

Considerando lo anteriormente expuesto, la evaluación que se describe a continuación, está basada en la implementación de las directrices del EGSI en la EEQ, tomando en cuenta los objetivos de control y controles de la norma ISO 27002, más no en el Sistema de Gestión de Seguridad de la Información, ya que la EEQ aún no cuenta con un sistema para la gestión de la seguridad de la información, debido a que su prioridad es implementar las directrices de acuerdo al EGSI y posterior a esto, la implantación del sistema como tal.

En esta evaluación, se consideraron dos temas importantes, el primero corresponde a la existencia de Documentación formal sobre cada una de las directrices del EGSI, y el segundo, la Implementación de dichas directrices a nivel institucional.

A continuación el análisis de la información recolectada:

De acuerdo a la información provista por el Oficial de Seguridad, en la EEQ existen una serie de documentos en los cuales se registra información detallada de los bienes o activos de dicha institución así como de los responsables de dichos activos y de las actividades que deben llevar a cabo. En algunos casos, la información de un determinado bien o activo se encuentra en dos o más documentos y dichos documentos son gestionados por diferentes áreas operativas, lo cual genera demasiada información y en cierto grado, un desorden de la misma.

A continuación se presenta una breve descripción de cada uno de los documentos que mantienen información sobre los activos de la EEQ, los mismos que fueron provistos por el Oficial de Seguridad para el desarrollo de la evaluación, para lo cual se utilizó el siguiente formato:

"EMPRESA ELÉCTRICA QUITO E.E.Q. S.A – Nombre del documento": Descripción.

Descripción de los documentos:

"EMPRESA ELÉCTRICA QUITO E.E.Q. S.A -EQUIPOS ACTIVOS EN LA EMPRESA ELECTRICA" [13]: Es un documento en formato Excel, gestionado por el área de Control de Bienes, en especial por el fiscalizador de Control de Bienes quien es el encargado de: ingresar la información de las características de un bien (activo) cuando dicho bien sea dado de alta, modificar la información del responsable del bien en caso de traspasos, y/o actualizar los registros del documento mencionado en caso de bajas por mal estado u obsolescencia después de inspeccionar físicamente el bien o los bienes con el fin de determinar si es necesario o no dar de baja a dicho bien por mal estado u obsolescencia.

Este documento tiene la siguiente estructura:

Característica del bien	Descripción
Row Count	Código autogenerado cada vez que se ingresa un bien
CODI_MATE	Código único del activo
DESCRIPCIÓN	Descripción del bien que incluye especificaciones técnicas
FECHA_ADQUI	Fecha de adquisición
ROL_CUSTODIA	Número de rol del responsable del activo
NOMBRE_CUSTODIA	Nombre del responsable del activo

Tabla 2.19 Estructura del documento Equipos Activos de la Empresa eléctrica.[24]

Es utilizado como un inventario general dentro del cual se registra la información de todos los activos de la empresa a excepción de los teléfonos

[24] Elaborado por la autora en base al documento Equipos Activos en la Empresa Eléctrica, provisto por el Oficial de Seguridad de la EEQ.

celulares y teléfonos inteligentes cuya información está pendiente de añadir a la fecha de consulta del mismo, sin embargo no tiene una estructura adecuada y no está gestionado por el área de DTIC, sino por Control de Bienes.

Las especificaciones técnicas de cada activo forman parte de la descripción del mismo y no se las trata por separado. Este inconveniente no le permite al área de TI tener un mayor control sobre los bienes en general y sobre las características de los mismos, por ejemplo, es difícil para el área DTIC obtener un reporte sobre las máquinas obsoletas en uso con el fin de brindar una solución oportuna, sino que es necesario que cada responsable del bien solicite una renovación, siendo ésta una acción reactiva que ocasionaría inconvenientes al responsable del bien (quien utiliza el equipo) en la ejecución de sus tareas diarias. Otro de los inconvenientes con este documento, es que el área DTIC no puede a través de éste, obtener un reporte detallado como por ejemplo, uno que le permita evidenciar los cambios en los componentes del activo o evidenciar los responsables del mismo a lo largo del tiempo de vida de dicho activo, ya que los datos en el documento, cada vez que se realiza un cambio, son sobrescritos lo que provoca que se pierda la información histórica del activo.

"EMPRESA ELÉCRICA QUITO E.E.Q. S.A. - Inventario de Plataforma" [14]***:*** Contiene información de los servidores tanto físicos como virtuales alojados en cada RACK[25] del Data Center de la EEQ.

Este documento está elaborado en formato Excel, contiene información únicamente de los servidores y es gestionado por el área de DTIC y permite conocer las características de cada servidor, así como también su ubicación física y virtual.

El documento tiene la siguiente estructura:

La sección de las características funcionales del servidor incluye:

- CARACTERÍSTICAS FUNCIONALES DEL SERVIDOR:

[25] Un Rack es un soporte metálico que se utiliza para alojar equipos electrónicos, informáticos y de comunicaciones.

Característica del bien	Descripción
N. RACK	Etiqueta identificativa del RACK
N.ID	Número de identificación
CODIGO EEQ	Código del bien en la EEQ
VIRTUAL	Número del servidor virtual
NOMBRE DEL EQUIPO DE	Nombre del servidor
IP	Dirección IP del servidor
TIPO SVR	Tipo de servidor (FÍSICO O VIRTUAL)
S/O	Sistema Operativo instalado en el servidor
S/O Versión	Versión del Sistema Operativo
S/O Servicio	Sistema Operativo de servicio
FUNCION	Función que desempeña el servidor
MARCA	Marca del servidor
MODELO	Modelo del servidor
# Serie	Número de serie del servidor

Tabla 2.20 Características funcionales de los servidores. [26]

[26] Elaborado por la autora en base al documento Inventario de Plataforma, provisto por el Oficial de Seguridad de la EEQ.

La sección para el inventario de las aplicaciones instaladas en cada servidor contiene:

- APLICACIONES INSTALADAS EN CADA SERVIDOR:

Característica del bien	Descripción
N. RACK	Etiqueta identificativa del RACK
N.ID	Número de identificación
# Serie	Número de serie del servidor
APLICACIÓN	Aplicación instalada en el servidor
BASE DE DATOS	Base de datos instalada en el servidor
FECHA INSTALACIÓN	Fecha de instalación de la aplicación
PROCESADOR	Características del procesador
No. Proc Instalados	Número de procesadores instalados
No. Proc Soportados	Número de procesadores soportados
CORES	Número de núcleos
Arquitectura (32-64 bits)	Tipo de arquitectura de la aplicación (32 o 64 bits)
Arquitectura RISC / CISC[27]	Tipo de arquitectura de la aplicación (RISC / CISC)
RAM Instalada	Capacidad de RAM instalada
RAM Soportada	Capacidad de RAM soportada
N. Dimm Instalada	Número de tarjeta DIMM instalada
DIMM c/ n	No identificado.

Tabla 2.21 Características de las aplicaciones instaladas en cada servidor. [28]

[27] Arquitectura RISC (Reduced Instruction Set Computer) es un diseño de CPU que utiliza instrucciones de carga y almacenamiento sencillas que se ejecutan rápidamente. – Arquitectura CISC (Complex Instruction Set Computer) es un diseño de CPU contrario a RISC.
[28] Elaborado por la autora en base al documento Inventario de Plataforma, provisto por el Oficial de Seguridad de la EEQ.

La sección de las características físicas del servidor incluye:

- CARACTERÍSTICAS FÍSICAS DEL SERVIDOR:

Característica del bien	Descripción
N. RACK	Etiqueta identificativa del RACK
N.ID	Número de identificación
DIMM c/ n	No identificado
N. Dimm Di	Número de tarjetas DIMM disponibles
Tipo Disco	Tipo de disco duro
Capacidad	Capacidad del disco duro
Tipo de RAM	Tipo de RAM
# de Fuentes de Poder	Número de fuentes de poder
# Interfaces	Número de interfaces
MAC ADDRESS	Dirección MAC del equipo (física)
Descripción	Descripción
Tipo	Tipo
Modelo	Modelo
Serial	Número de serie
Año de Fabricación	Año de fabricación
OBSERVACIONES	Observaciones adicionales

Tabla 2.22 Características físicas de los servidores. [29]

El Inventario de plataforma es un documento gestionado por el personal de la DTIC, es decir, personal con los conocimientos suficientes para identificar cada una de las características descritas en las tablas. Estas características le permiten a dicho personal un adecuado manejo de los recursos disponibles, además de una adecuada visualización de las necesidades de mejora en los servidores con el fin de que puedan adaptarse a los nuevos requerimientos del negocio o a los cambios en el tiempo.

"SISTEMA DE GESTIÓN DE LA CALIDAD – Procedimiento para control de bienes (GR-GBB-P003)" [15]: Contiene las acciones a realizar en cuanto al control y gestión de los bienes o activos en la EEQ. En este documento se

[29] Elaborado por la autora en base al documento Inventario de Plataforma, provisto por el Oficial de Seguridad de la EEQ.

definen los procedimientos a realizar para el uso, alta, baja, traspaso, mantenimiento y/o control de los bienes en dicha institución. Dichos procedimientos son realizados por las unidades administrativas encargadas de los bienes y éstas deberán reportar los movimientos de los bienes a la Dirección Administración de Activos y Bienes para que se actualicen los datos en los respectivos inventarios.

"SISTEMA DE GESTIÓN DE LA CALIDAD - Políticas para el uso y manejo de los recursos informáticos de la EEQ (TI-D001)" [16]: Contiene políticas institucionales para el uso y manejo de los recursos informáticos de la EEQ. En este documento se describen políticas como por ejemplo, la Política de Seguridad de la información que indica el uso del SGSI para garantizar la confidencialidad, integridad y/o disponibilidad de la información. Contiene también la Política de Control de acceso, que indica que cada miembro de la EEQ tendrá acceso a la información acorde a la acción de personal remitida por el área de Talento Humano; políticas de Escritorios y pantallas limpias, entre otras.

"SISTEMA DE GESTIÓN DE LA CALIDAD - Procedimiento para administración de redes y comunicaciones (TI-GRC-P001)>>" [17]: Contiene una serie de Políticas y Procedimientos para la Administración de la Infraestructura de Redes y Comunicaciones de la EEQ. Este documento permite al personal de DTIC conocer los lineamientos necesarios relativos al diseño, instalación, operación, mantenimiento y soporte de la Infraestructura de Redes y Comunicaciones en la institución.

"SISTEMA DE GESTIÓN DE LA CALIDAD - Procedimiento para la gestión del portal web empresarial (TI-GDS-P003)" [18]: Contiene políticas y procedimientos para la gestión y el buen funcionamiento del portal web de la EEQ. Este documento fue elaborado con el objetivo de maximizar la calidad, eficacia y eficiencia de los contenidos y los servicios que ofrece el portal web de la EEQ.

"SISTEMA DE GESTIÓN DE LA CALIDAD - Procedimiento administración de servicios Internet y Correo (TI-GBD-P004)" [19]: Contiene políticas y procedimientos para llevar a cabo correctamente las actividades relacionadas

con la prestación de servicios de Internet y correo electrónico al personal de la EEQ. Este documento permite al personal de la DTIC la correcta gestión de usuarios de los servicios de Internet así como también del uso adecuado del correo electrónico.

"Empresa Eléctrica Quito "E.E.Q. S.A.", << SISTEMA DE GESTIÓN DE LA CALIDAD - Procedimiento para administración de seguridades y accesos (TI-GBD-P003)" [20]: Contiene políticas y procedimientos que permiten al personal de la DTIC una correcta gestión de los accesos a las aplicaciones y herramientas de la EEQ, control de claves, y además contiene un diagrama de flujo que indica los pasos a seguir para la solicitud de una cuenta de correo institucional.

"Empresa Eléctrica Quito "E.E.Q. S.A.", << SISTEMA DE GESTIÓN DE LA CALIDAD – Instructivo para Control Bienes (GR-GBB-P003-I001)" [21]: Este documento contiene las actividades necesarias en la EEQ para el Registro y Control del uso y destino final de cada uno de los bienes asignados a los responsables. Este documento es un complemento al Procedimiento para control de bienes [15].

Una vez revisados los documentos provistos por el Oficial de Seguridad, se procede con el análisis de la situación actual de la EEQ, tomando en cuenta el dominio seleccionado para la evaluación en la sección 1.3.2, y las directrices y/o controles del EGSI que servirán de apoyo para la evaluación.

Para la evaluación, se consideró la siguiente estructura:

- Dominio de evaluación seleccionado de la ISO 27002,
    - Objetivos de control del dominio seleccionado
    - Directrices de evaluación del EGSI.
    - Evaluación de CSCs por cada objetivo de control.

DOMINIO 7. GESTIÓN DE ACTIVOS (ISO/IEC 27002:2005)

Según la ISO [12] (International Organization for Standardization, en español, Organización Internacional para Estadarización), “la ISO/IEC 27002:2005 establece los lineamientos y principios generales para la iniciar, implementar, mantener y mejorar la gestión de seguridad de la información en una organización.”

Objetivo de Control 7.1. Responsabilidad sobre los activos

“Se deberían identificar los responsables para todos los activos y asignar la responsabilidad para el mantenimiento de los controles adecuados. La implementación de los controles específicos puede ser delegada por el responsable, según el caso, pero él sigue siendo responsable de la protección adecuada de los activo” [24].

Control 7.1.1. Inventario de activos

Un inventario de activos es un documento (físico o electrónico) utilizado para la recopilación de información referente a todos los bienes o servicios de una organización, también denominados activos.

Entre la información que debe contener el inventario de activos, según la NTE INEN-ISO/IEC 27002:2009, está el tipo de activo, formato, ubicación, información de soporte, información sobre licencias y el valor para el negocio.

La información contenida en este documento debe permitir a las organizaciones conocer de forma precisa, las características de cada activo y su estado actual con la finalidad de gestionar adecuadamente dichos activos para su beneficio.

Si bien es cierto, los activos tienen características en común, como por ejemplo, modelo, marca, etc., sin embargo existen otras características específicas de cada activo que se deben tomar en cuenta a la hora de elaborar un inventario de activos de una institución.

Directriz 3.1.1. Inventario de activos primarios en formatos físicos y/o electrónicos

DOCUMENTACIÓN

La EEQ tiene formalmente definido un documento denominado PLAN ESTRATÉGICO 2012–2015, el cual se encuentra publicado en la página web de la institución [1] y contiene la información referente a los procesos estratégicos, claves y de apoyo, a las normas y reglamentos, y a los planes estratégicos y operativos de la institución.

Este documento no está elaborado a manera de inventario, sino que presenta la descripción de cada activo de información con un fin informativo. A este documento se tiene libre acceso y opción de descarga gratuita desde Internet.

La información generada y procesada por los funcionarios y trabajadores de la EEQ se almacena y está disponible en el sistema QUIPUX[30][22].

[30] QUIPUX es un Sistema de Gestión Documental adaptado a las necesidades de las empresas que pertenecen a la Administración Pública Central.

La información referente a manuales e instructivos de sistemas informáticos, información de la operación de los aplicativos de los servicios informáticos, información del desarrollo y soporte de dichos aplicativos, es gestionada por la Dirección de Tecnología de la Información y Comunicaciones (DTIC), y es ésta área la encargada de hacer llegar dicha información a las personas que lo necesiten. La DTIC si tiene elaborado un inventario para los activos antes mencionados, pero este no fue provisto para su evaluación.

La imagen corporativa de la empresa, como el manual corporativo de la misma que incluye información referente a: manual de marca de la institución, logos, colores, fuentes, entre otras, es gestionada por la Dirección de Comunicación Social, y no consta en un Inventario como tal.

IMPLEMENTACIÓN

La EEQ no cuenta con un documento formal para el Inventario de los activos primarios en formatos físicos o electrónicos.

Directriz 3.1.2. Inventario de activos de soporte de Hardware

DOCUMENTACIÓN

La información de equipos móviles como tabletas, computadores portátiles, PDAs, etc; se encuentra contenida en el documento Equipos Activos de la Empresa Eléctrica [13], el cual contiene más de 5000 registros, sin considerar la información sobre teléfonos inteligentes y teléfonos celulares, la misma que a la fecha de la consulta, está pendiente de añadir a dicho documento .

El documento Equipos Activos de la Empresa Eléctrica, contiene información de equipos fijos como servidores de rack, computadores de escritorio, computadores portátiles, entre otros. Cabe mencionar que en el Inventario de Activos de Plataforma [14] descrito anteriormente, también consta la información de los servidores fijos de rack.

El Inventario de Equipos Activos de la Empresa Eléctrica contiene información sobre los periféricos de entrada (teclado, mouse, micrófono, etc.), periféricos de

salida (monitor, proyector, impresora, etc.), periféricos y dispositivos de almacenamiento (discos duros externos, librerías de cintas magnéticas, etc.), periféricos de comunicaciones (tarjetas USB para redes inalámbricas, tarjetas de red para redes alámbricas, etc.), tableros de trasferencia de energía eléctrica, de salidas de energía eléctrica, etc; e información de sistemas de control, sistemas de aire acondicionado, o de circuito cerrado de televisión. Adicionalmente, la información de los periféricos de almacenamiento como NAS o SAN[31], se encuentra también en el Inventario de Activos de Plataforma.

IMPLEMENTACIÓN

En la EEQ se tienen dos documentos formalmente definidos como Inventarios de activos de soporte de Hardware. Estos documentos son el documento de Equipos Activos de la Empresa Eléctrica [13], el cual contiene más de 5000 registros y es gestionado por el área de Control de Bienes, y el Inventario de Plataforma [14], el cual es gestionado por la DTIC. Estos inventarios no contienen la información completa de todos los activos de soporte de Hardware, por ejemplo, a la fecha de consulta, la inclusión de la información de teléfonos celulares y teléfonos celulares inteligentes se encuentra pendiente.

CRITICAL SECURITY CONTROLS

De acuerdo al documento Looking at the SANS 20 Critical Security Controls [23] publicado por System Experts, el Control Crítico de Seguridad CSC 1. Inventario de dispositivos autorizados y no autorizados, se tiene lo siguiente:

CSC1-1: Se debe implementar una herramienta automatizada para el descubrimiento de activos y con la información que ésta devuelva, elaborar un inventario de activos de los sistemas conectados a la red pública y privada de la institución.

CSC 1-2: Se debe implementar el registro de servidor de protocolo de configuración dinámica de host (DHCP), y utilizar un sistema que ayude a

[31] SAN (Storage Area Network), es una red de almacenamiento que se conecta a las redes de comunicación de una organización. – NAS (Network Server Access), es un servidor de acceso a una red que trabaja como un punto de acceso que controla el acceso a un recurso protegido.

detectar los sistemas desconocidos conectados a la red, a través de la información del DHCP.

CSC 1-3: El Inventario de activos debe ser actualizado conforme se vayan realizando adquisiciones de activos en la institución.

CSC 1-4: Se debe mantener un inventario de los activos de todos los sistemas conectados a la red y de los dispositivos propios de la red, para lo cual se debe considerar agregar al inventario las siguientes características:

Característica	Descripción
Dirección de red	Dirección IP del activo
Nombre de la máquina	Nombre del activo
Propósito del sistema	Propósito del sistema al que pertenece el activo
Responsable del activo	Nombre o identificador del responsable del activo
Departamento asociado	Departamento asociado al activo
Tipo de computador	Indicar si el dispositivo es portátil o personal

Tabla 2.23 Características a añadir en un inventario de activos de hardware según SANS 20. [32]

CSC 1-5: Se debe implementar el control de acceso a red (NAC) para monitorear los sistemas autorizados, con el fin de que en caso de un ataque, sea fácil detectar el sistema sospechoso y se lo traslade a una red con accesos limitados.

CSC 1-6: Se deben utilizar certificados de cliente para validar y autenticar los sistemas antes de que estos sean conectados a la red interna de la organización.

Directriz 3.1.3. Inventario de activos de soporte de Software

DOCUMENTACIÓN

El inventario de Equipos Activos de la Empresa Eléctrica [13] contiene información sobre los Sistemas Operativos en uso en la EEQ, en el Inventario de Activos de Plataforma se detallan las características de los sistemas

[32] Elaborado por la autora en base a los Controles Críticos de Seguridad de SANS.

operativos instalados en los servidores de la EEQ. Además, en la sección 9.1. Anexos, del documento Políticas para el uso y manejo de recursos informáticos de EEQ. [16], se mencionan entre otras cosas, los sistemas operativos que se utilizan en la EEQ pero no contienen una descripción de los mismos.

La información de software de servicio, mantenimiento o administración de gabinetes de servidores de cuchilla, servidores, sistemas de almacenamiento, etc; no forma parte del Inventario de Equipos Activos de la Empresa Eléctrica sino que consta en un documento denominado Procedimiento para administración de redes y comunicaciones (TI-GRC-P001) [17]. En la sección 9.1. Anexos – Listado de Software Autorizado, del documento Políticas para el uso y manejo de recursos informáticos [16] se muestra una lista de software de servicio autorizado para el uso en la EEQ, y en el Inventario de Plataforma se incluye también información al respecto en cada plataforma.

La información referente a los paquetes de software utilizados en la EEQ, como por ejemplo, software de ofimática, navegadores de internet, clientes de correo electrónico, mensajería instantánea, software de edición de imágenes, software de videoconferencia o software de servidores proxy, de correo electrónico de impresiones, etc., se encuentra contenida en el Inventario de Equipos Activos en la Empresa Eléctrica [13], así como también en el Inventario de Activos de Plataforma [14], el mismo que contiene información referente a los servidores mencionados. La información actualizada se encuentra contenida en el documento Políticas para el uso y manejo de recursos informáticos [16], sección 9.1. Anexos - Listado de Software Autorizado y por último en el Inventario de Plataforma.

La información referente a los Aplicativos del Negocio se encuentra contenida en el documento de Políticas para el uso y manejo de recursos informáticos [16], sección 9.1. Anexos - Listado de Software Autorizado (Aplicaciones desarrolladas).

IMPLEMENTACIÓN

Al igual que con los activos de soporte de hardware, los inventarios Equipos Activos de la Empresa Eléctrica [13] y el Inventario de Plataforma [14] también

contienen información de los activos de soporte de software en la institución, sin embargo existen algunos sistemas que no constan en dichos inventarios y cuya descripción se encuentra en otros documentos, como Listado de Software Autorizado.

CRITICAL SECURITY CONTROLS

De acuerdo al documento Looking at the SANS 20 Critical Security Controls [23] publicado por System Experts, el Control Crítico de Seguridad CSC 2. Inventario de software autorizado y no autorizado, se tiene lo siguiente:

CSC 2-1: Se debe implementar aplicaciones tecnológicas de lista blanca, que permiten que los sistemas ejecuten software que conste en las listas blancas e impida la ejecución de software que no conste.

CSC 2-2: Se debe establecer una lista de software autorizado y su versión, que se necesita en la empresa por cada sistema de la misma. Esta lista debe ser supervisada con el fin de evitar alteraciones en el software incluido.

CSC 2-3: Se deben ejecutar búsquedas de software no autorizado y generar alertas cuando se descubra alguno. De igual forma, se deben implementar controles para la aplicación de algún cambio o instalación de nuevo software, estrictos, así como también de las versiones de software modificadas o no reconocidas.

CSC 2-4: Implementar herramientas de inventario de software en toda la organización, esta herramienta deberá almacenar, entre otras cosas, las siguientes características de cada sistema software identificado:

Característica	Descripción
Versión	Versión del sistema operativo o de la aplicación
Tipo	Tipo de software instalado
Nivel de parche	Nivel de parche instalado en el software
Responsable del activo	Nombre o identificador del responsable del activo
Departamento asociado	Departamento asociado al activo

Tabla 2.24 Características a añadir en un inventario de activos de software según SANS 20. [33]

CSC 2-5: El inventario de software debe estar integrado con el inventario de hardware, de tal manera que los sistemas y su software asociado se almacenen en una sola ubicación.

Directriz 3.1.4. Inventario de activos de soporte de Redes

DOCUMENTACIÓN

Parte de la información referente a cables de comunicaciones, paneles de conexiones, tomas o puntos de red, racks, etc., está contenida en el documento de Inventarios de Activos de Plataforma [14], otra parte se encuentra de forma generalizada, en el Inventario de Equipos Activos en la Empresa Eléctrica [13] y no existe información detallada de cada uno de los cables y tampoco cuentan con codificación alguna.

La información de switches se encuentra en el Inventario de Equipos Activos en la Empresa Eléctrica [13], así como también de forma gráfica y no detallada, en el documento de Procedimiento para administración de redes y comunicaciones [17].

La información referente a ruteadores, cortafuegos, controladores de redes inalámbricas, etc., se encuentra contenida en el Inventario de Equipos Activos en la Empresa Eléctrica [13].

La información referente a Sistemas de detección y prevención de intrusos (IDS/IPS), firewalls de aplicaciones web, balanceadores de carga, switches de contenido, etc., se encuentra también contenida en el Inventario de Equipos Activos en la Empresa Eléctrica [13].

IMPLEMENTACIÓN

La información referente a los activos de soporte de redes, no está completamente contemplada en los inventarios Equipos Activos de la Empresa Eléctrica [13] e Inventario de Plataforma [14]. En el caso de los cables de

[33] Elaborado por la autora en base a los Controles Críticos de Seguridad de SANS.

comunicaciones, la información se encuentra de forma generalizada, más no se cuenta con una descripción de cada cable existente.

Control 7.1.2. Responsable de los activos

Según la Norma ISO 27002, cada activo de información debe tener un propietario asignado, y cuyo nombre o identificativo debe constar en el Inventario de activos de la organización. El propietario del activo es el responsable de la confidencialidad, integridad y disponibilidad de la información del activo a su cargo.

Directriz 3.2.1. Asignación de Responsables de los activos

DOCUMENTACIÓN

En el EGSI, en esta sección se describen las tareas que debe cumplir cada responsable con el fin de mantener una protección adecuada de los activos a su cargo.

Cada responsable de uno o varios activos, debe elaborar un inventario de todos los activos a su cargo y además debe mantenerlo actualizado conforme el paso del tiempo. En la EEQ, el Inventario de Equipos Activos en la Empresa Eléctrica [13] contiene el nombre del responsable de cada uno de los activos, además, el documento Procedimiento para control de bienes [15], en la sección 4. Mantenimiento y control de activos; contiene la descripción de los responsables (por áreas) de los diferentes tipos de activos. Dichos documentos son gestionados por diferentes áreas (Control de Bienes y la Dirección de Tecnología de la Información y Comunicaciones), más no por los responsables de cada activo.

La delegación de tareas a los responsables se definen en el documento Procedimiento para control de bienes [15], a modo de actividades a realizar para la correcta gestión de los activos, así como también en el documento Políticas para el uso y manejo de recursos informáticos [16].

En la sección 6. Políticas, del documento Políticas para el uso y manejo de recursos informáticos [16] se incluyen políticas referentes a la administración de la información dentro de los procesos de la institución a los cuales ha sido asignado cada responsable, dentro de las cuales consta la política 6.6.3***: "La información operacional relativa al hardware, software, comunicaciones y servicios de TI, es de propiedad de la DTIC"***, que indica que la información solo es gestionada por la Dirección de Tecnología de la Información y Comunicaciones (DTIC). Además cabe mencionar que el documento está elaborado únicamente para salvaguardar la seguridad de la información, sistemas de información y los recursos tecnológicos Institucionales, más no de todos los activos de la EEQ.

El EGSI indica que cada responsable de los activos debe ***"Elaborar las reglas para el uso aceptable de los activos, e implantarlas previa autorización de la autoridad correspondiente"***, sin embargo en la EEQ, las reglas para el uso aceptable de los activos son desarrolladas a nivel empresarial por el área de Control de Bienes o la DTIC, más no por cada responsable, y por ende todo el personal de la EEQ debe cumplir con las mismas. Estas reglas están documentadas en documentos como el Instructivo para Control Bienes [21], y/o en el documento Políticas para el uso y manejo de recursos informáticos [16], en la sección Políticas Detalladas.

El área de Control de Bienes y la DTIC también son responsables de la clasificación, documentación y de mantener completamente actualizada la información de todos los activos existentes en la EEQ, así como también de definir los permisos de acceso a la información.

IMPLEMENTACIÓN

Los responsables de cada activo no tienen desarrollado un inventario de los activos a su cargo, el cual esté formalmente implementado. Las tareas rutinarias de cada responsable, así como las tareas de administración de la información de los procesos a los cuales ha sido asignado dicho responsable, están definidas en el documento Políticas para el uso y manejo de recursos informáticos, sin embargo estas tareas están definidas de forma global para todos los miembros de la EEQ. Son las áreas de Control de Bienes y la DTIC

las encargadas de mantener actualizada la información y los activos y los permisos de acceso a la información se definen en base a las tareas operativas que cumple cada responsable, en la EEQ.

Directriz 3.2.2. Consolidación de inventarios de activos con sus responsables

DOCUMENTACIÓN

El documento Inventario de Equipos Activos en la Empresa Eléctrica [13] contiene información de los activos de la EEQ así como de sus responsables. En dicho documento, se debe ingresar por cada activo, entre otras cosas, el código del bien, una descripción del mismo, la fecha de adquisición, el número de rol de la persona responsable de dicho activo y su nombre. Los procedimientos para el registro de ésta información se encuentran contenidos en el documento Instructivo para Control Bienes [21] y en el Procedimiento para control de bienes [15].

IMPLEMENTACIÓN

No se cuenta con documentación de consolidación de inventarios de Responsables y activos a su cargo por área o unidad organizacional. Únicamente se ingresa en el Inventario de Equipos Activos de la Empresa Eléctrica, el nombre y número de rol del responsable de cada activo.

CRITICAL SECURITY CONTROLS

De acuerdo al documento Looking at the SANS 20 Critical Security Controls [23] publicado por System Experts, el Control Crítico de Seguridad CSC 1. Inventario de dispositivos autorizados y no autorizados, se tiene lo siguiente:

CSC 1-4: Se debe mantener un inventario de los activos de todos los sistemas conectados a la red y de los dispositivos propios de la red, para lo cual se debe considerar agregar al inventario el nombre o un identificativo del responsable de cada activo, así como también el departamento asociado a dicho activo (Tabla 10).

De igual forma, en el inventario de software (CSC 2), también se debe incluir el nombre el nombre o un identificativo del responsable de cada activo, así como también el departamento asociado a dicho activo.

Control 7.1.3. Uso aceptable de los activos

Los activos de una organización solo pueden ser utilizados para llevar a cabo actividades propias del negocio en beneficio de la institución, más no actividades personales del responsable del mismo.

Directriz 3.3.1. Identificar documentar e implementar las reglas sobre el uso aceptable de los activos asociados con los servicios de procesamiento de la información.

DOCUMENTACIÓN

El EGSI indica que: ***"Para la elaboración de las reglas, el Responsable del Activos deberá tomar en cuenta las actividades definidas en los controles correspondientes a los ámbitos de "Intercambio de Información" y "Control de Acceso", donde sea aplicable."***, sin embargo en la EEQ, como se mencionó anteriormente, las reglas de uso aceptable de los activos no son desarrolladas por el responsable de dichos activos, sino por las áreas de Control de Bienes y la DTIC. Estas reglas están definidas en base a los procedimientos de altas, traspasos y/o bajas de los activos o bienes, pero no se considera la información como un bien prioritario de la EEQ. En cuanto al control de accesos, los mismos se definen en base a las necesidades de cada persona.

IMPLEMENTACIÓN

El responsable del activo no es el encargado de la definición de reglas sobre el uso aceptable de los activos. Los responsables de definirlas son las áreas de DTIC y Control de Bienes.

Directriz 3.3.2. El oficial de Seguridad de la Información es el encargado de asegurar los lineamientos para la utilización de los recursos de las Tecnologías de la Información.

DOCUMENTACIÓN

Los lineamientos para la utilización de los recursos de las Tecnologías de Información, antes de la contratación del personal para Oficial de Seguridad, eran gestionados por la DTIC, y se los definían en base a las necesidades de cada área de trabajo.

IMPLEMENTACIÓN

Los lineamientos para la utilización de los recursos de las Tecnologías de Información, antes de la contratación del personal para Oficial de Seguridad, eran gestionados por la DTIC, y se los definían en base a las necesidades de cada área de trabajo.

Directriz 3.3.3. La información y documentos generados en la institución y enviados por cualquier medio o herramienta electrónica con propiedad de la información que procesan.

IMPLEMENTACIÓN Y DOCUMENTACIÓN

La información generada y procesada por los funcionarios y trabajadores de la EEQ se almacena y está disponible en el sistema QUIPUX [22].

Directriz 3.3.4. Reglamentar el uso de correo electrónico institucional

DOCUMENTACIÓN

El EGSI indica que el correo electrónico institucional debe ser utilizado únicamente para realizar tareas que le permitan al usuario, cumplir con sus funciones laborales que demande la compañía. En la EEQ, en la sección 6.4

Correo Electrónico del documento Políticas para uso y manejo de recursos informáticos [16], se establecen políticas para el uso del correo institucional.

Dentro de la EEQ, existe un documento denominado Procedimiento administración de servicios Internet y Correo [19], el cual contiene procedimientos y políticas para la creación de cuentas de correo electrónico al personal de la organización, que así lo requiera. De igual forma contiene políticas de creación de contraseñas, en cuanto a estructura; procedimientos para solicitudes de acceso a Internet o correo electrónico; procedimientos para acceso a Internet en el firewall de la EEQ. Cada vez que se crea una cuenta de correo electrónico, siendo responsable de dicha actividad la DTIC, se le notifica al usuario que debe hacer uso de su cuenta en base a las políticas para uso y manejo de recursos informáticos [16].

El documento Procedimiento administración de servicios Internet y Correo [19], incluye como anexo, un acta de compromiso para el buen uso del servicio de Internet de la EEQ, la misma que debe ser firmada por cada usuario del correo institucional y/o Internet de la institución la primera vez que solicita acceso a cualquiera de los servicios antes descritos.

El acta de compromiso para el buen uso del servicio de Internet de la EEQ contiene las condiciones que debe cumplir el personal para utilizar los servicios de Internet de la EEQ, aceptando que el uso de dicho servicio deberá ser únicamente para fines de cumplimiento laboral e indicar si necesita tener acceso a sitios específicos con fines de consulta y/o investigación para beneficio de la institución.

Los correos y/o mensajes transmitidos por medio del correo electrónico institucional o por medio de Internet, no son monitoreados ni conservados permanentemente por parte de la EEQ.

Cada cuenta de correo electrónico perteneciente al correo electrónico institucional está asociada a una única cuenta de usuario según el número de rol asignado por el área de Recursos Humanos, y en caso de usuarios a contrato sin rol, en base a su nombre y apellido.

La información de los buzones de correo es gestionada por cada usuario en su estación de trabajo, más no de forma centralizada como indica el EGSI. Cada usuario es responsable de la eliminación de mensajes máximo cada 15 días con el fin de optimizar el tamaño de su bandeja de correos, así como también de respaldar la información que así lo requiera, en una unidad asignada para dicho fin.

No se cuenta con facilidades automáticas que notifiquen al usuario cuando un correo enviado por él, no es recibido correctamente por el destinatario, y que indiquen detalladamente el motivo del error.

Para el monitoreo de virus informáticos, tanto en correos o en archivos adjuntos, se utiliza un Software de Antivirus de Plataforma Integral, y se prohíbe al personal, la reproducción maliciosa o voluntaria de virus informáticos, o de mensajes con contenido ofensivo, ilegal, pornográfico o de cualquier otro tipo no autorizado que dañe la imagen de la institución.

Cada usuario es responsable de la información que reciba, por lo tanto, en caso de identificar un mensaje de origen desconocido, debe destruirlo y asumir la responsabilidad de las consecuencias que pueda ocasionar la apertura o ejecución de dicho mensaje. Además, debe notificar al Oficial de Seguridad de la Información de la presencia de dicha amenaza, con el fin de que sea analizado y se tomen las medidas preventivas o correctivas necesarias. Este procedimiento está descrito en el acta de compromiso para el buen uso del servicio de Internet de la EEQ.

Para la transmisión de información en la EEQ se utiliza HTTPS, que permite transmitir información cifrada por medio del canal. No se mantiene información conservada referente al uso de correo electrónico y/o servicio de internet.

Las cuentas de correo electrónico institucional, son creadas de tal forma que se limite el tamaño de los mensajes, así como también el envío masivo de los mismos. Cabe señalar que cada usuario es responsable de la cantidad y tamaño de los mensajes que se envíen desde su cuenta de correo.

IMPLEMENTACIÓN

En el documento Procedimiento Administración de Servicios Internet y Correo (TI-GBD-P004), se definen políticas y procedimientos para el uso aceptable de servicios de Internet y Correo Electrónico, en donde se indica que dichos servicios deben ser utilizados únicamente para tareas propias de la organización.

No se monitorea la información en el sistema de correo electrónico, ni tampoco es almacenada sino en cada equipo en el caso del correo electrónico, en su bandeja de correo.

Directriz 3.3.5. Reglamentar el acceso y uso de la Internet y sus aplicaciones/servicios

DOCUMENTACIÓN

Los procedimientos para el acceso y uso de Internet, así como de sus aplicaciones y servicios están incluidos en el documento Procedimiento para administración de seguridades y accesos [20], dentro del cual se incluyen políticas y procedimientos para el acceso a las aplicaciones y herramientas de la EEQ que requieren autenticación, procedimientos para control de claves para aplicaciones y herramientas de la EEQ que requieran autenticación (a excepción del sistema Sidecom); procedimientos para los usuarios del sistema Sidecom; entre otras.

En la sección 6.3 Seguridad Informática, del documento Políticas para uso y manejo de recursos informáticos [16], se establecen políticas para el acceso a los sistemas informáticos en la institución. Cada usuario es responsable de respetar la integridad de los sistemas de computación a los cuales tenga acceso, así como también de las contraseñas que se utilizan para dichos accesos. La Administración de la EEQ tiene el derecho de vigilar y auditar los sistemas de correo electrónico y todos los sistemas computarizados con el fin de garantizar que los usuarios utilicen dichos servicios con fines netamente laborales, en función de las actividades que realice en la EEQ. Estas auditorías

se realizan de forma periódica o al azar, según las necesidades de la institución. Además, cada usuario deberá guardar la información que requiera ser almacenada, en los directorios asignados a cada usuario, con el fin de protegerlos mediante mecanismos de respaldos.

Cada una de las personas que laboran en la EEQ y que requieran acceso a algún servicio de Internet, deberán llenar el acta de compromiso para el buen uso del servicio de Internet de la EEQ, indicando las razones por las cuales requiere los servicios informáticos. Además, en la red de la EEQ, se limita el acceso a portales, servicios o sitios web que puedan dañar la imagen de la institución, para lo cual se bloquea el acceso a sitios con contenidos de índole maliciosa. En la sección 9. Anexos, del documento Políticas para uso y manejo de recursos informáticos [16], se presenta el estado de software autorizado al cual tiene acceso cada miembro de la EEQ.

En la EEQ, para cada tipo de información se designa un custodio, cuya objetivo será proteger la información de la institución, , tomando en cuenta la criticidad de la información. Los custodios de la información son responsables de definir procedimientos de control específicos, administrar el control de acceso a la información, y suministrar capacidades de recuperación, en concordancia con las instrucciones de los dueños/propietarios de los datos. El Oficial de Seguridad de la Información forma parte de los custodios de la información, el mismo que puede solicitar la información de monitoreo de los contenidos a los que acceden los usuarios, bajo demanda para posteriormente revisarla y/o analizarla para la solución de requerimientos.

Se prohíbe el uso de la computadora o del sistema de correspondencia electrónica para enviar, recibir, crear o divulgar mensajes o documentos de contenido discriminatorio por razones de raza, género, credo, origen nacional, sexo, orientación sexual, edad, ideas políticas u origen social o nacional, o que puedan ser catalogados como hostigamiento sexual.

En la EEQ se utiliza un PROXY, el cual permite un mayor control de los sitios a los que se tiene acceso desde Internet, y cuando sea conveniente, se limitará o

bloqueará el acceso a sitios que se consideren una amenaza para la institución.

El correo institucional es un servicio de correo electrónico de libre uso, GMAIL adquirido en base a lo establecido en el EGSI (el cual indica que todas las disposiciones deben basarse en una gestión de riesgos).

La EEQ hace uso de servicios en la nube, para lo cual existe un acuerdo de uso de servicios en la nube, basado en el EGSI (todas las disposiciones deben basarse en una gestión de riesgos).

IMPLEMENTACIÓN

El documento Procedimiento Administración de Servicios Internet y Correo (TI-GBD-P004), contiene como anexo un acta de compromiso para el buen uso del servicio de Internet de la EEQ, en donde se le indica a cada usuario que es responsable del tráfico de información que genere.

Directriz 3.3.6. Reglamentar el uso de los sistemas de video – conferencia

DOCUMENTACIÓN

Durante la recaudación de la información, no se contaba con la definición de responsables para la administración de los sistemas de video conferencia, sin embargo el Oficial de Seguridad indicó que la información estaba pendiente de ser incluida en el documento Políticas para uso y manejo de recursos informáticos [16].

La EEQ cuenta únicamente con un ambiente de producción de los sistemas de video conferencia, no existe un ambiente de pruebas. La institución cuenta con un video instructivo para la administración del sistema de video conferencia, el cual a la fecha de la consulta, se encontraba en estado de revisión y no ha sido publicado formalmente. En dicho video instructivo, se definen los procedimientos para el acceso y uso del sistema de video conferencia en el ambiente de producción, antes mencionado.

El video instructivo contiene una descripción de las actividades que se deben ejecutar para la administración del sistema de video conferencia, más no se cuenta con un la lista de chequeo que sugiere el EGSI que debe contener los parámetros de seguridad que se deben cumplir para el correcto acceso a la red que soporta el servicio de video conferencia.

Al momento de la recaudación de la información, la inclusión de las políticas para creación de usuarios y contraseñas para el ingreso a la configuración de los equipos y salas virtuales de video conferencia, en el documento Políticas para uso y manejo de recursos informáticos [16] se encontraba. También se encontraba pendiente, la inclusión de políticas para deshabilitar las respuestas automáticas de los equipos de video conferencia de la institución.

IMPLEMENTACIÓN

No se han definido responsables para la administración de los sistemas de video conferencia, no existe un ambiente de pruebas, se cuenta con un ambiente de producción para cuyo acceso, se han definido procedimientos en el Video Instructivo, el cual estaba pendiente de publicación a la fecha de consulta.

No se cuenta con un documento en donde se definan los parámetros de seguridad para el acceso a la red interministerial que soporta el servicio de video-conferencia, y no se hace uso de contraseñas para el acceso a estos sistemas. La respuesta automática de los sistemas de videoconferencia, no está desactivada.

CRITICAL SECURITY CONTROLS

De acuerdo al documento Looking at the SANS 20 Critical Security Controls [23] publicado por System Experts, el Control Crítico de Seguridad CSC 13. Límites de Defensa se tiene lo siguiente:

Para asegurar el uso aceptable de los activos de la institución, es necesaria la aplicación de controles para denegar el acceso a direcciones IP identificadas como maliciosas, o limitar el acceso sólo a sitios de confianza.

Se debe monitorear el tráfico de la red, así como la información que viaja por ella, con la finalidad de determinar si se hace uso de la red para fines que no sean de la institución.

Objetivo de Control 7.2. Clasificación de la Información

Control 7.2.1. Directrices de Clasificación

Como se ha indicado anteriormente, la información es uno de los activos más importantes de las compañías hoy en día, por esta razón, es indispensable que en cada institución se implementen políticas y/o procedimientos para su control y manejo, como por ejemplo, procedimientos para la identificación y clasificación de los activos de información en la compañía, según su criticidad.

La información puede ser clasificada en dos grupos: Información Pública, es decir información a la que se puede tener libre acceso; e Información confidencial, a la cual el acceso se debe restringir. En ambos casos, el acceso a la información debe ser controlado y se debe establecer políticas para su entrega o difusión.

Directriz 3.4.1. Clasificación de la información como pública o confidencial.

DOCUMENTACIÓN

La EEQ cuenta con un documento denominado Listado de Activos de Información, el cual contiene la descripción de 251 activos con sus responsables. De estos 251 activos identificados en dicho documento, 54 son considerados como activos críticos y se incluye un perfil del responsable en donde termina el trato de la información. Contiene además, una clasificación de los activos de información, en función de su disponibilidad, confidencialidad e integridad de acuerdo a la LOTAIP[34] que rige a las empresas de Administración

[34] LOTAIP (Ley Orgánica de Transparencia y Acceso a la Información Pública), es una ley en estado vigente, publicada en el Registro Oficial Suplemento 337 de 18 de mayo de 2004, que garantiza el derecho a acceder a las fuentes de información públicas.

Pública como la EEQ. El documento no fue provisto por el Oficial de Seguridad por motivos internos, sin embargo el Oficial de Seguridad brindó información sobre dicho documento.

IMPLEMENTACIÓN

Información contenida en el Listado de Activos de Información, el cual contiene 251 activos con sus responsables, de éstos, 54 son considerados como activos críticos e incluye un perfil del responsable en donde termina el trato de la información (Contiene además, una clasificación de los activos de información, en función de su disponibilidad, confidencialidad e integridad de acuerdo a la LOTAIP).

Directriz 3.4.2. Elaborar y aprobar un catálogo de clasificación de la información. Se la deberá clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la institución. El nivel de protección se puede evaluar analizando la confidencialidad, la integridad y la disponibilidad.

DOCUMENTACIÓN E IMPLEMENTACIÓN

La EEQ dispone de un procedimiento de Clasificación de Información que se encuentra en revisión para aprobación, en consecuencia no puede ser entregado aún; además, se dispone del listado de activos de información de la EEQ clasificados en función de su disponibilidad, confidencialidad en integridad, el cual no puede ser entregado aún por motivos internos. Sin embargo para este caso en particular, se puede visitar la página Web www.eeq.com.ec, donde se encuentra la información acorde a la LOTAIP.

CRITICAL SECURITY CONTROLS

De acuerdo al documento Looking at the SANS 20 Critical Security Controls [23] publicado por System Experts, el Control Crítico de Seguridad CSC 15. Acceso controlado en base a la necesidad de conocer, se tiene lo siguiente:

CSC 15-1: Localizar la información sensible y encriptar todo tipo de comunicación en la que se la utilice.

CSC 15-2: Se debe controlar el cumplimiento del registro de auditoría para el acceso a datos no públicos y se debe implementar una autenticación especial para datos sensibles.

CSC 15-3: Se debe segmentar la red basándose en los niveles de confianza de la información almacenada en los servidores. Si el nivel de confianza de una red es bajo, la información debe ser encriptada.

CSC 15-4: Controlar el acceso a los datos mediante las ACLs (Listas de control de acceso) implementadas en cada servidor.

Control 7.2.1. Etiquetado y manipulado de la información

Toda la información que se manipule dentro de una organización, debe ser correctamente etiquetada.

En la EEQ, se dispone de un Procedimiento de Clasificación de Información que se encuentra en revisión para aprobación, en consecuencia no puede ser entregado aún. Además, se dispone del listado de activos de información de la EEQ clasificados en función de su disponibilidad, confidencialidad e integridad, el cual no puede ser entregado aún por motivos internos. Sin embargo para este caso en particular, se puede visitar la página web de la EEQ [1], donde se encuentra información publicada acorde a lo establecido en la LOTAIP.

Directriz 3.5.1. Incluir datos mediante abreviaturas, acerca del tipo de activo y su funcionalidad para la generación de etiquetas.

DOCUMENTACIÓN

En el documento Listado de Activos de Información, cada uno de los activos contenidos se encuentra etiquetado formalmente en base al área en la que es administrado y a un secuencial asignado por el área DTIC.

IMPLEMENTACIÓN

Información contenida en el Listado de activos de información de la EEQ, en el que se etiqueta a cada activo, según el área y un secuencial.

Directriz 3.5.2. En caso de repetición de la etiqueta del activo, deberá añadirse un número secuencial único al final.

DOCUMENTACIÓN E IMPLEMENTACIÓN

Las etiquetas de los activos contenidos en el documento Listado de Activos de Información incluyen un secuencial para su diferenciación.

Directriz 3.5.3. En caso de documentos en formato electrónico, la etiqueta deberá asociarse a un metadato único, pudiendo ser éste un código MD5.

DOCUMENTACIÓN E IMPLEMENTACIÓN

Los activos de información en formato electrónico no están asociados a un metadato único.

Directriz 3.5.4. Las etiquetas generadas deberán estar incluidas en el inventario, asociadas a su respectivo activo.

DOCUMENTACIÓN E IMPLEMENTACIÓN

Las etiquetas de los activos de información están incluidas en el documento de Listado de Activos de Información.

Directriz 3.5.5. Los responsables de los activos deberán supervisar el cumplimiento del proceso de generación de etiquetas y rotulación de los activos.

DOCUMENTACIÓN E IMPLEMENTACIÓN

Los responsables de los activos de la información no son los responsables de la supervisión de cumplimiento del proceso de generación de etiquetas y rotulación de activos, el área responsable es el área DTIC.

Directriz 3.5.6. Para el caso de etiquetas físicas, los responsables de los activos verificarán con una periocidad no mayor a 6 meses, que los activos se encuentren rotulados y con etiquetas legibles.

DOCUMENTACIÓN E IMPLEMENTACIÓN

Los responsables de los activos no se encargan de la verificación de que los activos se encuentren rotulados y con etiquetas legibles, estos procesos se están empezando a implementar en la EEQ. La rotulación de los activos lo realiza el área de Control de Bienes mediante la asignación de un código único de barras.

Directriz 3.5.7. En caso de destrucción de un activo, la etiqueta asociada a éste debe mantenerse en el inventario respectivo con los registros de las acciones realizadas.

DOCUMENTACIÓN E IMPLEMETACIÓN

Los responsables de los activos no verifican que los activos estén rotulados y con etiquetas legibles, esto lo realiza el área de Control de Bienes.

CRITICAL SECURITY CONTROLS

De acuerdo al documento Looking at the SANS 20 Critical Security Controls [23] publicado por System Experts, el Control Crítico de Seguridad CSC 15. Acceso controlado en base a la necesidad de conocer, se tiene lo siguiente:

CSC 15-1: Localizar la información sensible y encriptar todo tipo de comunicación en la que se la utilice.

CSC 15-2: Se debe controlar el cumplimiento del registro de auditoría para el acceso a datos no públicos y se debe implementar una autenticación especial para datos sensibles.

CSC 15-3: Se debe segmentar la red basándose en los niveles de confianza de la información almacenada en los servidores. Si el nivel de confianza de una red es bajo, la información debe ser encriptada.

CSC 15-4: Controlar el acceso a los datos mediante las ACLs (Listas de control de acceso) implementadas en cada servidor.

Por otro lado, con respecto al CSC 17. Protección de datos, se tiene lo siguiente.

CSC 17-1: Implementar software para el cifrado de la información sensible en los discos duros de dispositivos específicos.

CSC 17-2: Verificar que los dispositivos criptográficos y de software estén configurados para utilizar algoritmos examinados públicamente.

CSC 17-3: Realizar una evaluación de los datos para identificar la información confidencial que exige la aplicación de controles de encriptación e integridad.

CSC 17-4: Implementar herramientas automatizadas para identificar intentos de acceso no autorizado a los sistemas que contienen información sensible.

CSC 17-5: Llevar a cabo análisis periódicos de la información sensible almacenada de forma cifrada, con el fin de identificar cambios no autorizados en la misma.

2.2.1. RESULTADOS FINALES

Considerando lo expuesto en el numeral 9. Análisis de datos y reporte de los resultados de la medición, sección 9.2 Analizar los datos y desarrollar los resultados de la medición, de la NTE INEN ISO/IEC 27004:2012 [25], que indica: “El análisis de los datos deben identificar las brechas entre los resultados esperados y los de la medición real de un SGSI implementado, controles o grupo de controles.”, por lo tanto, en este proyecto de titulación se evaluaron los niveles de cumplimiento de los controles correspondientes al dominio 7. Gestión de Activos de la NTE INEN ISO/IEC 27002:2009, más no el SGSI implementado en su totalidad.

Comparación entre la NTE-ISO/IEC 27002:2009 y el EGSI

En las tablas de la 2.25 a la 2.29 se muestra una comparación del Dominio 7. Gestión de Activos de la NTE-ISO/IEC 27002:2009 y el Dominio 3. Gestión de los Activos del EGSI.

Esta comparación se llevó a cabo con el fin de identificar si el EGSI contempla todos los aspectos de la NTE-ISO/IEC 27002:2009, en base a la cual fue desarrollado, para lo cual se creó una tabla para la comparación por cada objetivo de control:

- **Objetivo de control 7.1.1 Inventario de activos**

NTE INEN-ISO/IEC 27002:2009	EGSI
Tipos de activos a inventariar	**Controles para el inventario de cada tipo de activo según la NTE-ISO/IEC 27002:2009**
Información: bases de datos y archivos de datos, contratos y acuerdos, documentación del sistema, información sobre investigación, manuales de usuario, material de formación, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos de recuperación, registros de auditoría e información archivada.	3.1.3. Inventario de activos de soporte de Software.
Archivos de software: software de aplicación, software del sistema, herramientas de desarrollo y utilidades.	3.1.3. Inventario de activos de soporte de Software.
Activos físicos: equipos de computación, equipos de comunicaciones, medios removibles y otros equipos.	3.1.2. Inventario de activos de soporte de Hardware.
Servicios: servicios de computación y comunicaciones, servicios generales como por ejemplo iluminación, calefacción, energía y aire acondicionado.	3.1.3. Inventario de activos de soporte de Software.
Personas y sus calificaciones, habilidades y experiencias.	No se contempla a las personas como activos.
Intangibles tales como reputación e imagen de la organización.	3.1.1. Inventario de activos primarios en formatos físicos y/o electrónicos.

Tabla 2.25 Comparación entre NTE-ISO/IEC 27002:2009 y EGSI, para el dominio 7. Gestión de Activos (Objetivo de control 7.1.1 Inventario de activos). [35]

En base a la comparación realizada en la tabla 2.25 a nivel del objetivo de control 7.1.1 Inventario de activos, el EGSI no contempla a las personas como parte de los activos de la organización.

[35] Elaborado por la autora.

Objetivo de control 7.1.2 Responsable de los activos

NTE INEN-ISO/IEC 27002:2009	EGSI
Tareas del responsable de los activos	**Controles que abarcan las tareas del responsable de los activos según la NTE-ISO/IEC 27002:2009**
Garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente.	3.2.1. Asignación de Responsables de los Activos. 3.2.2. Consolidación de inventarios de activos con sus responsables.
Definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control de acceso	3.2.1. Asignación de Responsables de los Activos.

Tabla 2.26 Comparación entre NTE-ISO/IEC 27002:2009 y EGSI, para el dominio 7. Gestión de Activos (Objetivo de control 7.1.2 Responsable de los activos). [36]

En base a la comparación realizada en la tabla 2.26 a nivel del objetivo de control 7.1.2 Responsable de los activos, el EGSI contempla todos los aspectos de la NTE INEN ISO/IEC 27002:2009.

[36] Elaborado por la autora.

- **Objetivo de control 7.1.3 Uso aceptable de los activos**

NTE INEN-ISO/IEC 27002:2009	EGSI
Reglas para el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información	**Controles que abarcan las reglas para el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de información.**
Reglas para el uso del correo electrónico y de Internet.	3.3.1. Reglamentar el uso del correo electrónico institucional 3.3.2. Reglamentar el acceso y uso de la Internet y sus aplicaciones/servicios.
Directrices para el uso de los dispositivos móviles, especialmente para su utilización fuera de las instalaciones de la organización.	No se contemplan las directrices para el uso de los dispositivos móviles.

Tabla 2.27 Comparación entre NTE-ISO/IEC 27002:2009 y EGSI, para el dominio 7. Gestión de Activos (Objetivo de control 7.1.3 Uso aceptable de los activos). [37]

En base a la comparación realizada en la tabla 2.27 a nivel del objetivo de control 7.1.3 Uso aceptable de los activos, el EGSI no contempla directrices para el uso de dispositivos móviles.

[37] Elaborado por la autora.

- **Objetivo de control 7.2.1 Directrices de clasificación**

NTE INEN-ISO/IEC 27002:2009	EGSI
Características de las directrices de clasificación de la información	**Controles que abarcan las características de las directrices de clasificación de la información**
Deberían incluir convenciones para la clasificación inicial y la reclasificación con el paso del tiempo, de acuerdo con alguna política predeterminada de control del acceso.	3.4.1. Clasificar la información como pública o confidencial.
Debería ser responsabilidad del responsable del activo definir la clasificación del activo, revisarlo periódicamente y asegurarse de que se mantiene actualizado y en el nivel adecuado.	3.4.2. Elaborar y aprobar un catálogo de clasificación de la información.
Es conveniente considerar la cantidad de categorías de la información y los beneficios a obtener con su utilización.	3.4.1. Clasificar la información como pública o confidencial.

Tabla 2.28 Comparación entre NTE-ISO/IEC 27002:2009 y EGSI, para el dominio 7. Gestión de Activos (Objetivo de control 7.2.1 Directrices de Clasificación). [38]

En base a la comparación realizada en la tabla 2.28 a nivel del objetivo de control 7.2.1 Directrices de clasificación, el EGSI contempla todos los aspectos de la NTE INEN ISO/IEC 27002:2009.

[38] Elaborado por la autora.

- **Objetivo de control 7.2.2 Etiquetado y manipulado de la información**

NTE INEN-ISO/IEC 27002:2009	EGSI
Procedimientos para el etiquetado y manipulado de la información	**Controles para la definición de procedimientos para el etiquetado y manipulado de la información**
Deberían comprender los activos de información en formatos físico y electrónico.	3.5.1. Procedimientos de etiquetado de la información
Las salidas de los sistemas que contienen información que se clasifica como sensible o crítica deberían portar una etiqueta de clasificación adecuada.	3.5.2. Procedimientos para verificación de cumplimiento del proceso de etiquetado de información
El etiquetado debería reflejar la clasificación según el objetivo de control 7.2.1. Directrices de clasificación.	3.5.2. Procedimientos para verificación de cumplimiento del proceso de etiquetado de información
Los elementos a considerar incluyen informes impresos, presentaciones en pantalla, medios grabados, mensajes electrónicos y transferencia de archivos.	3.5.1. Procedimientos de etiquetado de la información
Por cada nivel de clasificación es recomendable definir los procedimientos de manejo, incluyendo procesamiento, almacenamiento, transmisión, desclasificación, y destrucción seguros.	3.5.2. Procedimientos para verificación de cumplimiento del proceso de etiquetado de información
Los acuerdos con otras organizaciones que incluyen compartir información deberían incluir procedimientos para identificar la clasificación de dicha información y para interpretar las etiquetas de clasificación de otras organizaciones.	3.5.2. Procedimientos para verificación de cumplimiento del proceso de etiquetado de información

Tabla 2.29 Comparación entre NTE-ISO/IEC 27002:2009 y EGSI, para el dominio 7. Gestión de Activos (Objetivo de control 7.2.2 Etiquetado y manipulado de la información). [39]

[39] Elaborado por la autora.

En base a la comparación realizada en la tabla 2.28 a nivel del objetivo de control 7.2.2 Etiquetado y manipulado de la información, el EGSI contempla todos los aspectos de la NTE INEN ISO/IEC 27002:2009.

Conclusión general

De la comparación mostrada en las tablas de la 2.25 a la 2.29, se puede concluir que el EGSI (elaborado en base a la NTE-ISO/IEC 27002:2009) no contempla dos aspectos de la NTE-ISO/IEC 27002:2009:

1. No se considera a las personas y sus calificaciones, habilidades y experiencias como parte de los activos de la organización.
2. No se establecen directrices para el uso de los dispositivos móviles, especialmente para su utilización fuera de las instalaciones de la organización.

Declaración de Aplicabilidad

Debido a la necesidad de evaluación de los niveles de cumplimiento de los objetivos de control y controles del dominio 7. Gestión de Activos en la EEQ, se considera para la evaluación, al EGSI y sus respectivas directrices como la Declaración de Aplicabilidad a utilizar para el análisis de la información recopilada.

Criterios de evaluación de los niveles de cumplimiento

Para la evaluación de los niveles de cumplimiento de los objetivos de control y controles seleccionados, se elaboró la tabla 2.30 que contiene los criterios de evaluación en base a un porcentaje de cumplimiento que oscila desde el 0% al 100%:

Criterio	Descripción	Simbología
Total	Indica que la directriz evaluada tiene un nivel de cumplimiento del 71 al 100%.	T
Parcial	Indica que la directriz evaluada tiene un nivel de cumplimiento del 31 al 70%.	P
Nulo	Indica que la directriz evaluada tiene un nivel de cumplimiento del 0 al 30%.	N

Tabla 2.30 Tabla de criterios de evaluación. [40]

Matriz de criterios de evaluación

Para el cálculo de los criterios de evaluación, se elaboró la matriz de criterios de evaluación mostrada en la tabla 2.31:

Matriz de Criterios de Evaluación	
T / T	T
T / P	P
T / N	P
P / P	P
P / N	P
N / N	N

Tabla 2.31 Matriz de criterios de evaluación. [41]

Resumen del proceso de evaluación

Para el análisis de los datos recopilados, se desarrolló el proceso descrito a continuación:

Utilizando la plantilla de medición de seguridad de la información del Anexo A de la NTE INEN ISO/IEC 27004:2012, se elaboraron las tablas de medición mostradas en las tablas de la 2.32 a la 2.36.

En base a los criterios de evaluación establecidos en la tabla 2.30, se evalúo el nivel de cumplimiento de cada directriz del EGSI tal como se muestra en la tabla 2.37 considerando que, como parte de la recolección de información, se tomaron en cuenta dos ámbitos de evaluación, la Documentación y la Implementación.

A continuación, utilizando la matriz de criterios de evaluación de la tabla 2.31, se obtuvo el nivel de cumplimiento general de cada una de las directrices del EGSI, obteniéndose así el Indicador de cumplimiento por Directriz (EGSI).

Finalmente, utilizando la matriz de criterios de evaluación de la tabla 2.31, se obtuvo el indicador de cumplimiento por cada uno de los controles de la norma

[40] Elaborado por la autora.
[41] Elaborado por la autora.

ISO/IEC 27002, obteniéndose así el Indicador de cumplimiento por Control (ISO / IEC 27002), tal como se muestra en la tabla 2.37.

Medición de la Seguridad de la Información

Para el desarrollo de la medición se utilizó la Plantilla para construcción de la medición de la seguridad de la información, descrita en el Anexo A de la NTE INEN ISO/IEC 27004:2012 [25] y se elaboraron las siguientes tablas (de la Tabla 2.32 a la 2.36), para cada uno de los objetivos de control del dominio 7. Gestión de Activos:

7.1 Responsabilidad sobre los activos	
7.1.1. Inventario de activos	
Identificación de la construcción de la medición	
Nombre de la construcción de la medición	Evaluación del desarrollo de Inventario de activos
Identificador numérico	Específico de la Organización
Propósito de la construcción de la medición	Evaluar el cumplimiento de la política sobre la elaboración del Inventario de activos
Objetivo Control/Proceso	7.1. Responsabilidad sobre los activos
Control (1)/proceso (1)	7.1.1. Inventario de activos
Objeto de la Medición y Atributos	
Objeto de Medición	Inventario de activos
Atributos	Inventario de activos primarios en formatos físicos y/o electrónicos. Inventario de activos de soporte de hardware. Inventario de activos de soporte de software. Inventario de activos de soporte de redes.
Especificación Medida Base (1)	
Medida Base	Nivel de cumplimiento del inventario de activos primarios en formatos físicos y/o electrónicos. Nivel de cumplimiento del inventario de activos de soporte de hardware. Nivel de cumplimiento del inventario de activos de soporte de software. Nivel de cumplimiento del inventario de activos de soporte de redes.
Método de Medición	Ponderar el cumplimiento de la elaboración del inventario de activos.
Tipo de Método de Medición	Subjetivo
Escala	Niveles de cumplimiento: Total (T): Cumplimiento del 71% al 100% Parcial (P): Cumplimiento del 31 al 70% Nulo (N): Cumplimiento del 0 al 305
Tipo de Escala	Relación
Unidad de Medición	Personal Porcentaje

Especificación Medida Derivada	
Medida Derivada	Progreso a la fecha
Función de Medición	Calificación del cumplimiento de la norma, en base a los niveles de cumplimiento de cada control.
Especificación del Indicador	
Indicador	Relación de la cantidad de activos que forman parte del inventario.
Modelo Analítico	Obtener los niveles de cumplimiento de cada control, en base a los niveles de cumplimiento de cada directriz del EGSI.
Especificación Criterios de Decisión	
Criterios de decisión	El objetivo de control se cumple de forma satisfactoria cuando se cumple cuando el nivel de cumplimiento es mayor o igual a 71%, se cumple parcialmente cuando el nivel de cumplimiento va del 31 al 70%, y no se cumple cuando el nivel de cumplimiento es menor o igual al 30%, y es una oportunidad de mejora.
Resultados de la medición	
Interpretación del Indicador	La interpretación del indicador es: - La elaboración del inventario se cumple satisfactoriamente cuando el nivel de cumplimiento es mayor o igual al 71%. - La elaboración del inventario se cumple parcialmente cuando el nivel de cumplimiento varía entre el 31 al 70%, y tiene tendencia a mejorar. - La elaboración del inventario no se cumple cuando el nivel de cumplimiento es menor o igual al 30%, y será considerada como una oportunidad de mejora.
Formatos de Reporte	Tablas de cumplimiento (Tablas de la 2.1 a la 2.6 del proyecto de titulación)
Interesados	
Cliente para medición	Personal de la EEQ
Supervisor de medición	Oficial de Seguridad de la Información
Propietario de la Información	EEQ
Recolector de la Información	Autora del proyecto de titulación
Comunicador de Información	Autora del proyecto de titulación
Frecuencia/Período	
Frecuencia de Recolección de Datos	Una vez
Frecuencia de Análisis de Datos	Una vez
Frecuencia del Reporte de Resultados de Medición	Una vez
Revisión de la Medición	Una vez
Período de Medición	Una vez

Tabla 2.32 Medición de cumplimiento – 7.1.1. Inventario de activos

7.1 Responsabilidad sobre los activos	
7.1.2. Responsable de los activos	
Identificación de la construcción de la medición	
Nombre de la construcción de la medición	Asignación de Responsable de los activos
Identificador numérico	Específico de la Organización
Propósito de la construcción de la medición	Evaluar el cumplimiento de la política sobre el Responsable de los activos
Objetivo Control/Proceso	7.1. Responsabilidad sobre los activos
Control (1)/proceso (1)	7.1.2. Responsable de los activos
Objeto de la Medición y Atributos	
Objeto de Medición	Responsable de los activos
Atributo	Asignación de Responsables de los activos Consolidación de inventarios de activos con sus responsables
Especificación Medida Base (1)	
Medida Base	Nivel de cumplimiento de la asignación de responsables de los activos. Nivel de cumplimiento de la consolidación de inventarios de activos con sus responsables.
Método de Medición	Ponderar el cumplimiento de la política de Responsables de los activos
Tipo de Método de Medición	Subjetivo
Escala	Niveles de cumplimiento: Total (T): Cumplimiento del 71% al 100% Parcial (P): Cumplimiento del 31 al 70% Nulo (N): Cumplimiento del 0 al 305
Tipo de Escala	Relación
Unidad de Medición	Personal Porcentaje
Especificación Medida Derivada	
Medida Derivada	Progreso a la fecha
Función de Medición	Calificación del cumplimiento de la norma, en base a los niveles de cumplimiento de cada control.
Especificación del Indicador	
Indicador	Cantidad de activos asignados a un responsable. Porcentaje de consolidación de inventarios de activos con sus responsables.
Modelo Analítico	Obtener los niveles de cumplimiento de cada control, en base a los niveles de cumplimiento de cada directriz del EGSI.

Especificación Criterios de Decisión	
Criterios de decisión	El objetivo de control se cumple de forma satisfactoria cuando se cumple cuando el nivel de cumplimiento es mayor o igual a 71%, se cumple parcialmente cuando el nivel de cumplimiento va del 31 al 70%, y no se cumple cuando el nivel de cumplimiento es menor o igual al 30%, y es una oportunidad de mejora.
Resultados de la medición	
Interpretación del Indicador	La interpretación del indicador es: - La elaboración del inventario se cumple satisfactoriamente cuando el nivel de cumplimiento es mayor o igual al 71%. - La elaboración del inventario se cumple parcialmente cuando el nivel de cumplimiento varía entre el 31 al 70%, y tiene tendencia a mejorar. - La elaboración del inventario no se cumple cuando el nivel de cumplimiento es menor o igual al 30%, y será considerada como una oportunidad de mejora.
Formatos de Reporte	Tablas de cumplimiento (Tablas de la 2.7 a la 2.8 del proyecto de titulación)
Interesados	
Cliente para medición	Personal de la EEQ
Supervisor de medición	Oficial de Seguridad de la Información
Propietario de la Información	EEQ
Recolector de la Información	Autora del proyecto de titulación
Comunicador de Información	Autora del proyecto de titulación
Frecuencia/Período	
Frecuencia de Recolección de Datos	Una vez
Frecuencia de Análisis de Datos	Una vez
Frecuencia del Reporte de Resultados de Medición	Una vez
Revisión de la Medición	Una vez
Período de Medición	Una vez

Tabla 2.33 Medición de la seguridad de la información - 7.1.2. Responsable de los activos

7.1 Responsabilidad sobre los activos	
7.1.3. Uso aceptable de los activos	
Identificación de la construcción de la medición	
Nombre de la construcción de la medición	Uso aceptable de los activos
Identificador numérico	Específico de la Organización
Propósito de la construcción de la medición	Evaluar el cumplimiento de la política sobre el Uso aceptable de los activos
Objetivo Control/Proceso	7.1. Responsabilidad sobre los activos
Control (1)/proceso (1)	7.1.3. Uso aceptable de los activos
Objeto de la Medición y Atributos	
Objeto de Medición	Uso aceptable de los activos
Atributo	Reglamentar el uso de correo electrónico institucional. Reglamentar el acceso y uso de la Internet y sus aplicaciones/servicios. Reglamentar el uso de los sistemas de video-conferencia.
Especificación Medida Base (1)	
Medida Base	Nivel de cumplimiento de la reglamentación del uso de correo electrónico institucional. Nivel de cumplimiento de la reglamentación del acceso y uso de la Internet y sus aplicaciones/servicios. Nivel de cumplimiento de la reglamentación del uso de los sistemas de video-conferencia.
Método de Medición	Ponderar el cumplimiento de la política de Uso aceptable de los activos.
Tipo de Método de Medición	Subjetivo
Escala	Niveles de cumplimiento: Total (T): Cumplimiento del 71% al 100% Parcial (P): Cumplimiento del 31 al 70% Nulo (N): Cumplimiento del 0 al 305
Tipo de Escala	Relación
Unidad de Medición	Personal Porcentaje
Especificación Medida Derivada	
Medida Derivada	Progreso a la fecha
Función de Medición	Calificación del cumplimiento de la norma, en base a los niveles de cumplimiento de cada control.
Especificación del Indicador	

Indicador	Existencia de políticas y/o procedimientos para el uso de correo electrónico institucional. Existencia de políticas y/o procedimientos para el acceso y uso de la Internet y sus aplicaciones/servicios. Existencia de políticas y/o procedimientos para el uso de los sistemas de video-conferencia.
Modelo Analítico	Obtener los niveles de cumplimiento de cada control, en base a los niveles de cumplimiento de cada directriz del EGSI.
Especificación Criterios de Decisión	
Criterios de decisión	El objetivo de control se cumple de forma satisfactoria cuando se cumple cuando el nivel de cumplimiento es mayor o igual a 71%, se cumple parcialmente cuando el nivel de cumplimiento va del 31 al 70%, y no se cumple cuando el nivel de cumplimiento es menor o igual al 30%, y es una oportunidad de mejora.
Resultados de la medición	
Interpretación del Indicador	La interpretación del indicador es: - La elaboración del inventario se cumple satisfactoriamente cuando el nivel de cumplimiento es mayor o igual al 71%. - La elaboración del inventario se cumple parcialmente cuando el nivel de cumplimiento varía entre el 31 al 70%, y tiene tendencia a mejorar. - La elaboración del inventario no se cumple cuando el nivel de cumplimiento es menor o igual al 30%, y será considerada como una oportunidad de mejora.
Formatos de Reporte	Tablas de cumplimiento (Tablas de la 2.9 a la 2.15 del proyecto de titulación)
Interesados	
Cliente para medición	Personal de la EEQ
Supervisor de medición	Oficial de Seguridad de la Información
Propietario de la Información	EEQ
Recolector de la Información	Autora del proyecto de titulación
Comunicador de Información	Autora del proyecto de titulación
Frecuencia/Período	
Frecuencia de Recolección de Datos	Una vez
Frecuencia de Análisis de Datos	Una vez
Frecuencia del Reporte de Resultados de Medición	Una vez
Revisión de la Medición	Una vez
Período de Medición	Una vez

Tabla 2.34 Medición de la Seguridad de la Información – 7.1.3. Uso aceptable de los activos

7.2. Clasificación de la información	
7.2.1. Directrices de clasificación	
Identificación de la construcción de la medición	
Nombre de la construcción de la medición	Directrices de clasificación de la información
Identificador numérico	Específico de la Organización
Propósito de la construcción de la medición	Evaluar el cumplimiento de la política sobre las Directrices de clasificación
Objetivo Control/Proceso	7.2. Clasificación de la información
Control (1)/proceso (1)	7.2.1. Directrices de clasificación
Objeto de la Medición y Atributos	
Objeto de Medición	Directrices de clasificación de la información
Atributos	Clasificación de la información como pública o confidencial. Elaboración y aprobación de un catálogo de clasificación de la información.
Especificación Medida Base (1)	
Medida Base	Nivel de cumplimiento de la clasificación de la información como pública o confidencial. Nivel de cumplimiento de la elaboración y aprobación de un catálogo de clasificación de la información.
Método de Medición	Ponderar el cumplimiento de la creación de directrices de clasificación de la información.
Tipo de Método de Medición	Subjetivo
Escala	Niveles de cumplimiento: Total (T): Cumplimiento del 71% al 100% Parcial (P): Cumplimiento del 31 al 70% Nulo (N): Cumplimiento del 0 al 305
Tipo de Escala	Relación
Unidad de Medición	Personal Porcentaje
Especificación Medida Derivada	
Medida Derivada	Progreso a la fecha
Función de Medición	Calificación del cumplimiento de la norma, en base a los niveles de cumplimiento de la cada control.
Especificación del Indicador	
Indicador	Relación de la cantidad de información clasificada como pública o confidencial. Elaboración y aprobación de un catálogo de clasificación de la información.
Modelo Analítico	Obtener los niveles de cumplimiento de cada control, en base a los niveles de cumplimiento de cada directriz del EGSI.

Especificación Criterios de Decisión	
Criterios de decisión	El objetivo de control se cumple de forma satisfactoria cuando se cumple cuando el nivel de cumplimiento es mayor o igual a 71%, se cumple parcialmente cuando el nivel de cumplimiento va del 31 al 70%, y no se cumple cuando el nivel de cumplimiento es menor o igual al 30%, y es una oportunidad de mejora.
Resultados de la medición	
Interpretación del Indicador	La interpretación del indicador es: - La elaboración del inventario se cumple satisfactoriamente cuando el nivel de cumplimiento es mayor o igual al 71%. - La elaboración del inventario se cumple parcialmente cuando el nivel de cumplimiento varía entre el 31 al 70%, y tiene tendencia a mejorar. - La elaboración del inventario no se cumple cuando el nivel de cumplimiento es menor o igual al 30%, y será considerada como una oportunidad de mejora.
Formatos de Reporte	Tablas de cumplimiento (Tabla 2.16 del proyecto de titulación)
Interesados	
Cliente para medición	Personal de la EEQ
Supervisor de medición	Oficial de Seguridad de la Información
Propietario de la Información	EEQ
Recolector de la Información	Autora del proyecto de titulación
Comunicador de Información	Autora del proyecto de titulación
Frecuencia/Período	
Frecuencia de Recolección de Datos	Una vez
Frecuencia de Análisis de Datos	Una vez
Frecuencia del Reporte de Resultados de Medición	Una vez
Revisión de la Medición	Una vez
Período de Medición	Una vez

Tabla 2.35 Medición de la seguridad de la información – 7.2.1. Directrices de clasificación

7.2 Responsabilidad sobre los activos	
7.2.2. Etiquetado y manipulado de la información	
Identificación de la construcción de la medición	
Nombre de la construcción de la medición	Etiquetado y manipulación de la información
Identificador numérico	Específico de la Organización
Propósito de la construcción de la medición	Evaluar el cumplimiento de la política sobre el etiquetado y manipulado de la información.
Objetivo Control/Proceso	7.2. Clasificación de la información
Control (1)/proceso (1)	7.2.2. Etiquetado y manipulado de la información.
Objeto de la Medición y Atributos	
Objeto de Medición	Etiquetado y manipulación de la información
Atributos	Procedimientos de etiquetado de la información. Procedimientos para verificación de cumplimiento del proceso de etiquetado de información.
Especificación Medida Base (1)	
Medida Base	Nivel de cumplimiento de la elaboración de procedimientos para el etiquetado de la información. Nivel de cumplimiento de la elaboración de procedimientos para la verificación del cumplimiento del proceso de etiquetado de información.
Método de Medición	Ponderar el cumplimiento del Etiquetado y manipulado de la información.
Tipo de Método de Medición	Subjetivo
Escala	Niveles de cumplimiento: Total (T): Cumplimiento del 71% al 100% Parcial (P): Cumplimiento del 31 al 70% Nulo (N): Cumplimiento del 0 al 305
Tipo de Escala	Relación
Unidad de Medición	Personal Porcentaje
Especificación Medida Derivada	
Medida Derivada	Progreso a la fecha
Función de Medición	Calificación del cumplimiento de la norma, en base a los niveles de cumplimiento de la cada control.
Especificación del Indicador	
Indicador	Existencia de procedimientos de etiquetado de la información. Existencia de procedimientos para la verificación de cumplimiento del proceso de etiquetado de la información.
Modelo Analítico	Obtener los niveles de cumplimiento de cada control, en base a los niveles de cumplimiento de cada directriz del EGSI.

Especificación Criterios de Decisión	
Criterios de decisión	El objetivo de control se cumple de forma satisfactoria cuando se cumple cuando el nivel de cumplimiento es mayor o igual a 71%, se cumple parcialmente cuando el nivel de cumplimiento va del 31 al 70%, y no se cumple cuando el nivel de cumplimiento es menor o igual al 30%, y es una oportunidad de mejora.
Resultados de la medición	
Interpretación del Indicador	La interpretación del indicador es: - La elaboración del inventario se cumple satisfactoriamente cuando el nivel de cumplimiento es mayor o igual al 71%. - La elaboración del inventario se cumple parcialmente cuando el nivel de cumplimiento varía entre el 31 al 70%, y tiene tendencia a mejorar. - La elaboración del inventario no se cumple cuando el nivel de cumplimiento es menor o igual al 30%, y será considerada como una oportunidad de mejora.
Formatos de Reporte	Tablas de cumplimiento (Tabla 2.17 del proyecto de titulación)
Interesados	
Cliente para medición	Personal de la EEQ
Supervisor de medición	Oficial de Seguridad de la Información
Propietario de la Información	EEQ
Recolector de la Información	Autora del proyecto de titulación
Comunicador de Información	Autora del proyecto de titulación
Frecuencia/Período	
Frecuencia de Recolección de Datos	Una vez
Frecuencia de Análisis de Datos	Una vez
Frecuencia del Reporte de Resultados de Medición	Una vez
Revisión de la Medición	Una vez
Período de Medición	Una vez

Tabla 2.36 Medición de seguridad de la información – 7.2.2. Etiquetado y manipulado de la información

Evaluación del nivel de cumplimiento de cada directriz del EGSI

La tabla 2.37 mostrada a continuación, contiene la evaluación de los niveles de cumplimiento de cada una de las directrices del EGSI, en base a los criterios de evaluación indicados en la tabla 2.30 (columnas 5 y 7) y de cada uno de los

controles de la NTE INEN ISO/IEC 27002 en base a la matriz de criterios de evaluación de la tabla 2.31 (columnas 6 y 8):

ISO/IEC 27002:2005			EGSI	Documentación		Implementación	
Dominios	**Objetivos de Control**	**Controles**	**Directriz**	**Nivel de cumplimiento por Directriz (EGSI)**	**Nivel de cumplimiento por Control (ISO/IEC 27002)**	**Nivel de cumplimiento por Directriz (EGSI)**	**Nivel de cumplimiento por Control (ISO/IEC 27002)**
7. Gestión de Activos	**7.1. Responsabilidad sobre los activos**	7.1.1. Inventario de activos	3.1.1. Inventario de activos primarios en formatos físicos y/o electrónicos 3.1.2. Inventario de activos de soporte de Hardware 3.1.3. Inventario de activos de soporte de Software 3.1.4. Inventario de activos de soporte de Redes	**T** **T** **T** **T**	**T**	**P** **T** **P** **T**	**P**
		7.1.2. Responsable de los activos	3.2.1. Asignación de Responsables de los Activos 3.2.2. Consolidación inventarios de activos con sus responsables	**P** **T**	**P**	**T** **P**	**P**
		7.1.3. Uso aceptable de los activos.	3.3.1. Reglamentar uso de correo electrónico institucional 3.3.2. Reglamentar el acceso y uso de la Internet y sus aplicaciones/servicios 3.3.3. Reglamentar el uso de los sistemas de video - conferencias	**P** **N** **P**	**P**	**T** **T** **P**	**P**
	7.2. Clasificación de la información	7.2.1. Directrices de clasificación	3.4.1. Clasificar la información como pública o confidencial 3.4.2. Elaborar y aprobar un catálogo de clasificación de la información	**T** **T**	**T**	**P** **P**	**P**
		7.2.2. Etiquetado y manipulado de la información	3.5.1. Procedimientos de etiquetado de la información 3.5.2. Procedimiento para verificación de cumplimiento del proceso de etiquetado de información	**P** **P**	**P**	**P** **P**	**P**

Tabla 2.37 Niveles de cumplimiento en base a los criterios de evaluación. [42]

[42] Elaborado por la autora.

Conclusión del proceso de evaluación

La información recopilada corresponde a las directrices de evaluación del EGSI correspondientes a los controles y objetivos de control del dominio 7. Gestión de activos de la norma ISO 27002, es decir, que se realiza una evaluación parcial de la normal en relación a lo establecido con el Oficial de Seguridad de la Información.

De los niveles de resultados obtenidos en la evaluación, se puede determinar que los niveles de cumplimiento de la Documentación son mayores que los niveles de cumplimiento de la Implementación.

Estos resultados indican que en la EEQ se considera primordial la elaboración de documentación formal que rija a toda la organización, con el fin de definir claramente el camino a seguir previo a la implementación de un Sistema de Gestión de Seguridad de la Información.

Además, cabe recalcar que debido al proceso de mejora en el que se encuentra la EEQ, los controles evaluados están en proceso de implementación, para la cual se están elaborando y formalizando documentos que contienen políticas y/o procedimientos que permitirán una correcta gestión de la seguridad de la información en la EEQ, y a futuro, una correcta implementación de un SGSI en toda la organización.

2.3. ELABORACIÓN DEL INFORME EJECUTIVO

Adjunto a este documento se encuentra el Informe Ejecutivo (Anexo A) elaborado en base a la información recopilada y analizada, presentada en este proyecto de titulación y cuya finalidad es la de dar a conocer dicho análisis al personal técnico de la EEQ responsable del manejo de la seguridad de la información.

2.4. ELABORACIÓN DEL INFORME TÉCNICO

Adjunto a este documento se encuentra el Informe Técnico (Anexo B) elaborado en base a la información recopilada y analizada, el mismo que tiene por objetivo servir de ayuda al personal técnico de la EEQ para la evaluación de una correcta Gestión de la Seguridad de la Información.

3. CAPÍTULO 3. CONCLUSIONES Y RECOMENDACIONES

3.1. CONCLUSIONES

- Para la evaluación parcial del sistema de gestión de la seguridad de la información de la Empresa Eléctrica Quito desarrollada en este proyecto de titulación, se utilizó como dominio de evaluación, al Dominio 7. Gestión de Activos de la norma ISO 27002 junto con sus objetivos de control y controles respetivos. Como soporte a dicho dominio de evaluación, se utilizaron las directrices de evaluación del EGSI, y los CSCs de Sans Institute, lo cual permitió identificar las oportunidades de mejora de la EEQ.
- La EEQ se encuentra en un proceso de mejora continua, el mismo que está basado en la implementación de las directrices del EGSI, y que contempla actividades de mejora para la correcta gestión de la seguridad de la información.
- Para la evaluación, se utilizó una propuesta metodológica elaborada por la autora, la misma que fue desarrolla en base a la información recolectada y a las directrices, normas y controles utilizados para llevar a cabo dicha evaluación.
- Como resultado de la evaluación a la información recopilada, se logró identificar que en la EEQ se rigen estrictamente a la documentación formal elaborada en base a la norma ISO / IEC 27002, siendo ésta el punto de partida para la implementación de un Sistema de Gestión de Seguridad de la Información.
- Los resultados obtenidos durante la evaluación, indican que en la EEQ se tiene un nivel parcial de cumplimiento, lo cual indica que las tareas que se han estado llevando a cabo en la EEQ si están siendo documentadas e implementadas exitosamente, y con el futuro se podrá implantar un Sistema de Gestión de la Seguridad de la Información de una forma más fácil.

- Con respecto a la Documentación, se determinó que la EEQ cumple un 58,82% de las directrices del EGSI en cuanto a la Gestión de Activos. Se cumple parcialmente un 17,65%, y no se cumple un 23,53%. Es decir, la mayoría de las directrices del EGSI están contempladas en la documentación formal publicada y por publicar.
- Con respecto a la Implementación, se determinó que la EEQ cumple un 44,11% de las directrices del EGSI en cuanto a la Gestión de Activos. Se cumple parcialmente un 19,11%, y no se cumple un 36,77%. El nivel de incumplimiento de las directrices es alto y se debe a que se está elaborando previamente la documentación formal que respalde la implementación.

3.2. RECOMENDACIONES

- La EEQ, de acuerdo a los resultados obtenidos, debería implementar todas las directrices del EGSI, para que en un futuro cercano se implemente un Sistema de Gestión de Seguridad de la Información, el cual les permitirá automatizar varios procesos para una adecuada gestión de la seguridad de la información.
- Con respecto a la situación actual de la EEQ, se debería utilizar la NTE-ISO/IEC 27002 como parte del proceso de mejora, con la finalidad de que se identifiquen los sectores más vulnerables y se tomen las medidas correctivas necesarias para la disminución o eliminación de riesgos de seguridad, no solo de la información, sino de todos los elementos que conforman la organización.
- En la Empresa Eléctrica Quito se debería definir un solo documento para el Inventario de Activos, el mismo que debe ser gestionado por la DTIC y en cual se identifiquen claramente las características de todos los activos, de tal forma que se tenga una mayor conocimiento de la situación de la institución y se puedan tomar medidas preventivas o correctivas en cuanto al uso de los equipos activos en la EEQ.
- Se recomienda a la EEQ, la utilización de la NTE ISO/IEC 27004 [25] como ayuda para la evaluación de la eficacia de un Sistema de Gestión de Seguridad de la Información, la misma que incluye un Programa de

Medición de Seguridad de la Información que ayudará a la organización, en la identificación y evaluación de los procesos y controles del SGSI ineficaces y dará prioridades a las acciones asociadas con el mejoramiento o cambio de dichos procesos y/o controles.

- En la EEQ, antes de implementar cambios estratégicos en la compañía, se debería brindar la información necesaria a todo el personal sobre dicho cambio y las ventajas que se obtendrán. De ésta forma las personas tendrán claro el objetivo del cambio y por lo tanto cooperarán de mejor manera con el mismo y se evitará que se reúsen por miedo o desconocimiento.

BIBLIOGRAFÍA

[1] Empresa Eléctrica Quito, <<Servicio Público de Energía Eléctrica y su área de concesión – Empresa Eléctrica Quito>>, 2015. [En línea] Disponible en: http://www.eeq.com.ec/. [Último ingreso: 06/08/2014].

[2] Empresa Eléctrica Quito, <<PLAN ESTRATÉGICO EEQ 2012 – 2015>>, 2012 -2015. [En línea]. Disponible en: http://ftp.eeq.com.ec/upload/informacionPublica/PLANESTRATEGICO2012-2015.pdf. [Último ingreso: 07/12/2014].

[3] Information Security del Ecuador Inc. (I-SEC), <<Sistema de Gestión de Seguridad de la Información>>, Octubre 2013.

[4] Subsecretaría Nacional de la Gestión Pública, 2014. [En línea] Disponible en http://www.administracionpublica.gob.ec/subsecretaria-general-de-la-gestion-publica/. [Último ingreso: 07/12/2014].

[5] **REGISTRO OFICIAL** – ÓRGANO DEL GOBIENO DEL ECUADOR Administración del Sr. Ec. Rafael Correa Delgado Presidente Constitucional de la República, SEGUNDO SUPLEMENTO, Secretaría Nacional de la Administración Pública, Acuerdo No. 166. Septiembre 2013.

[6] Empresa Eléctrica Quito, << Resolución de Gerencia General No. GCG-2884-2014>>, 16 de Abril de 2014.

[7] Empresa Eléctrica Quito, <<Reforma a la Resolución de Gerencia General No. GEG-2884-2014 del 16 de Abril de 2014>>, 04 de Septiembre de 2014.

[8] Secretaría Nacional de la Administración Pública, <<**Anexo 1 del Acuerdo No. 166 del 19 de septiembre de 2013.** Esquema Gubernamental de la Seguridad de la Información (EGSI)>>, Versión 1.0, Septiembre de 2013.

[9] iso27002.es, <<El Anexo de ISO 27001 en español>> [En línea] Disponible en: http://www.iso27002.es/ [Último ingreso: 07/12/2014].

[10] SANS, <<SANS Institute>> [En línea] Disponible en: http://www.sans.org [Último ingreso: 07/12/2014].

[11] SANS, <<Critical Security Controls>> [En línea] Disponible en: http://www.sans.org/critical-security-controls [Último ingreso: 07/12/2014].

[12] ISO, <<ISO/IEC 27002:2005>> [En línea] Disponible en: http://www.iso.org/iso/catalogue_detail?csnumber=50297 [Último ingreso: 22/02/2015].

[13] Empresa Eléctrica Quito "E.E.Q. S.A.", <<EQUIPOS ACTIVOS EN LA EMPRESA ELÉCTRICA>> [Documento digital], Fecha de consulta: 29/01/2015.

[14] Empresa Eléctrica Quito "E.E.Q. S.A.", <<Inventario de Plataforma>> [Documento digital], Fecha de consulta: 22/02/2015.

[15] Empresa Eléctrica Quito "E.E.Q. S.A.", << SISTEMA DE GESTIÓN DE LA CALIDAD – Procedimiento para control de bienes. (GR-GBB-P003)>>, Revisión 08. [Documento digital].

[16] Empresa Eléctrica Quito "E.E.Q. S.A.", <<SISTEMA DE GESTIÓN DE LA CALIDAD - Políticas para el uso y manejo de los recursos informáticos de la EEQ. (TI-D001)>>, Revisión 02. [Documento digital].

[17] Empresa Eléctrica Quito "E.E.Q. S.A.", << SISTEMA DE GESTIÓN DE LA CALIDAD - Procedimiento para administración de redes y comunicaciones (TI-GRC-P001)>>, Revisión 03. [Documento digital].

[18] Empresa Eléctrica Quito "E.E.Q. S.A.", << SISTEMA DE GESTIÓN DE LA CALIDAD - Procedimiento para la gestión del portal web empresarial (TI-GDS-P003)>>, Revisión 00. [Documento digital].

[19] Empresa Eléctrica Quito "E.E.Q. S.A.", << SISTEMA DE GESTIÓN DE LA CALIDAD - Procedimiento administración de servicios Internet y Correo (TI-GBD-P004)>>, Revisión 02. [Documento Digital].

[20] Empresa Eléctrica Quito "E.E.Q. S.A.", << SISTEMA DE GESTIÓN DE LA CALIDAD - Procedimiento para administración de seguridades y accesos (TI-GBD-P003)>>, Revisión 02. [Documento Digital].

[21] Empresa Eléctrica Quito “E.E.Q. S.A.”, << SISTEMA DE GESTIÓN DE LA CALIDAD – Instructivo para Control Bienes (GR-GBB-P003-I001)>>, Revisión 08. [Documento Digital].

[22] Secretaría Nacional de la Administración Pública, <<Quipux Gestión Documental>> [En línea] Disponible en: http://www.gestiondocumental.gob.ec/ [Último ingreso 27/04/2015].

[23] Systems Experts, <<Looking at the SANS 20 Critical Security Controls – Mapping de SANS 20 to NIST 800-53 to ISO 27002 by Brad C. Jhonson>> [En línea] Disponible en: http://systemexperts.com/media/pdf/SystemExperts-SANS20-1.pdf [Último ingreso: 26/07/2015].

[24] INEN Instituto Ecuatoriano de Normalización, <<NORMA TÉCNICA ECUATORIANA NTE INEN-ISO/IEC 27002:2009>>, Primera edición, Quito-Ecuador. [Documento Digital], [Último ingreso: 06/08/2015].

[25] INEN Instituto Ecuatoriano de Normalización, <<NORMA TÉCNICA ECUATORIANA NTE INEN-ISO/IEC 27004:2012>>, Primera edición, Quito-Ecuador. [Documento Digital], [Último ingreso: 21/09/2015].

ANEXOS

ANEXO A: Informe Ejecutivo

INFORME EJECUTIVO

Yo, Sara Echeverría, estudiante de la Escuela Politécnica Nacional, mediante el presente documento agradezco a la Empresa Eléctrica Quito S.A. por todas las facilidades brindadas para realizar el proyecto de titulación EVALUACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA ELÉCTRICA QUITO UTILIZANDO LA NORMA ISO 27002, tomando en cuenta que al momento de la evaluación, la Empresa Eléctrica Quito S.A. se encontraba en el proceso de implementación del Esquema Gubernamental la Seguridad de la Información (EGSI).

Además, expongo a mandos gerenciales, las conclusiones y recomendaciones elaboradas después de finalizar mi proyecto de titulación, y que fue llevado a cabo mediante la aplicación de procedimientos de evaluación de la ISO 27002 y del EGSI.

Durante la evaluación, se cumplió con las siguientes etapas principales y etapas secundarias:

- Planteamiento del problema
  - Reconocimiento de la E.E.Q. S.A.,
  - Situación Actual de la Seguridad de la Información en la E.E.Q. S.A.,
- Evaluación del Sistema de Gestión de Seguridad de la Información de la E.E.Q. S.A
  - Aplicación de los dominios de la Norma ISO 27002 seleccionados al S.G.S.I. de la E.E.Q. S.A.,

    - Análisis de Resultados,
    - Elaboración del Informe Ejecutivo,
    - Elaboración del Informe Técnico.
- Conclusiones y Recomendaciones
    - Conclusiones,
    - Recomendaciones.

Para las dos primeras etapas principales y sus respectivas etapas secundarias, se requirió de la información de la institución, la misma que se obtuvo gracias a la ayuda del Oficial de Seguridad de la Información, Ing. Eduardo Alvear, y a la información publicada en la página web www.eeq.com.ec.

La recolección de información se hizo a través de entrevistas personales con el Oficial de Seguridad de la Información, el cual fue muy amable al indicarme cada documento existente y los procesos que se llevan a cabo en la EEQ, siempre que le fue posible ya que por cuestiones de seguridad, no fue posible la entrega de información con mayor detalle.

Para el proceso de Evaluación, se utilizó Esquema Gubernamental de Seguridad de la Información, contenido en el Acuerdo 166 de la Secretaría Nacional de la Administración Pública (SNAP). Además, se utilizaron varios de los Critical Security Controls, establecidos por el SANS Institute (SysAdmin Audit, Networking and Security Institute) con el fin de brindar un análisis más adecuado de la seguridad de la información en la EEQ.

Finalmente, después de la evaluación de la información recolectada, pongo a disposición de la Empresa Eléctrica Quito S.A. las siguientes conclusiones y recomendaciones:

CONCLUSIONES

- Para la evaluación parcial del sistema de gestión de la seguridad de la información de la Empresa Eléctrica Quito desarrollada en este proyecto de titulación, se utilizó como dominio de evaluación, al Dominio 7. Gestión de Activos de la norma ISO 27002 junto con sus objetivos de control y controles respetivos. Como soporte a dicho dominio de evaluación, se utilizaron las directrices de evaluación del EGSI, y los CSCs de Sans Institute, lo cual permitió identificar las oportunidades de mejora de la EEQ.
- La EEQ se encuentra en un proceso de mejora continua, el mismo que está basado en la implementación de las directrices del EGSI, y que contempla actividades de mejora para la correcta gestión de la seguridad de la información.
- Para la evaluación, se utilizó una propuesta metodológica elaborada por la autora, la misma que fue desarrolla en base a la información recolectada y a las directrices, normas y controles utilizados para llevar a cabo dicha evaluación.
- Como resultado de la evaluación a la información recopilada, se logró identificar que en la EEQ se rigen estrictamente a la documentación formal elaborada en base a la norma ISO / IEC 27002, siendo ésta el punto de partida para la implementación de un Sistema de Gestión de Seguridad de la Información.
- Los resultados obtenidos durante la evaluación, indican que en la EEQ se tiene un nivel parcial de cumplimiento, lo cual indica que las tareas que se han estado llevando a cabo en la EEQ si están siendo documentadas e implementadas exitosamente, y con el futuro se podrá implantar un Sistema de Gestión de la Seguridad de la Información de una forma más fácil.
- Con respecto a la Documentación, se determinó que la EEQ cumple un 58,82% de las directrices del EGSI en cuanto a la Gestión de Activos. Se cumple parcialmente un 17,65%, y no se cumple un 23,53%. Es decir, la

mayoría de las directrices del EGSI están contempladas en la documentación formal publicada y por publicar.

- Con respecto a la Implementación, se determinó que la EEQ cumple un 44,11% de las directrices del EGSI en cuanto a la Gestión de Activos. Se cumple parcialmente un 19,11%, y no se cumple un 36,77%. El nivel de incumplimiento de las directrices es alto y se debe a que se está elaborando previamente la documentación formal que respalde la implementación.

RECOMENDACIONES

- La EEQ, de acuerdo a los resultados obtenidos, debería implementar todas las directrices del EGSI, para que en un futuro cercano se implemente un Sistema de Gestión de Seguridad de la Información, el cual les permitirá automatizar varios procesos para una adecuada gestión de la seguridad de la información.
- Con respecto a la situación actual de la EEQ, se debería utilizar la NTE-ISO/IEC 27002 como parte del proceso de mejora, con la finalidad de que se identifiquen los sectores más vulnerables y se tomen las medidas correctivas necesarias para la disminución o eliminación de riesgos de seguridad, no solo de la información, sino de todos los elementos que conforman la organización.
- En la Empresa Eléctrica Quito se debería definir un solo documento para el Inventario de Activos, el mismo que debe ser gestionado por la DTIC y en cual se identifiquen claramente las características de todos los activos, de tal forma que se tenga una mayor conocimiento de la situación de la institución y se puedan tomar medidas preventivas o correctivas en cuanto al uso de los equipos activos en la EEQ.
- Se recomienda a la EEQ, la utilización de la NTE ISO/IEC 27004 [25] como ayuda para la evaluación de la eficacia de un Sistema de Gestión de Seguridad de la Información, la misma que incluye un Programa de Medición de Seguridad de la Información que ayudará a la organización,

en la identificación y evaluación de los procesos y controles del SGSI ineficaces y dará prioridades a las acciones asociadas con el mejoramiento o cambio de dichos procesos y/o controles.

- En la EEQ, antes de implementar cambios estratégicos en la compañía, se debería brindar la información necesaria a todo el personal sobre dicho cambio y las ventajas que se obtendrán. De ésta forma las personas tendrán claro el objetivo del cambio y por lo tanto cooperarán de mejor manera con el mismo y se evitará que se reúsen por miedo o desconocimiento.

ANEXO B: Informe Técnico

INFORME TÉCNICO

Yo, Sara Echeverría, estudiante de la Escuela Politécnica Nacional, mediante el presente documento agradezco a la Empresa Eléctrica Quito S.A. por todas las facilidades brindadas para realizar mi proyecto de titulación EVALUACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA ELÉCTRICA QUITO UTILIZANDO LA NORMA ISO 27002, tomando en cuenta que al momento de la evaluación, la Empresa Eléctrica Quito S.A. se encontraba en el proceso de implementación del Esquema Gubernamental la Seguridad de la Información (EGSI).

Además, expongo al personal técnico, el siguiente Informe Técnico elaborado como producto de la finalización de mi proyecto de titulación.

MARCO TEÓRICO

CAPÍTULO 1. PLANTEAMIENTO DEL PROBLEMA

En este capítulo se realiza una descripción general de la Empresa Eléctrica Quito S.A. (EEQ en adelante), así como también, de la situación actual de la misma en base a las normativas establecidas en la Constitución de la República del Ecuador, referentes a los sectores estratégicos, de decisión y control exclusivo del Estado Ecuatoriano.

A continuación, se presentará un resumen de la norma ISO 27002, la misma que servirá como guía en la evaluación del Sistema de Gestión de Seguridad de la

Información (SGSI en adelante)43 que se llevará a cabo en la EEQ. Además, se resumirán también, el Esquema Gubernamental de la Seguridad de la Información (EGSI en adelante), que rige a las empresas de control exclusivo del Estado Ecuatoriano y que fue establecido por la Secretaría Nacional de Administración Pública (SNAP en adelante)44 ; así como también, los Controles Críticos de Seguridad (CSC en adelante)45 de SANS Institute, que serán utilizados como apoyo para la evaluación antes mencionada.

- **RECONOCIMIENTO DE LA E.E.Q. S.A**

DATOS DE LA EMPRESA

A continuación se muestran datos generales de la empresa, los mismos que fueron tomados de la página web de la EEQ. [1]

Nombre: EMPRESA ELÉCTICA QUITO S.A. (E.E.Q. S.A.)

Dirección: Avenida 10 de Agosto y las Casas

Teléfono: (593) (02) 3964 - 700

RESEÑA HISTÓRICA Y CONSTITUCIÓN

La Empresa Eléctrica Quito S.A. en la actualidad tiene 119 años de existencia. Desde 1894 ha iluminado la ciudad, partiendo del Centro Histórico de Quito expandiendo su servicio hasta zonas rurales y urbano marginal. En la actualidad se trabaja en el plan de expansión que se extiende hasta el año 2015. Adquiriendo nuevas líneas de Sub-transmisión y subestaciones para mejorar la confiabilidad del sistema eléctrico del Distrito Metropolitano de Quito.

[43] El SGSI es un conjunto de políticas para una correcta y adecuada gestión de la información.
[44] La SNAP establece herramientas para el mejoramiento de la eficiencia en la administración de las empresas de control del Estado Ecuatoriano.
[45] Los CSCs son una serie de 20 controles enfocados en la seguridad de la información.

PRINCIPAL ACTIVIDAD

La actividad principal de la empresa es brindar servicio eléctrico a ciertas zonas de las provincias de Pichincha, Imbabura, Napo y Cotopaxi.

INFRAESTRUCTURA

La EEQ opera en diferentes ciudades del Ecuador, teniendo su edificio matriz en la ciudad de Quito, y sus sucursales en ciudades como Rumiñahui, Mejía, Pedro Vicente Maldonado, San Miguel de los Bancos, parte de Puerto Quito, Cayambe Quijos y El Chaco.

Todas las oficinas, centros de operación y demás estaciones de trabajo cuentan con la tecnología necesaria para la correcta ejecución de sus tareas para llevar a cabo la actividad principal de la EEQ.

PLANES

En la siguiente figura se muestra una síntesis de la implementación de ciertos planes dentro de la E.E.Q., los mismos que se encuentran detallados en la sección 1.1.5 Planes, del proyecto de titulación:

PLANES	SI TIENE		NO TIENE
	IMPLEMENTADO FORMALMENTE	NO IMPLEMENTADO FORMALMENTE	
Plan de Capacitaciones	x		
Plan de Contingencia		x	
Plan de Expansión	x		
Plan Estratégico	x		
Plan Operativo	x		
Plan de Recuperación en caso de desastres		x	
Sistema de Calidad (Certificación ISO 9000 - 2008)	x		

Figura 0.1 Síntesis de planes en la EEQ.

LINEAMIENTOS EMPRESARIALES

Los lineamientos empresariales mostrados a continuación, fueron tomados del Plan Estratégico 2012-2015 [2]:

Misión

"Proveer a Quito y al área de concesión, el servicio público de electricidad de calidad, con eficiencia, solidaridad y responsabilidad socio ambiental, contribuyendo al desarrollo del sector eléctrico y la construcción del buen vivir."

Visión

"Ser referente en el contexto nacional y regional, por la calidad y eficiencia en la prestación del servicio público de electricidad y por su aporte al desarrollo sostenible de la comunidad."

- **SITUACIÓN ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN EN LA E.E.Q.**

SITUACIÓN ACTUAL

La EEQ al ser parte de la Administración Pública del Estado Ecuatoriano, se acoge al Acuerdo No. 166 de la Secretaría Nacional de la Administración Pública, detallado en la sección 1.2.2 Situación Actual, del proyecto de titulación, y mediante Resolución de Gerencia General No. GCG-2884-2014, descrita en la misma sección, se dispone la implementación del Esquema Gubernamental de Seguridad de la Información (ESGI) en la Empresa Eléctrica Quito S.A.

EGSI

El Esquema Gubernamental de Seguridad de la Información, nació como respuesta a los avances en las Tecnologías de la Información y Comunicaciones

(TIC), y a su vez, la necesidad de los gobiernos de salvaguardar sus activos de información de la ciudadanía manejados en sus instituciones y minimizar los riesgos que puedan existir.

Está basado en la norma técnica ecuatoriana NTE-INEN ISO/IEC 27000:2009 para la Gestión de la Seguridad de la Información y está dirigido para las Instituciones de la Administración Pública Central, Dependiente e Institucional. Para una mayor descripción del EGSI, ver sección 1.2.2 Situación Actual del proyecto de Titulación EVALUACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA ELÉCTRICA QUITO UTILIZANDO LA NORMA ISO 27002.

- **ESPECIFICACIÓN DE LOS DOMINIOS DE LA NORMA ISO 27002 A UTILIZAR PARA LA EVALUACIÓN.**

Debido a la necesidad de evaluación y análisis de la situación actual de la EEQ, se decidió conjuntamente con el Oficial de Seguridad de la misma que se considerará al dominio **7. Gestión de Activos** de la norma ISO/IEC 27002:2005 como el control a evaluar en el proyecto de titulación EVALUACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA ELÉCTRICA QUITO UTILIZANDO LA NORMA ISO 27002.

Además, como complemento para la evaluación, se utilizan las directrices del EGSI respectivas a dicho dominio, así como también los Controles Críticos de Seguridad de Sans Institute (Sección 1.3.2 Especificación de dominios de la ISO 27002, directrices del EGSI y controles de CSC a utilizar para la evaluación del proyecto de titulación).

De acuerdo al dominio seleccionado para la evaluación, sus objetivos de control y controles, a las directrices prioritarias del EGSI y a las recomendaciones del Critical Security Controls, se realizó la Tabla 1 en la que se muestran los puntos a evaluar:

ISO/IEC 27002:2005			EGSI	SANS 20
Dominios	**Objetivos de Control**	**Controles**	**Controles a evaluar según EGSI**	**System Experts[46]**
7. Gestión de Activos	**7.1. Responsabilidad sobre los activos**	7.1.1. Inventario de activos	3.1.1. Inventario de activos primarios en formatos físicos y/o electrónicos 3.1.2. Inventario de activos de soporte de Hardware 3.1.3. Inventario de activos de soporte de Software 3.1.4. Inventario de activos de soporte de Redes	**CSC 1** **CSC 2**
		7.1.2. Responsable de los activos	3.2.1. Asignación de Responsables de los Activos 3.2.2. Consolidación inventarios de activos con sus responsables	**CSC 1** **CSC 2**
		7.1.3. Uso aceptable de los activos.	3.3.1. Reglamentar el uso de correo electrónico institucional 3.3.2. Reglamentar el acceso y uso de la Internet y sus aplicaciones/servicios 3.3.3. Reglamentar el uso de los sistemas de video – conferencia	**CSC 13**
	7.2. Clasificación de la información	7.2.1. Directrices de clasificación	3.4.1. Clasificar la información como pública o confidencial 3.4.2. Elaborar y aprobar un catálogo de clasificación de la información	**CSC 15**
		7.2.2. Etiquetado y manipulado de la información	3.5.1. Procedimientos de etiquetado de la información 3.5.2. Procedimientos para verificación de cumplimiento del proceso de etiquetado de información	**CSC 15** **CSC 17**

Tabla.1 Marco de evaluación para el proyecto de titulación[47]

[46] System Experts es un proveedor líder en servicios de consultoría de cumplimientos de TI y seguridad (http://systemexperts.com).
[47] Elaborado por la autora.

CAPÍTULO 2. EVALUACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE LA E.E.Q. S.A.

En este capítulo se realiza la evaluación del SGSI en la EEQ, conforme a la información recopilada durante la evaluación.

- **APLICACIÓN DE LOS DOMINIOS DE LA NORMA ISO 27002 SELECCIONADOS AL S.G.S.I. DE LA E.E.Q.**

A continuación se realiza la evaluación en base al dominio seleccionado, sus objetivos de control y controles, así como también de las directrices del EGSI y de los CSCs.

RECOLECCIÓN DE INFORMACIÓN

Debido a las normativas internas, no toda la información de la EEQ puede ser entregada en su totalidad a entes externos a la misma, por ésta razón, el proceso de recolección de información se llevó a cabo mediante entrevistas personales, así como también mediante el uso del correo electrónico y la consulta de la información publicada en la página web de la EEQ, la misma que es de carácter público.

Las entrevistas personales fueron sobre temas puntuales y se llevaron a cabo en las instalaciones de la EEQ, con el Oficial de Seguridad de la Información, y en una ocasión con el Asesor de Gerencia, con la finalidad de dar a conocer el alcance de este proyecto de titulación, y de recabar la información necesaria para llevar el cabo el análisis objetivo de dicho proyecto de titulación.

Para la recolección de información en el documento del proyecto de titulación, sección 2.1.1 Recolección de Información, se elaboraron las tablas de cumplimiento de la 2.1 a la 2.17 que incluyen una correlación entre el dominio a evaluar de la ISO/IEC 27002, es decir, el dominio 7.Gestión de Activos, y los controles de evaluación del EGSI relacionados a dicho dominio.

De la información obtenida,, se evaluaron 68 controles tomados del EGSI, en base a la norma ISO/IEC 27002, de los cuales se tuvieron los siguientes resultados:

ASPECTO DE EVALUACIÓN	NIVEL DE CUMPLIMIENTO	TOTAL
DOCUMENTACIÓN	Cumple	40
	No Cumple	16
	Cumple Parcialmente	12
IMPLEMENTACIÓN	Cumple	30
	No Cumple	25
	Cumple Parcialmente	13

Tabla. 2 Tabla de recolección de información – Totales[48]

Documentación

La EEQ cumple con un 58.82% de los controles del EGSI a nivel de documentación, es decir, cuenta con documentación formal y publicada referente a cada control. No cumple con un 23,53% de los controles y un 17,65% de dichos controles se cumplen parcialmente.

Implementación

La EEQ cumple con un 44.11% de los controles del EGSI a nivel de la implementación, es decir, tiene implementados 30 controles en las diferentes áreas y se vigila que se cumplan con los mismos. No cumple con un 36.77% de los controles y un 19,11% de dichos controles se cumplen parcialmente.

ANÁLISIS DE RESULTADOS

La evaluación que se describe a continuación, está basada en la implementación de las directrices del EGSI en la EEQ, tomando en cuenta los objetivos de control y controles de la norma ISO 27002, más no en el Sistema de Gestión de Seguridad de la Información, ya que la EEQ aún no cuenta con un sistema para la gestión de la seguridad de la información, debido a que su prioridad es implementar las directrices de acuerdo al EGSI y posterior a esto, la implantación del sistema como tal.

[48] Elaborado por la autora

En esta evaluación, se consideraron dos temas importantes, el primero corresponde a la existencia de Documentación formal sobre cada una de las directrices del EGSI, y el segundo, la Implementación de dichas directrices a nivel institucional.

Para la evaluación, se consideró la siguiente estructura:

- Dominio de evaluación seleccionado de la ISO 27002,
    - Objetivos de control del dominio seleccionado
    - Directrices de evaluación del EGSI.
    - Evaluación de CSCs por cada objetivo de control.

DOMINIO 7. GESTIÓN DE ACTIVOS (ISO/IEC 27002:2005)

Según la ISO [12] (International Organization for Standardization, en español, Organización Internacional para Estadarización), “la ISO/IEC 27002:2005 establece los lineamientos y principios generales para la iniciar, implementar, mantener y mejorar la gestión de seguridad de la información en una organización.”

Objetivo de Control 7.1. Responsabilidad sobre los activos

“Se deberían identificar los responsables para todos los activos y asignar la responsabilidad para el mantenimiento de los controles adecuados. La implementación de los controles específicos puede ser delegada por el responsable, según el caso, pero él sigue siendo responsable de la protección adecuada de los activo” [24].

Control 7.1.1. Inventario de activos

Un inventario de activos es un documento (físico o electrónico) utilizado para la recopilación de información referente a todos los bienes o servicios de una organización, también denominados activos.

Entre la información que debe contener el inventario de activos, según la NTE INEN-ISO/IEC 27002:2009, está el tipo de activo, formato, ubicación, información de soporte, información sobre licencias y el valor para el negocio.

La información contenida en este documento debe permitir a las organizaciones conocer de forma precisa, las características de cada activo y su estado actual con la finalidad de gestionar adecuadamente dichos activos para su beneficio.

Si bien es cierto, los activos tienen características en común, como por ejemplo, modelo, marca, etc., sin embargo existen otras características específicas de cada activo que se deben tomar en cuenta a la hora de elaborar un inventario de activos de una institución.

Directriz 3.1.1. Inventario de activos primarios en formatos físicos y/o electrónicos

DOCUMENTACIÓN

La EEQ tiene formalmente definido un documento denominado PLAN ESTRATÉGICO 2012–2015, el cual se encuentra publicado en la página web de la institución [1] y contiene la información referente a los procesos estratégicos, claves y de apoyo, a las normas y reglamentos, y a los planes estratégicos y operativos de la institución.

Este documento no está elaborado a manera de inventario, sino que presenta la descripción de cada activo de información con un fin informativo. A este documento se tiene libre acceso y puede ser descargado gratuitamente desde Internet.

La información generada y procesada por los funcionarios y trabajadores de la EEQ se almacena y está disponible en el sistema QUIPUX[49][22].

La información referente a manuales e instructivos de sistemas informáticos, información de la operación de los aplicativos de los servicios informáticos,

[49] QUIPUX es un Sistema de Gestión Documental adaptado a las necesidades de las empresas que pertenecen a la Administración Pública Central.

información del desarrollo y soporte de dichos aplicativos, es gestionada por la Dirección de Tecnología de la Información y Comunicaciones (DTIC), y es ésta área la encargada de hacer llegar dicha información a las personas que lo necesiten. La DTIC si tiene elaborado un inventario para los activos antes mencionados, pero este no fue provisto para su evaluación.

La imagen corporativa de la empresa, como el manual corporativo de la misma que incluye información referente a: manual de marca de la institución, logos, colores, fuentes, entre otras, es gestionada por la Dirección de Comunicación Social, y no consta en un Inventario como tal.

IMPLEMENTACIÓN

La EEQ no cuenta con un documento formal para el Inventario de los activos primarios en formatos físicos o electrónicos.

Directriz 3.1.2. Inventario de activos de soporte de Hardware

DOCUMENTACIÓN

La información de equipos móviles como tabletas, computadores portátiles, PDAs, etc; se encuentra contenida en el documento Equipos Activos de la Empresa Eléctrica [13], el cual contiene más de 5000 registros, sin considerar la información sobre teléfonos inteligentes y teléfonos celulares, la misma que a la fecha de la consulta, está pendiente de añadir a dicho documento .

El documento Equipos Activos de la Empresa Eléctrica, contiene información de equipos fijos como servidores de rack, computadores de escritorio, computadores portátiles, entre otros. Cabe mencionar que en el Inventario de Activos de Plataforma [14] descrito anteriormente, también consta la información de los servidores fijos de rack.

El Inventario de Equipos Activos de la Empresa Eléctrica contiene información sobre los periféricos de entrada (teclado, mouse, micrófono, etc.), periféricos de salida (monitor, proyector, impresora, etc.), periféricos y dispositivos de almacenamiento (discos duros externos, librerías de cintas magnéticas, etc.),

periféricos de comunicaciones (tarjetas USB para redes inalámbricas, tarjetas de red para redes alámbricas, etc.), tableros de trasferencia de energía eléctrica, de salidas de energía eléctrica, etc; e información de sistemas de control, sistemas de aire acondicionado, o de circuito cerrado de televisión. Adicionalmente, la información de los periféricos de almacenamiento como NAS o SAN[50], se encuentra también en el Inventario de Activos de Plataforma.

IMPLEMENTACIÓN

En la EEQ se tienen dos documentos formalmente definidos como Inventarios de activos de soporte de Hardware. Estos documentos son el documento de Equipos Activos de la Empresa Eléctrica [13], el cual contiene más de 5000 registros y es gestionado por el área de Control de Bienes, y el Inventario de Plataforma [14], el cual es gestionado por la DTIC. Estos inventarios no contienen la información completa de todos los activos de soporte de Hardware, por ejemplo, a la fecha de consulta, la inclusión de la información de teléfonos celulares y teléfonos celulares inteligentes se encuentra pendiente.

CRITICAL SECURITY CONTROLS

De acuerdo al documento Looking at the SANS 20 Critical Security Controls [23] publicado por System Experts, el Control Crítico de Seguridad CSC 1. Inventario de dispositivos autorizados y no autorizados, se tiene lo siguiente:

CSC1-1: Se debe implementar una herramienta automatizada para el descubrimiento de activos y con la información que ésta devuelva, elaborar un inventario de activos de los sistemas conectados a la red pública y privada de la institución.

CSC 1-2: Se debe implementar el registro de servidor de protocolo de configuración dinámica de host (DHCP), y utilizar un sistema que ayude a detectar los sistemas desconocidos conectados a la red, a través de la información del DHCP.

[50] SAN (Storage Area Network), es una red de almacenamiento que se conecta a las redes de comunicación de una organización. – NAS (Network Server Access), es un servidor de acceso a una red que trabaja como un punto de acceso que controla el acceso a un recurso protegido.

CSC 1-3: El Inventario de activos debe ser actualizado conforme se vayan realizando adquisiciones de activos en la institución.

CSC 1-4: Se debe mantener un inventario de los activos de todos los sistemas conectados a la red y de los dispositivos propios de la red, para lo cual se debe considerar agregar al inventario las siguientes características:

Característica	Descripción
Dirección de red	Dirección IP del activo
Nombre de la máquina	Nombre del activo
Propósito del sistema	Propósito del sistema al que pertenece el activo
Responsable del activo	Nombre o identificador del responsable del activo
Departamento asociado	Departamento asociado al activo
Tipo de computador	Indicar si el dispositivo es portátil o personal

Tabla. 3 Características a añadir en un inventario de activos de hardware según SANS 20. [51]

CSC 1-5: Se debe implementar el control de acceso a red (NAC) para monitorear los sistemas autorizados, con el fin de que en caso de un ataque, sea fácil detectar el sistema sospechoso y se lo traslade a una red con accesos limitados.

CSC 1-6: Se deben utilizar certificados de cliente para validar y autenticar los sistemas antes de que estos sean conectados a la red interna de la organización.

Directriz 3.1.3. Inventario de activos de soporte de Software

DOCUMENTACIÓN

El inventario de Equipos Activos de la Empresa Eléctrica [13] contiene información sobre los Sistemas Operativos en uso en la EEQ, en el Inventario

[51] Elaborado por la autora en base a los Controles Críticos de Seguridad de SANS.

de Activos de Plataforma se detallan las características de los sistemas operativos instalados en los servidores de la EEQ. Además, en la sección 9.1. Anexos, del documento Políticas para el uso y manejo de recursos informáticos de EEQ. [16], se mencionan entre otras cosas, los sistemas operativos que se utilizan en la EEQ pero no contienen una descripción de los mismos.

La información de software de servicio, mantenimiento o administración de gabinetes de servidores de cuchilla, servidores, sistemas de almacenamiento, etc; no forma parte del Inventario de Equipos Activos de la Empresa Eléctrica sino que consta en un documento denominado Procedimiento para administración de redes y comunicaciones (TI-GRC-P001) [17]. En la sección 9.1. Anexos – Listado de Software Autorizado, del documento Políticas para el uso y manejo de recursos informáticos [16] se muestra una lista de software de servicio autorizado para el uso en la EEQ, y en el Inventario de Plataforma se incluye también información al respecto en cada plataforma.

La información referente a los paquetes de software utilizados en la EEQ, como por ejemplo, software de ofimática, navegadores de internet, clientes de correo electrónico, mensajería instantánea, software de edición de imágenes, software de videoconferencia o software de servidores proxy, de correo electrónico de impresiones, etc., se encuentra contenida en el Inventario de Equipos Activos en la Empresa Eléctrica [13], así como también en el Inventario de Activos de Plataforma [14], el mismo que contiene información referente a los servidores mencionados. La información actualizada se encuentra contenida en el documento Políticas para el uso y manejo de recursos informáticos [16], sección 9.1. Anexos - Listado de Software Autorizado y por último en el Inventario de Plataforma.

La información referente a los Aplicativos del Negocio se encuentra contenida en el documento de Políticas para el uso y manejo de recursos informáticos [16], sección 9.1. Anexos - Listado de Software Autorizado (Aplicaciones desarrolladas).

IMPLEMENTACIÓN

Al igual que con los activos de soporte de hardware, los inventarios Equipos Activos de la Empresa Eléctrica [13] y el Inventario de Plataforma [14] también contienen información de los activos de soporte de software en la institución, sin embargo existen algunos sistemas que no constan en dichos inventarios y cuya descripción se encuentra en otros documentos, como Listado de Software Autorizado.

CRITICAL SECURITY CONTROLS

De acuerdo al documento Looking at the SANS 20 Critical Security Controls [23] publicado por System Experts, el Control Crítico de Seguridad CSC 2. Inventario de software autorizado y no autorizado, se tiene lo siguiente:

CSC 2-1: Se debe implementar aplicaciones tecnológicas de lista blanca, que permiten que los sistemas ejecuten software que conste en las listas blancas e impida la ejecución de software que no conste.

CSC 2-2: Se debe establecer una lista de software autorizado y su versión, que se necesita en la empresa por cada sistema de la misma. Esta lista debe ser supervisada con el fin de evitar alteraciones en el software incluido.

CSC 2-3: Se deben ejecutar búsquedas de software no autorizado y generar alertas cuando se descubra alguno. De igual forma, se deben implementar controles para la aplicación de algún cambio o instalación de nuevo software, estrictos, así como también de las versiones de software modificadas o no reconocidas.

CSC 2-4: Implementar herramientas de inventario de software en toda la organización, esta herramienta deberá almacenar, entre otras cosas, las siguientes características de cada sistema software identificado:

Característica	Descripción
Versión	Versión del sistema operativo o de la aplicación
Tipo	Tipo de software instalado
Nivel de parche	Nivel de parche instalado en el software
Responsable del activo	Nombre o identificador del responsable del activo
Departamento asociado	Departamento asociado al activo

Tabla. 4 Características a añadir en un inventario de activos de software según SANS 20. [52]

CSC 2-5: El inventario de software debe estar integrado con el inventario de hardware, de tal manera que los sistemas y su software asociado se almacenen en una sola ubicación.

Directriz 3.1.4. Inventario de activos de soporte de Redes

DOCUMENTACIÓN

Parte de la información referente a cables de comunicaciones, paneles de conexiones, tomas o puntos de red, racks, etc., está contenida en el documento de Inventarios de Activos de Plataforma [14], otra parte se encuentra de forma generalizada, en el Inventario de Equipos Activos en la Empresa Eléctrica [13] y no existe información detallada de cada uno de los cables y tampoco cuentan con codificación alguna.

La información de switches se encuentra en el Inventario de Equipos Activos en la Empresa Eléctrica [13], así como también de forma gráfica y no detallada, en el documento de Procedimiento para administración de redes y comunicaciones [17].

La información referente a ruteadores, cortafuegos, controladores de redes inalámbricas, etc., se encuentra contenida en el Inventario de Equipos Activos en la Empresa Eléctrica [13].

[52] Elaborado por la autora en base a los Controles Críticos de Seguridad de SANS.

La información referente a Sistemas de detección y prevención de intrusos (IDS/IPS), firewalls de aplicaciones web, balanceadores de carga, switches de contenido, etc., se encuentra también contenida en el Inventario de Equipos Activos en la Empresa Eléctrica [13].

IMPLEMENTACIÓN

La información referente a los activos de soporte de redes, no está completamente contemplada en los inventarios Equipos Activos de la Empresa Eléctrica [13] e Inventario de Plataforma [14]. En el caso de los cables de comunicaciones, la información se encuentra de forma generalizada, más no se cuenta con una descripción de cada cable existente.

Control 7.1.2. Responsable de los activos

Según la Norma ISO 27002, cada activo de información debe tener un propietario asignado, y cuyo nombre o identificativo debe constar en el Inventario de activos de la organización. El propietario del activo es el responsable de la confidencialidad, integridad y disponibilidad de la información del activo a su cargo.

Directriz 3.2.1. Asignación de Responsables de los activos

DOCUMENTACIÓN

En el EGSI, en esta sección se describen las tareas que debe cumplir cada responsable con el fin de mantener una protección adecuada de los activos a su cargo.

Cada responsable de uno o varios activos, debe elaborar un inventario de todos los activos a su cargo y además debe mantenerlo actualizado conforme el paso del tiempo. En la EEQ, el Inventario de Equipos Activos en la Empresa Eléctrica [13] contiene el nombre del responsable de cada uno de los activos, además, el documento Procedimiento para control de bienes [15], en la sección 4. Mantenimiento y control de activos; contiene la descripción de los

responsables (por áreas) de los diferentes tipos de activos. Dichos documentos son gestionados por diferentes áreas (Control de Bienes y la Dirección de Tecnología de la Información y Comunicaciones), más no por los responsables de cada activo.

La delegación de tareas a los responsables se definen en el documento Procedimiento para control de bienes [15], a modo de actividades a realizar para la correcta gestión de los activos, así como también en el documento Políticas para el uso y manejo de recursos informáticos [16].

En la sección 6. Políticas, del documento Políticas para el uso y manejo de recursos informáticos [16] se incluyen políticas referentes a la administración de la información dentro de los procesos de la institución a los cuales ha sido asignado cada responsable, dentro de las cuales consta la política 6.6.3***: "La información operacional relativa al hardware, software, comunicaciones y servicios de TI, es de propiedad de la DTIC"***, que indica que la información solo puede ser gestionada por la Dirección de Tecnología de la Información y Comunicaciones (DTIC). Además cabe mencionar que el documento está elaborado únicamente para salvaguardar la seguridad de la información, sistemas de información y los recursos tecnológicos Institucionales, más no de todos los activos de la EEQ.

El EGSI indica que cada responsable de los activos debe ***"Elaborar las reglas para el uso aceptable de los activos, e implantarlas previa autorización de la autoridad correspondiente"***, sin embargo en la EEQ, las reglas para el uso aceptable de los activos son desarrolladas a nivel empresarial por el área de Control de Bienes o la DTIC, más no por cada responsable, y por ende todo el personal de la EEQ debe cumplir con las mismas. Estas reglas están documentadas en documentos como el Instructivo para Control Bienes [21], y/o en el documento Políticas para el uso y manejo de recursos informáticos [16], en la sección Políticas Detalladas.

El área de Control de Bienes y la DTIC también son responsables de la clasificación, documentación y de mantener completamente actualizada la información de todos los activos existentes en la EEQ, así como también de definir los permisos de acceso a la información.

IMPLEMENTACIÓN

Los responsables de cada activo no tienen desarrollado un inventario de los activos a su cargo, el cual esté formalmente implementado. Las tareas rutinarias de cada responsable, así como las tareas de administración de la información de los procesos a los cuales ha sido asignado dicho responsable, están definidas en el documento Políticas para el uso y manejo de recursos informáticos, sin embargo estas tareas están definidas de forma global para todos los miembros de la EEQ. Son las áreas de Control de Bienes y la DTIC las encargadas de mantener actualizada la información y los activos y los permisos de acceso a la información se definen en base a las tareas operativas que cumple cada responsable, en la EEQ.

Directriz 3.2.2. Consolidación de inventarios de activos con sus responsables

DOCUMENTACIÓN

El documento Inventario de Equipos Activos en la Empresa Eléctrica [13] contiene información de los activos de la EEQ así como de sus responsables. En dicho documento, se debe ingresar por cada activo, entre otras cosas, el código del bien, una descripción del mismo, la fecha de adquisición, el número de rol de la persona responsable de dicho activo y su nombre. Los procedimientos para el registro de ésta información se encuentran contenidos en el documento Instructivo para Control Bienes [21] y en el Procedimiento para control de bienes [15].

IMPLEMENTACIÓN

No se cuenta con documentación de consolidación de inventarios de Responsables y activos a su cargo por área o unidad organizacional. Únicamente se ingresa en el Inventario de Equipos Activos de la Empresa Eléctrica, el nombre y número de rol del responsable de cada activo.

CRITICAL SECURITY CONTROLS

De acuerdo al documento Looking at the SANS 20 Critical Security Controls [23] publicado por System Experts, el Control Crítico de Seguridad CSC 1. Inventario de dispositivos autorizados y no autorizados, se tiene lo siguiente:

CSC 1-4: Se debe mantener un inventario de los activos de todos los sistemas conectados a la red y de los dispositivos propios de la red, para lo cual se debe considerar agregar al inventario el nombre o un identificativo del responsable de cada activo, así como también el departamento asociado a dicho activo (Tabla 10).

De igual forma, en el inventario de software (CSC 2), también se debe incluir el nombre el nombre o un identificativo del responsable de cada activo, así como también el departamento asociado a dicho activo.

Control 7.1.3. Uso aceptable de los activos

Los activos de una organización solo pueden ser utilizados para llevar a cabo actividades propias del negocio en beneficio de la institución, más no actividades personales del responsable del mismo.

Directriz 3.3.1. Identificar documentar e implementar las reglas sobre el uso aceptable de los activos asociados con los servicios de procesamiento de la información.

DOCUMENTACIÓN

El EGSI indica que: ***"Para la elaboración de las reglas, el Responsable del Activos deberá tomar en cuenta las actividades definidas en los controles correspondientes a los ámbitos de "Intercambio de Información" y "Control de Acceso", donde sea aplicable."***, sin embargo en la EEQ, como se mencionó anteriormente, las reglas de uso aceptable de los activos no son desarrolladas por el responsable de dichos activos, sino por las áreas de Control de Bienes y la DTIC. Estas reglas están definidas en base a los procedimientos de altas, traspasos y/o bajas de los activos o bienes, pero no se

considera la información como un bien prioritario de la EEQ. En cuanto al control de accesos, los mismos se definen en base a las necesidades de cada persona.

IMPLEMENTACIÓN

El responsable del activo no es el encargado de la definición de reglas sobre el uso aceptable de los activos. Los responsables de definirlas son las áreas de DTIC y Control de Bienes.

Directriz 3.3.2. El oficial de Seguridad de la Información es el encargado de asegurar los lineamientos para la utilización de los recursos de las Tecnologías de la Información.

DOCUMENTACIÓN

Los lineamientos para la utilización de los recursos de las Tecnologías de Información, antes de la contratación del personal para Oficial de Seguridad, eran gestionados por la DTIC, y se los definían en base a las necesidades de cada área de trabajo.

IMPLEMENTACIÓN

Los lineamientos para la utilización de los recursos de las Tecnologías de Información, antes de la contratación del personal para Oficial de Seguridad, eran gestionados por la DTIC, y se los definían en base a las necesidades de cada área de trabajo.

Directriz 3.3.3. La información y documentos generados en la institución y enviados por cualquier medio o herramienta electrónica con propiedad de la información que procesan.

IMPLEMENTACIÓN Y DOCUMENTACIÓN

La información generada y procesada por los funcionarios y trabajadores de la EEQ se almacena y está disponible en el sistema QUIPUX [22].

Directriz 3.3.4. Reglamentar el uso de correo electrónico institucional

DOCUMENTACIÓN

El EGSI indica que el correo electrónico institucional debe ser utilizado únicamente para realizar tareas que le permitan al usuario, cumplir con sus funciones laborales que demande la compañía. En la EEQ, en la sección 6.4 Correo Electrónico del documento Políticas para uso y manejo de recursos informáticos [16], se establecen políticas para el uso del correo institucional.

Dentro de la EEQ, existe un documento denominado Procedimiento administración de servicios Internet y Correo [19], el cual contiene procedimientos y políticas para la creación de cuentas de correo electrónico al personal de la organización, que así lo requiera. De igual forma contiene políticas de creación de contraseñas, en cuanto a estructura; procedimientos para solicitudes de acceso a Internet o correo electrónico; procedimientos para acceso a Internet en el firewall de la EEQ. Cada vez que se crea una cuenta de correo electrónico, siendo responsable de dicha actividad la DTIC, se le notifica al usuario que debe hacer uso de su cuenta en base a las políticas para uso y manejo de recursos informáticos [16].

El documento Procedimiento administración de servicios Internet y Correo [19], incluye como anexo, un acta de compromiso para el buen uso del servicio de Internet de la EEQ, la misma que debe ser firmada por cada usuario del correo institucional y/o Internet de la institución la primera vez que solicita acceso a cualquiera de los servicios antes descritos.

El acta de compromiso para el buen uso del servicio de Internet de la EEQ contiene las condiciones que debe cumplir el personal para utilizar los servicios de Internet de la EEQ, aceptando que el uso de dicho servicio deberá ser únicamente para fines de cumplimiento laboral e indicar si necesita tener acceso a sitios específicos con fines de consulta y/o investigación para beneficio de la institución.

Los correos y/o mensajes transmitidos por medio del correo electrónico institucional o por medio de Internet, no son monitoreados ni conservados permanentemente por parte de la EEQ.

Cada cuenta de correo electrónico perteneciente al correo electrónico institucional está asociada a una única cuenta de usuario según el número de rol asignado por el área de Recursos Humanos, y en caso de usuarios a contrato sin rol, en base a su nombre y apellido.

La información de los buzones de correo es gestionada por cada usuario en su estación de trabajo, más no de forma centralizada como indica el EGSI. Cada usuario es responsable de la eliminación de mensajes máximo cada 15 días con el fin de optimizar el tamaño de su bandeja de correos, así como también de respaldar la información que así lo requiera, en una unidad asignada para dicho fin.

No se cuenta con facilidades automáticas que notifiquen al usuario cuando un correo enviado por él, no es recibido correctamente por el destinatario, y que indiquen detalladamente el motivo del error.

Para el monitoreo de virus informáticos, tanto en correos o en archivos adjuntos, se utiliza un Software de Antivirus de Plataforma Integral, y se prohíbe al personal, la reproducción maliciosa o voluntaria de virus informáticos, o de mensajes con contenido ofensivo, ilegal, pornográfico o de cualquier otro tipo no autorizado que dañe la imagen de la institución.

Cada usuario es responsable de la información que reciba, por lo tanto, en caso de identificar un mensaje de origen desconocido, debe destruirlo y asumir la responsabilidad de las consecuencias que pueda ocasionar la apertura o ejecución de dicho mensaje. Además, debe notificar al Oficial de Seguridad de la Información de la presencia de dicha amenaza, con el fin de que sea analizado y se tomen las medidas preventivas o correctivas necesarias. Este procedimiento está descrito en el acta de compromiso para el buen uso del servicio de Internet de la EEQ.

Para la transmisión de información en la EEQ se utiliza HTTPS, que permite transmitir información cifrada por medio del canal. No se mantiene información conservada referente al uso de correo electrónico y/o servicio de internet.

Las cuentas de correo electrónico institucional, son creadas de tal forma que se limite el tamaño de los mensajes, así como también el envío masivo de los mismos. Cabe señalar que cada usuario es responsable de la cantidad y tamaño de los mensajes que se envíen desde su cuenta de correo.

IMPLEMENTACIÓN

En el documento Procedimiento Administración de Servicios Internet y Correo (TI-GBD-P004), se definen políticas y procedimientos para el uso aceptable de servicios de Internet y Correo Electrónico, en donde se indica que dichos servicios deben ser utilizados únicamente para tareas propias de la organización.

No se monitorea la información en el sistema de correo electrónico, ni tampoco es almacenada sino en cada equipo en el caso del correo electrónico, en su bandeja de correo.

Directriz 3.3.5. Reglamentar el acceso y uso de la Internet y sus aplicaciones/servicios

DOCUMENTACIÓN

Los procedimientos para el acceso y uso de Internet, así como de sus aplicaciones y servicios están incluidos en el documento Procedimiento para administración de seguridades y accesos [20], dentro del cual se incluyen políticas y procedimientos para el acceso a las aplicaciones y herramientas de la EEQ que requieren autenticación, procedimientos para control de claves para aplicaciones y herramientas de la EEQ que requieran autenticación (a excepción del sistema Sidecom); procedimientos para los usuarios del sistema Sidecom; entre otras.

En la sección 6.3 Seguridad Informática, del documento Políticas para uso y manejo de recursos informáticos [16], se establecen políticas para el acceso a los sistemas informáticos en la institución. Cada usuario es responsable de respetar la integridad de los sistemas de computación a los cuales tenga acceso, así como también de las contraseñas que se utilizan para dichos accesos. La Administración de la EEQ tiene el derecho de vigilar y auditar los sistemas de correo electrónico y todos los sistemas computarizados con el fin de garantizar que los usuarios utilicen dichos servicios con fines netamente laborales, en función de las actividades que realice en la EEQ. Estas auditorías se realizan de forma periódica o al azar, según las necesidades de la institución. Además, cada usuario deberá guardar la información que requiera ser almacenada, en los directorios asignados a cada usuario, con el fin de protegerlos mediante mecanismos de respaldos.

Cada una de las personas que laboran en la EEQ y que requieran acceso a algún servicio de Internet, deberán llenar el acta de compromiso para el buen uso del servicio de Internet de la EEQ, indicando las razones por las cuales requiere los servicios informáticos. Además, en la red de la EEQ, se limita el acceso a portales, servicios o sitios web que puedan dañar la imagen de la institución, para lo cual se bloquea el acceso a sitios con contenidos de índole maliciosa. En la sección 9. Anexos, del documento Políticas para uso y manejo de recursos informáticos [16], se presenta el estado de software autorizado al cual pueden tener acceso cada miembro de la EEQ.

En la EEQ, para cada tipo de información se designa un custodio, cuya objetivo será proteger la información de la institución, , tomando en cuenta la criticidad de la información. Los custodios de la información son responsables de definir procedimientos de control específicos, administrar el control de acceso a la información, y suministrar capacidades de recuperación, en concordancia con las instrucciones de los dueños/propietarios de los datos. El Oficial de Seguridad de la Información forma parte de los custodios de la información, el mismo que puede solicitar la información de monitoreo de los contenidos a los que acceden los usuarios, bajo demanda para posteriormente revisarla y/o analizarla para la solución de requerimientos.

Se prohíbe el uso de la computadora o del sistema de correspondencia electrónica para enviar, recibir, crear o divulgar mensajes o documentos de contenido discriminatorio por razones de raza, género, credo, origen nacional, sexo, orientación sexual, edad, ideas políticas u origen social o nacional, o que puedan ser catalogados como hostigamiento sexual.

En la EEQ se utiliza un PROXY, el cual permite un mayor control de los sitios a los que se tiene acceso desde Internet, y cuando sea conveniente, se limitará o bloqueará el acceso a sitios que se consideren una amenaza para la institución.

El correo institucional es un servicio de correo electrónico de libre uso, GMAIL adquirido en base a lo establecido en el EGSI (el cual indica que todas las disposiciones deben basarse en una gestión de riesgos).

La EEQ hace uso de servicios en la nube, para lo cual existe un acuerdo de uso de servicios en la nube, basado en el EGSI (todas las disposiciones deben basarse en una gestión de riesgos).

IMPLEMENTACIÓN

El documento Procedimiento Administración de Servicios Internet y Correo (TI-GBD-P004), contiene como anexo un acta de compromiso para el buen uso del servicio de Internet de la EEQ, en donde se le indica a cada usuario que es responsable del tráfico de información que genere.

Directriz 3.3.6. Reglamentar el uso de los sistemas de video – conferencia

DOCUMENTACIÓN

Durante la recaudación de la información, no se contaba con la definición de responsables para la administración de los sistemas de video conferencia, sin embargo el Oficial de Seguridad indicó que la información estaba pendiente de ser incluida en el documento Políticas para uso y manejo de recursos informáticos [16].

La EEQ cuenta únicamente con un ambiente de producción de los sistemas de video conferencia, no existe un ambiente de pruebas. La institución cuenta con un video instructivo para la administración del sistema de video conferencia, el cual a la fecha de la consulta, se encontraba en estado de revisión y no ha sido publicado formalmente. En dicho video instructivo, se definen los procedimientos para el acceso y uso del sistema de video conferencia en el ambiente de producción, antes mencionado.

El video instructivo contiene una descripción de las actividades que se deben ejecutar para la administración del sistema de video conferencia, más no se cuenta con un la lista de chequeo que sugiere el EGSI que debe contener los parámetros de seguridad que se deben cumplir para el correcto acceso a la red que soporta el servicio de video conferencia.

Al momento de la recaudación de la información, la inclusión de las políticas para creación de usuarios y contraseñas para el ingreso a la configuración de los equipos y salas virtuales de video conferencia, en el documento Políticas para uso y manejo de recursos informáticos [16] se encontraba. También se encontraba pendiente, la inclusión de políticas para deshabilitar las respuestas automáticas de los equipos de video conferencia de la institución.

IMPLEMENTACIÓN

No se han definido responsables para la administración de los sistemas de video conferencia, no existe un ambiente de pruebas, se cuenta con un ambiente de producción para cuyo acceso, se han definido procedimientos en el Video Instructivo, el cual estaba pendiente de publicación a la fecha de consulta.

No se cuenta con un documento en donde se definan los parámetros de seguridad para el acceso a la red interministerial que soporta el servicio de video-conferencia, y no se hace uso de contraseñas para el acceso a estos sistemas. La respuesta automática de los sistemas de videoconferencia, no está desactivada.

CRITICAL SECURITY CONTROLS

De acuerdo al documento Looking at the SANS 20 Critical Security Controls [23] publicado por System Experts, el Control Crítico de Seguridad CSC 13. Límites de Defensa se tiene lo siguiente:

Para asegurar el uso aceptable de los activos de la institución, es necesaria la aplicación de controles para denegar el acceso a direcciones IP identificadas como maliciosas, o limitar el acceso sólo a sitios de confianza.

Se debe monitorear el tráfico de la red, así como la información que viaja por ella, con la finalidad de determinar si se hace uso de la red para fines que no sean de la institución.

Objetivo de Control 7.2. Clasificación de la Información

Control 7.2.1. Directrices de Clasificación

Como se ha indicado anteriormente, la información es uno de los activos más importantes de las compañías hoy en día, por esta razón, es indispensable que en cada institución se implementen políticas y/o procedimientos para su control y manejo, como por ejemplo, procedimientos para la identificación y clasificación de los activos de información en la compañía, según su criticidad.

La información puede ser clasificada en dos grupos: Información Pública, es decir información a la que se puede tener libre acceso; e Información confidencial, a la cual el acceso se debe restringir. En ambos casos, el acceso a la información debe ser controlado y se debe establecer políticas para su entrega o difusión.

Directriz 3.4.1. Clasificación de la información como pública o confidencial.

DOCUMENTACIÓN

La EEQ cuenta con un documento denominado Listado de Activos de Información, el cual contiene la descripción de 251 activos con sus responsables. De estos 251 activos identificados en dicho documento, 54 son considerados como activos críticos y se incluye un perfil del responsable en donde termina el trato de la información. Contiene además, una clasificación de los activos de información, en función de su disponibilidad, confidencialidad e integridad de acuerdo a la LOTAIP[53] que rige a las empresas de Administración Pública como la EEQ. El documento fue provisto por el Oficial de Seguridad por motivos internos, sin embargo el Oficial de Seguridad brindó información sobre dicho documento.

IMPLEMENTACIÓN

Información contenida en el Listado de Activos de Información, el cual contiene 251 activos con sus responsables, de éstos, 54 son considerados como activos críticos e incluye un perfil del responsable en donde termina el trato de la información (Contiene además, una clasificación de los activos de información, en función de su disponibilidad, confidencialidad e integridad de acuerdo a la LOTAIP).

Directriz 3.4.2. Elaborar y aprobar un catálogo de clasificación de la información. Se la deberá clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la institución. El nivel de protección se puede evaluar analizando la confidencialidad, la integridad y la disponibilidad.

DOCUMENTACIÓN E IMPLEMENTACIÓN

[53] LOTAIP (Ley Orgánica de Transparencia y Acceso a la Información Pública), es una ley en estado vigente, publicada en el Registro Oficial Suplemento 337 de 18 de mayo de 2004, que garantiza el derecho a acceder a las fuentes de información públicas.

La EEQ dispone de un procedimiento de Clasificación de Información que se encuentra en revisión para aprobación, en consecuencia no puede ser entregado aún; además, se dispone del listado de activos de información de la EEQ clasificados en función de su disponibilidad, confidencialidad en integridad, el cual no puede ser entregado aún por motivos internos. Sin embargo para este caso en particular, se puede visitar la página Web www.eeq.com.ec, donde se encuentra la información acorde a la LOTAIP.

CRITICAL SECURITY CONTROLS

De acuerdo al documento Looking at the SANS 20 Critical Security Controls [23] publicado por System Experts, el Control Crítico de Seguridad CSC 15. Acceso controlado en base a la necesidad de conocer, se tiene lo siguiente:

CSC 15-1: Localizar la información sensible y encriptar todo tipo de comunicación en la que se la utilice.

CSC 15-2: Se debe controlar el cumplimiento del registro de auditoría para el acceso a datos no públicos y se debe implementar una autenticación especial para datos sensibles.

CSC 15-3: Se debe segmentar la red basándose en los niveles de confianza de la información almacenada en los servidores. Si el nivel de confianza de una red es bajo, la información debe ser encriptada.

CSC 15-4: Controlar el acceso a los datos mediante las ACLs (Listas de control de acceso) implementadas en cada servidor.

Control 7.2.1. Etiquetado y manipulado de la información

Toda la información que se manipule dentro de una organización, debe ser correctamente etiquetada.

En la EEQ, se dispone de un Procedimiento de Clasificación de Información que se encuentra en revisión para aprobación, en consecuencia no puede ser entregado aún. Además, se dispone del listado de activos de información de la EEQ clasificados en función de su disponibilidad, confidencialidad e integridad,

el cual no fue entregado aún por motivos internos. Sin embargo para este caso en particular, visitar la página web de la EEQ [1], donde se encuentra información publicada acorde a lo establecido en la LOTAIP.

Directriz 3.5.1. Incluir datos mediante abreviaturas, acerca del tipo de activo y su funcionalidad para la generación de etiquetas.

DOCUMENTACIÓN

En el documento Listado de Activos de Información, cada uno de los activos contenidos se encuentra etiquetado formalmente en base al área en la que es administrado y a un secuencial asignado por el área DTIC.

IMPLEMENTACIÓN

Información contenida en el Listado de activos de información de la EEQ, en el que se etiqueta a cada activo, según el área y un secuencial.

Directriz 3.5.2. En caso de repetición de la etiqueta del activo, deberá añadirse un número secuencial único al final.

DOCUMENTACIÓN E IMPLEMENTACIÓN

Las etiquetas de los activos contenidos en el documento Listado de Activos de Información incluyen un secuencial para su diferenciación.

Directriz 3.5.3. En caso de documentos en formato electrónico, la etiqueta deberá asociarse a un metadato único, pudiendo ser éste un código MD5.

DOCUMENTACIÓN E IMPLEMENTACIÓN

Los activos de información en formato electrónico no están asociados a un metadato único.

Directriz 3.5.4. Las etiquetas generadas deberán estar incluidas en el inventario, asociadas a su respectivo activo.

DOCUMENTACIÓN E IMPLEMENTACIÓN

Las etiquetas de los activos de información están incluidas en el documento de Listado de Activos de Información.

Directriz 3.5.5. Los responsables de los activos deberán supervisar el cumplimiento del proceso de generación de etiquetas y rotulación de los activos.

DOCUMENTACIÓN E IMPLEMENTACIÓN

Los responsables de los activos de la información no son los responsables de la supervisión de cumplimiento del proceso de generación de etiquetas y rotulación de activos, el área responsable es el área DTIC.

Directriz 3.5.6. Para el caso de etiquetas físicas, los responsables de los activos verificarán con una periocidad no mayor a 6 meses, que los activos se encuentren rotulados y con etiquetas legibles.

DOCUMENTACIÓN E IMPLEMENTACIÓN

Los responsables de los activos no se encargan de la verificación de que los activos se encuentren rotulados y con etiquetas legibles, estos procesos se están empezando a implementar en la EEQ. La rotulación de los activos lo realiza el área de Control de Bienes mediante la asignación de un código único de barras.

Directriz 3.5.7. En caso de destrucción de un activo, la etiqueta asociada a éste debe mantenerse en el inventario respectivo con los registros de las acciones realizadas.

DOCUMENTACIÓN E IMPLEMETACIÓN

Los responsables de los activos no verifican que los activos estén rotulados y con etiquetas legibles, esto lo realiza el área de Control de Bienes.

CRITICAL SECURITY CONTROLS

De acuerdo al documento Looking at the SANS 20 Critical Security Controls [23] publicado por System Experts, el Control Crítico de Seguridad CSC 15. Acceso controlado en base a la necesidad de conocer, se tiene lo siguiente:

CSC 15-1: Localizar la información sensible y encriptar todo tipo de comunicación en la que se la utilice.

CSC 15-2: Se debe controlar el cumplimiento del registro de auditoría para el acceso a datos no públicos y se debe implementar una autenticación especial para datos sensibles.

CSC 15-3: Se debe segmentar la red basándose en los niveles de confianza de la información almacenada en los servidores. Si el nivel de confianza de una red es bajo, la información debe ser encriptada.

CSC 15-4: Controlar el acceso a los datos mediante las ACLs (Listas de control de acceso) implementadas en cada servidor.

Por otro lado, con respecto al CSC 17. Protección de datos, se tiene lo siguiente.

CSC 17-1: Implementar software para el cifrado de la información sensible en los discos duros de dispositivos específicos.

CSC 17-2: Verificar que los dispositivos criptográficos y de software estén configurados para utilizar algoritmos examinados públicamente.

CSC 17-3: Realizar una evaluación de los datos para identificar la información confidencial que exige la aplicación de controles de encriptación e integridad.

CSC 17-4: Implementar herramientas automatizadas para identificar intentos de acceso no autorizado a los sistemas que contienen información sensible.

CSC 17-5: Llevar a cabo análisis periódicos de la información sensible almacenada de forma cifrada, con el fin de identificar cambios no autorizados en la misma.

RESULTADOS FINALES

A continuación se muestra el análisis de la información recopilada:

Declaración de Aplicabilidad

Debido a la necesidad de evaluación de los niveles de cumplimiento de los objetivos de control y controles del dominio 7. Gestión de Activos en la EEQ, se considera para la evaluación, al EGSI y sus respectivas directrices como la Declaración de Aplicabilidad a utilizar para el análisis de la información recopilada.

Criterios de evaluación de los niveles de cumplimiento

Para la evaluación de los niveles de cumplimiento de los objetivos de control y controles seleccionados, se elaboró la tabla 5 que contiene los criterios de evaluación en base a un porcentaje de cumplimiento que oscila desde el 0% al 100%:

Criterio	Descripción	Simbología
Total	Indica que la directriz evaluada tiene un nivel de cumplimiento del 71 al 100%.	T
Parcial	Indica que la directriz evaluada tiene un nivel de cumplimiento del 31 al 70%.	P
Nulo	Indica que la directriz evaluada tiene un nivel de cumplimiento del 0 al 30%.	N

Tabla 5 Tabla de criterios de evaluación. [54]

[54] Elaborado por la autora.

Matriz de criterios de evaluación

Para el cálculo de los criterios de evaluación, se elaboró la matriz de criterios de evaluación mostrada en la tabla 6:

Matriz de Criterios de Evaluación	
T / T	T
T / P	P
T / N	P
P / P	P
P / N	P
N / N	N

Tabla 6 Matriz de criterios de evaluación. [55]

Resumen del proceso de evaluación

Para el análisis de los datos recopilados, se desarrolló el proceso descrito a continuación:

Utilizando la plantilla de medición de seguridad de la información del Anexo A de la NTE INEN ISO/IEC 27004:2012, se elaboraron las tablas de medición mostradas en las tablas de la 7 a la 12.

En base a los criterios de evaluación establecidos en la tabla 7, se evalúo el nivel de cumplimiento de cada directriz del EGSI tal como se muestra en la tabla 12 considerando que, como parte de la recolección de información, se tomaron en cuenta dos ámbitos de evaluación, la Documentación y la Implementación.

A continuación, utilizando la matriz de criterios de evaluación de la tabla 6, se obtuvo el nivel de cumplimiento general de cada una de las directrices del EGSI, obteniéndose así el Indicador de cumplimiento por Directriz (EGSI).

Finalmente, utilizando la matriz de criterios de evaluación de la tabla 6, se obtuvo el indicador de cumplimiento por cada uno de los controles de la norma ISO/IEC 27002, obteniéndose así el Indicador de cumplimiento por Control (ISO / IEC 27002), tal como se muestra en la tabla 12.

[55] Elaborado por la autora.

Medición de la Seguridad de la Información

Para el desarrollo de la medición se utilizó la Plantilla para construcción de la medición de la seguridad de la información, descrita en el Anexo A de la NTE INEN ISO/IEC 27004:2012 [25] y se elaboraron las siguientes tablas (de la Tabla 2.32 a la 2.36), para cada uno de los objetivos de control del dominio 7. Gestión de Activos:

7.1 Responsabilidad sobre los activos	
7.1.1. Inventario de activos	
Identificación de la construcción de la medición	
Nombre de la construcción de la medición	Evaluación del desarrollo de Inventario de activos
Identificador numérico	Específico de la Organización
Propósito de la construcción de la medición	Evaluar el cumplimiento de la política sobre la elaboración del Inventario de activos
Objetivo Control/Proceso	7.1. Responsabilidad sobre los activos
Control (1)/proceso (1)	7.1.1. Inventario de activos
Objeto de la Medición y Atributos	
Objeto de Medición	Inventario de activos
Atributos	Inventario de activos primarios en formatos físicos y/o electrónicos. Inventario de activos de soporte de hardware. Inventario de activos de soporte de software. Inventario de activos de soporte de redes.
Especificación Medida Base (1)	
Medida Base	Nivel de cumplimiento del inventario de activos primarios en formatos físicos y/o electrónicos. Nivel de cumplimiento del inventario de activos de soporte de hardware. Nivel de cumplimiento del inventario de activos de soporte de software. Nivel de cumplimiento del inventario de activos de soporte de redes.
Método de Medición	Ponderar el cumplimiento de la elaboración del inventario de activos.
Tipo de Método de Medición	Subjetivo
Escala	Niveles de cumplimiento: Total (T): Cumplimiento del 71% al 100% Parcial (P): Cumplimiento del 31 al 70% Nulo (N): Cumplimiento del 0 al 305
Tipo de Escala	Relación
Unidad de Medición	Personal Porcentaje
Especificación Medida Derivada	
Medida Derivada	Progreso a la fecha

Función de Medición	Calificación del cumplimiento de la norma, en base a los niveles de cumplimiento de cada control.
Especificación del Indicador	
Indicador	Relación de la cantidad de activos que forman parte del inventario.
Modelo Analítico	Obtener los niveles de cumplimiento de cada control, en base a los niveles de cumplimiento de cada directriz del EGSI.
Especificación Criterios de Decisión	
Criterios de decisión	El objetivo de control se cumple de forma satisfactoria cuando se cumple cuando el nivel de cumplimiento es mayor o igual a 71%, se cumple parcialmente cuando el nivel de cumplimiento va del 31 al 70%, y no se cumple cuando el nivel de cumplimiento es menor o igual al 30%, y es una oportunidad de mejora.
Resultados de la medición	
Interpretación del Indicador	La interpretación del indicador es: - La elaboración del inventario se cumple satisfactoriamente cuando el nivel de cumplimiento es mayor o igual al 71%. - La elaboración del inventario se cumple parcialmente cuando el nivel de cumplimiento varía entre el 31 al 70%, y tiene tendencia a mejorar. - La elaboración del inventario no se cumple cuando el nivel de cumplimiento es menor o igual al 30%, y será considerada como una oportunidad de mejora.
Formatos de Reporte	Tablas de cumplimiento (Tablas de la 2.1 a la 2.6 del proyecto de titulación)
Interesados	
Cliente para medición	Personal de la EEQ
Supervisor de medición	Oficial de Seguridad de la Información
Propietario de la Información	EEQ
Recolector de la Información	Autora del proyecto de titulación
Comunicador de Información	Autora del proyecto de titulación
Frecuencia/Período	
Frecuencia de Recolección de Datos	Una vez
Frecuencia de Análisis de Datos	Una vez
Frecuencia del Reporte de Resultados de Medición	Una vez
Revisión de la Medición	Una vez
Período de Medición	Una vez

Tabla 7 Medición de cumplimiento – 7.1.1. Inventario de activos

7.1 Responsabilidad sobre los activos	
7.1.2. Responsable de los activos	
Identificación de la construcción de la medición	
Nombre de la construcción de la medición	Asignación de Responsable de los activos
Identificador numérico	Específico de la Organización
Propósito de la construcción de la medición	Evaluar el cumplimiento de la política sobre el Responsable de los activos
Objetivo Control/Proceso	7.1. Responsabilidad sobre los activos
Control (1)/proceso (1)	7.1.2. Responsable de los activos
Objeto de la Medición y Atributos	
Objeto de Medición	Responsable de los activos
Atributo	Asignación de Responsables de los activos Consolidación de inventarios de activos con sus responsables
Especificación Medida Base (1)	
Medida Base	Nivel de cumplimiento de la asignación de responsables de los activos. Nivel de cumplimiento de la consolidación de inventarios de activos con sus responsables.
Método de Medición	Ponderar el cumplimiento de la política de Responsables de los activos
Tipo de Método de Medición	Subjetivo
Escala	Niveles de cumplimiento: Total (T): Cumplimiento del 71% al 100% Parcial (P): Cumplimiento del 31 al 70% Nulo (N): Cumplimiento del 0 al 305
Tipo de Escala	Relación
Unidad de Medición	Personal Porcentaje
Especificación Medida Derivada	
Medida Derivada	Progreso a la fecha
Función de Medición	Calificación del cumplimiento de la norma, en base a los niveles de cumplimiento de cada control.
Especificación del Indicador	
Indicador	Cantidad de activos asignados a un responsable. Porcentaje de consolidación de inventarios de activos con sus responsables.
Modelo Analítico	Obtener los niveles de cumplimiento de cada control, en base a los niveles de cumplimiento de cada directriz del EGSI.

Especificación Criterios de Decisión	
Criterios de decisión	El objetivo de control se cumple de forma satisfactoria cuando se cumple cuando el nivel de cumplimiento es mayor o igual a 71%, se cumple parcialmente cuando el nivel de cumplimiento va del 31 al 70%, y no se cumple cuando el nivel de cumplimiento es menor o igual al 30%, y es una oportunidad de mejora.
Resultados de la medición	
Interpretación del Indicador	La interpretación del indicador es: - La elaboración del inventario se cumple satisfactoriamente cuando el nivel de cumplimiento es mayor o igual al 71%. - La elaboración del inventario se cumple parcialmente cuando el nivel de cumplimiento varía entre el 31 al 70%, y tiene tendencia a mejorar. - La elaboración del inventario no se cumple cuando el nivel de cumplimiento es menor o igual al 30%, y será considerada como una oportunidad de mejora.
Formatos de Reporte	Tablas de cumplimiento (Tablas de la 2.7 a la 2.8 del proyecto de titulación)
Interesados	
Cliente para medición	Personal de la EEQ
Supervisor de medición	Oficial de Seguridad de la Información
Propietario de la Información	EEQ
Recolector de la Información	Autora del proyecto de titulación
Comunicador de Información	Autora del proyecto de titulación
Frecuencia/Período	
Frecuencia de Recolección de Datos	Una vez
Frecuencia de Análisis de Datos	Una vez
Frecuencia del Reporte de Resultados de Medición	Una vez
Revisión de la Medición	Una vez
Período de Medición	Una vez

Tabla 8 Medición de la seguridad de la información - 7.1.2. Responsable de los activos

7.1 Responsabilidad sobre los activos	
7.1.3. Uso aceptable de los activos	
Identificación de la construcción de la medición	
Nombre de la construcción de la medición	Uso aceptable de los activos
Identificador numérico	Específico de la Organización
Propósito de la construcción de la medición	Evaluar el cumplimiento de la política sobre el Uso aceptable de los activos
Objetivo Control/Proceso	7.1. Responsabilidad sobre los activos
Control (1)/proceso (1)	7.1.3. Uso aceptable de los activos
Objeto de la Medición y Atributos	
Objeto de Medición	Uso aceptable de los activos
Atributo	Reglamentar el uso de correo electrónico institucional. Reglamentar el acceso y uso de la Internet y sus aplicaciones/servicios. Reglamentar el uso de los sistemas de video-conferencia.
Especificación Medida Base (1)	
Medida Base	Nivel de cumplimiento de la reglamentación del uso de correo electrónico institucional. Nivel de cumplimiento de la reglamentación del acceso y uso de la Internet y sus aplicaciones/servicios. Nivel de cumplimiento de la reglamentación del uso de los sistemas de video-conferencia.
Método de Medición	Ponderar el cumplimiento de la política de Uso aceptable de los activos.
Tipo de Método de Medición	Subjetivo
Escala	Niveles de cumplimiento: Total (T): Cumplimiento del 71% al 100% Parcial (P): Cumplimiento del 31 al 70% Nulo (N): Cumplimiento del 0 al 305
Tipo de Escala	Relación
Unidad de Medición	Personal Porcentaje
Especificación Medida Derivada	
Medida Derivada	Progreso a la fecha
Función de Medición	Calificación del cumplimiento de la norma, en base a los niveles de cumplimiento de cada control.

Especificación del Indicador	
Indicador	Existencia de políticas y/o procedimientos para el uso de correo electrónico institucional. Existencia de políticas y/o procedimientos para el acceso y uso de la Internet y sus aplicaciones/servicios. Existencia de políticas y/o procedimientos para el uso de los sistemas de video-conferencia.
Modelo Analítico	Obtener los niveles de cumplimiento de cada control, en base a los niveles de cumplimiento de cada directriz del EGSI.
Especificación Criterios de Decisión	
Criterios de decisión	El objetivo de control se cumple de forma satisfactoria cuando se cumple cuando el nivel de cumplimiento es mayor o igual a 71%, se cumple parcialmente cuando el nivel de cumplimiento va del 31 al 70%, y no se cumple cuando el nivel de cumplimiento es menor o igual al 30%, y es una oportunidad de mejora.
Resultados de la medición	
Interpretación del Indicador	La interpretación del indicador es: - La elaboración del inventario se cumple satisfactoriamente cuando el nivel de cumplimiento es mayor o igual al 71%. - La elaboración del inventario se cumple parcialmente cuando el nivel de cumplimiento varía entre el 31 al 70%, y tiene tendencia a mejorar. - La elaboración del inventario no se cumple cuando el nivel de cumplimiento es menor o igual al 30%, y será considerada como una oportunidad de mejora.
Formatos de Reporte	Tablas de cumplimiento (Tablas de la 2.9 a la 2.15 del proyecto de titulación)
Interesados	
Cliente para medición	Personal de la EEQ
Supervisor de medición	Oficial de Seguridad de la Información
Propietario de la Información	EEQ
Recolector de la Información	Autora del proyecto de titulación
Comunicador de Información	Autora del proyecto de titulación
Frecuencia/Período	
Frecuencia de Recolección de Datos	Una vez
Frecuencia de Análisis de Datos	Una vez
Frecuencia del Reporte de Resultados de Medición	Una vez
Revisión de la Medición	Una vez
Período de Medición	Una vez

Tabla 9 Medición de la Seguridad de la Información – 7.1.3. Uso aceptable de los activos

7.2. Clasificación de la información	
7.2.1. Directrices de clasificación	
Identificación de la construcción de la medición	
Nombre de la construcción de la medición	Directrices de clasificación de la información
Identificador numérico	Específico de la Organización
Propósito de la construcción de la medición	Evaluar el cumplimiento de la política sobre las Directrices de clasificación
Objetivo Control/Proceso	7.2. Clasificación de la información
Control (1)/proceso (1)	7.2.1. Directrices de clasificación
Objeto de la Medición y Atributos	
Objeto de Medición	Directrices de clasificación de la información
Atributos	Clasificación de la información como pública o confidencial. Elaboración y aprobación de un catálogo de clasificación de la información.
Especificación Medida Base (1)	
Medida Base	Nivel de cumplimiento de la clasificación de la información como pública o confidencial. Nivel de cumplimiento de la elaboración y aprobación de un catálogo de clasificación de la información.
Método de Medición	Ponderar el cumplimiento de la creación de directrices de clasificación de la información.
Tipo de Método de Medición	Subjetivo
Escala	Niveles de cumplimiento: Total (T): Cumplimiento del 71% al 100% Parcial (P): Cumplimiento del 31 al 70% Nulo (N): Cumplimiento del 0 al 305
Tipo de Escala	Relación
Unidad de Medición	Personal Porcentaje
Especificación Medida Derivada	
Medida Derivada	Progreso a la fecha
Función de Medición	Calificación del cumplimiento de la norma, en base a los niveles de cumplimiento de la cada control.
Especificación del Indicador	
Indicador	Relación de la cantidad de información clasificada como pública o confidencial. Elaboración y aprobación de un catálogo de clasificación de la información.
Modelo Analítico	Obtener los niveles de cumplimiento de cada control, en base a los niveles de cumplimiento de cada directriz del EGSI.

Especificación Criterios de Decisión	
Criterios de decisión	El objetivo de control se cumple de forma satisfactoria cuando se cumple cuando el nivel de cumplimiento es mayor o igual a 71%, se cumple parcialmente cuando el nivel de cumplimiento va del 31 al 70%, y no se cumple cuando el nivel de cumplimiento es menor o igual al 30%, y es una oportunidad de mejora.
Resultados de la medición	
Interpretación del Indicador	La interpretación del indicador es: - La elaboración del inventario se cumple satisfactoriamente cuando el nivel de cumplimiento es mayor o igual al 71%. - La elaboración del inventario se cumple parcialmente cuando el nivel de cumplimiento varía entre el 31 al 70%, y tiene tendencia a mejorar. - La elaboración del inventario no se cumple cuando el nivel de cumplimiento es menor o igual al 30%, y será considerada como una oportunidad de mejora.
Formatos de Reporte	Tablas de cumplimiento (Tabla 2.16 del proyecto de titulación)
Interesados	
Cliente para medición	Personal de la EEQ
Supervisor de medición	Oficial de Seguridad de la Información
Propietario de la Información	EEQ
Recolector de la Información	Autora del proyecto de titulación
Comunicador de Información	Autora del proyecto de titulación
Frecuencia/Período	
Frecuencia de Recolección de Datos	Una vez
Frecuencia de Análisis de Datos	Una vez
Frecuencia del Reporte de Resultados de Medición	Una vez
Revisión de la Medición	Una vez
Período de Medición	Una vez

Tabla 10 Medición de la seguridad de la información – 7.2.1. Directrices de clasificación

7.2 Responsabilidad sobre los activos	
7.2.2. Etiquetado y manipulado de la información	
Identificación de la construcción de la medición	
Nombre de la construcción de la medición	Etiquetado y manipulación de la información
Identificador numérico	Específico de la Organización
Propósito de la construcción de la medición	Evaluar el cumplimiento de la política sobre el etiquetado y manipulado de la información.
Objetivo Control/Proceso	7.2. Clasificación de la información
Control (1)/proceso (1)	7.2.2. Etiquetado y manipulado de la información.
Objeto de la Medición y Atributos	
Objeto de Medición	Etiquetado y manipulación de la información
Atributos	Procedimientos de etiquetado de la información. Procedimientos para verificación de cumplimiento del proceso de etiquetado de información.
Especificación Medida Base (1)	
Medida Base	Nivel de cumplimiento de la elaboración de procedimientos para el etiquetado de la información. Nivel de cumplimiento de la elaboración de procedimientos para la verificación del cumplimiento del proceso de etiquetado de información.
Método de Medición	Ponderar el cumplimiento del Etiquetado y manipulado de la información.
Tipo de Método de Medición	Subjetivo
Escala	Niveles de cumplimiento: Total (T): Cumplimiento del 71% al 100% Parcial (P): Cumplimiento del 31 al 70% Nulo (N): Cumplimiento del 0 al 305
Tipo de Escala	Relación
Unidad de Medición	Personal Porcentaje
Especificación Medida Derivada	
Medida Derivada	Progreso a la fecha
Función de Medición	Calificación del cumplimiento de la norma, en base a los niveles de cumplimiento de la cada control.
Especificación del Indicador	
Indicador	Existencia de procedimientos de etiquetado de la información. Existencia de procedimientos para la verificación de cumplimiento del proceso de etiquetado de la información.
Modelo Analítico	Obtener los niveles de cumplimiento de cada control, en base a los niveles de cumplimiento de cada directriz del EGSI.

Especificación Criterios de Decisión	
Criterios de decisión	El objetivo de control se cumple de forma satisfactoria cuando se cumple cuando el nivel de cumplimiento es mayor o igual a 71%, se cumple parcialmente cuando el nivel de cumplimiento va del 31 al 70%, y no se cumple cuando el nivel de cumplimiento es menor o igual al 30%, y es una oportunidad de mejora.
Resultados de la medición	
Interpretación del Indicador	La interpretación del indicador es: - La elaboración del inventario se cumple satisfactoriamente cuando el nivel de cumplimiento es mayor o igual al 71%. - La elaboración del inventario se cumple parcialmente cuando el nivel de cumplimiento varía entre el 31 al 70%, y tiene tendencia a mejorar. - La elaboración del inventario no se cumple cuando el nivel de cumplimiento es menor o igual al 30%, y será considerada como una oportunidad de mejora.
Formatos de Reporte	Tablas de cumplimiento (Tabla 2.17 del proyecto de titulación)
Interesados	
Cliente para medición	Personal de la EEQ
Supervisor de medición	Oficial de Seguridad de la Información
Propietario de la Información	EEQ
Recolector de la Información	Autora del proyecto de titulación
Comunicador de Información	Autora del proyecto de titulación
Frecuencia/Período	
Frecuencia de Recolección de Datos	Una vez
Frecuencia de Análisis de Datos	Una vez
Frecuencia del Reporte de Resultados de Medición	Una vez
Revisión de la Medición	Una vez
Período de Medición	Una vez

Tabla 11 Medición de seguridad de la información – 7.2.2. Etiquetado y manipulado de la información

Evaluación del nivel de cumplimiento de cada directriz del EGSI

La tabla 12 mostrada a continuación, contiene la evaluación de los niveles de cumplimiento de cada una de las directrices del EGSI, en base a los criterios de evaluación indicados en la tabla 2.30 (columnas 5 y 7) y de cada uno de los

controles de la NTE INEN ISO/IEC 27002 en base a la matriz de criterios de evaluación de la tabla 2.31 (columnas 6 y 8):

ISO/IEC 27002:2005			EGSI	Documentación		Implementación	
Dominios	**Objetivos de Control**	**Controles**	**Directriz**	**Indicador de cumplimiento por Directriz (EGSI)**	**Indicador de cumplimiento por Control (ISO/IEC 27002)**	**Indicador de cumplimiento por Directriz (EGSI)**	**Indicador de cumplimiento por Control (ISO/IEC 27002)**
7. Gestión de Activos	**7.1. Responsabilidad sobre los activos**	7.1.1. Inventario de activos	3.1.1. Inventario de activos primarios en formatos físicos y/o electrónicos 3.1.2. Inventario de activos de soporte de Hardware 3.1.3. Inventario de activos de soporte de Software 3.1.4. Inventario de activos de soporte de Redes	**T** **T** **T** **T**	**T**	**P** **T** **P** **T**	**P**
		7.1.2. Responsable de los activos	3.2.1. Asignación de Responsables de los Activos 3.2.2. Consolidación inventarios de activos con sus responsables	**P** **T**	**P**	**T** **P**	**P**
		7.1.3. Uso aceptable de los activos.	3.3.1. Reglamentar uso de correo electrónico institucional 3.3.2. Reglamentar el acceso y uso de la Internet y sus aplicaciones/servicios 3.3.3. Reglamentar el uso de los sistemas de video - conferencias	**P** **N** **P**	**P**	**T** **T** **P**	**P**
	7.2. Clasificación de la información	7.2.1. Directrices de clasificación	3.4.1. Clasificar la información como pública o confidencial 3.4.2. Elaborar y aprobar un catálogo de clasificación de la información	**T** **T**	**T**	**P** **P**	**P**
		7.2.2. Etiquetado y manipulado de la información	3.5.1. Procedimientos de etiquetado de la información 3.5.2. Procedimiento para verificación de cumplimiento del proceso de etiquetado de información	**P** **P**	**P**	**P** **P**	**P**

Tabla. 12 Calificación de los indicadores de cumplimiento. [56]

[56] Elaborado por la autora.

Conclusión del proceso de evaluación

La información recopilada corresponde a las directrices de evaluación del EGSI correspondientes a los controles y objetivos de control del dominio 7. Gestión de activos de la norma ISO 27002, es decir, que se realiza una evaluación parcial de la normal en relación a lo establecido con el Oficial de Seguridad de la Información.

De los niveles de resultados obtenidos en la evaluación, se determina que los niveles de cumplimiento de la Documentación son mayores que los niveles de cumplimiento de la Implementación.

Estos resultados indican que en la EEQ se considera primordial la elaboración de documentación formal que rija a toda la organización, con el fin de definir claramente el camino a seguir previo a la implementación de un Sistema de Gestión de Seguridad de la Información.

Además, cabe recalcar que debido al proceso de mejora en el que se encuentra la EEQ, los controles evaluados están en proceso de implementación, para la cual se están elaborando y formalizando documentos que contienen políticas y/o procedimientos que permitirán una correcta gestión de la seguridad de la información en la EEQ, y a futuro, una correcta implementación de un SGSI en toda la organización.

CAPÍTULO 3. CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- Para la evaluación parcial del sistema de gestión de la seguridad de la información de la Empresa Eléctrica Quito desarrollada en este proyecto de titulación, se utilizó como dominio de evaluación, al Dominio 7. Gestión de Activos de la norma ISO 27002 junto con sus objetivos de control y controles respetivos. Como soporte a dicho dominio de evaluación, se utilizaron las directrices de evaluación del EGSI, y los CSCs de Sans Institute, lo cual permitió identificar las oportunidades de mejora de la EEQ.
- La EEQ se encuentra en un proceso de mejora continua, el mismo que está basado en la implementación de las directrices del EGSI, y que contempla actividades de mejora para la correcta gestión de la seguridad de la información.
- Para la evaluación, se utilizó una propuesta metodológica elaborada por la autora, la misma que fue desarrolla en base a la información recolectada y a las directrices, normas y controles utilizados para llevar a cabo dicha evaluación.
- Como resultado de la evaluación a la información recopilada, se logró identificar que en la EEQ se rigen estrictamente a la documentación formal elaborada en base a la norma ISO / IEC 27002, siendo ésta el punto de partida para la implementación de un Sistema de Gestión de Seguridad de la Información.
- Los resultados obtenidos durante la evaluación, indican que en la EEQ se tiene un nivel parcial de cumplimiento, lo cual indica que las tareas que se han estado llevando a cabo en la EEQ si están siendo documentadas e implementadas exitosamente, y con el futuro se podrá implantar un Sistema de Gestión de la Seguridad de la Información de una forma más fácil.

- Con respecto a la Documentación, se determinó que la EEQ cumple un 58,82% de las directrices del EGSI en cuanto a la Gestión de Activos. Se cumple parcialmente un 17,65%, y no se cumple un 23,53%. Es decir, la mayoría de las directrices del EGSI están contempladas en la documentación formal publicada y por publicar.
- Con respecto a la Implementación, se determinó que la EEQ cumple un 44,11% de las directrices del EGSI en cuanto a la Gestión de Activos. Se cumple parcialmente un 19,11%, y no se cumple un 36,77%. El nivel de incumplimiento de las directrices es alto y se debe a que se está elaborando previamente la documentación formal que respalde la implementación.

RECOMENDACIONES

- La EEQ, de acuerdo a los resultados obtenidos, debería implementar todas las directrices del EGSI, para que en un futuro cercano se implemente un Sistema de Gestión de Seguridad de la Información, el cual les permitirá automatizar varios procesos para una adecuada gestión de la seguridad de la información.
- Con respecto a la situación actual de la EEQ, se debería utilizar la NTE-ISO/IEC 27002 como parte del proceso de mejora, con la finalidad de que se identifiquen los sectores más vulnerables y se tomen las medidas correctivas necesarias para la disminución o eliminación de riesgos de seguridad, no solo de la información, sino de todos los elementos que conforman la organización.
- En la Empresa Eléctrica Quito se debería definir un solo documento para el Inventario de Activos, el mismo que debe ser gestionado por la DTIC y en cual se identifiquen claramente las características de todos los activos, de tal forma que se tenga una mayor conocimiento de la situación de la institución y se puedan tomar medidas preventivas o correctivas en cuanto al uso de los equipos activos en la EEQ.
- Se recomienda a la EEQ, la utilización de la NTE ISO/IEC 27004 [25] como ayuda para la evaluación de la eficacia de un Sistema de Gestión de Seguridad de la Información, la misma que incluye un Programa de

Medición de Seguridad de la Información que ayudará a la organización, en la identificación y evaluación de los procesos y controles del SGSI ineficaces y dará prioridades a las acciones asociadas con el mejoramiento o cambio de dichos procesos y/o controles.

- En la EEQ, antes de implementar cambios estratégicos en la compañía, se debería brindar la información necesaria a todo el personal sobre dicho cambio y las ventajas que se obtendrán. De ésta forma las personas tendrán claro el objetivo del cambio y por lo tanto cooperarán de mejor manera con el mismo y se evitará que se reúsen por miedo o desconocimiento.

BIBLIOGRAFÍA

[1] Empresa Eléctrica Quito, <<Servicio Público de Energía Eléctrica y su área de concesión – Empresa Eléctrica Quito>>, 2015. [En línea] Disponible en: http://www.eeq.com.ec/. [Último ingreso: 06/08/2014].

[2] Empresa Eléctrica Quito, <<PLAN ESTRATÉGICO EEQ 2012 – 2015>>, 2012 -2015. [En línea]. Disponible en: http://ftp.eeq.com.ec/upload/informacionPublica/PLANESTRATEGICO2012-2015.pdf. [Último ingreso: 07/12/2014].

[3] Information Security del Ecuador Inc. (I-SEC), <<Sistema de Gestión de Seguridad de la Información>>, Octubre 2013.

[4] Subsecretaría Nacional de la Gestión Pública, 2014. [En línea] Disponible en http://www.administracionpublica.gob.ec/subsecretaria-general-de-la-gestion-publica/. [Último ingreso: 07/12/2014].

[5] **REGISTRO OFICIAL** – ÓRGANO DEL GOBIENO DEL ECUADOR Administración del Sr. Ec. Rafael Correa Delgado Presidente Constitucional de la República, SEGUNDO SUPLEMENTO, Secretaría Nacional de la Administración Pública, Acuerdo No. 166. Septiembre 2013.

[6] Empresa Eléctrica Quito, << Resolución de Gerencia General No. GCG-2884-2014>>, 16 de Abril de 2014.

[7] Empresa Eléctrica Quito, <<Reforma a la Resolución de Gerencia General No. GEG-2884-2014 del 16 de Abril de 2014>>, 04 de Septiembre de 2014.

[8] Secretaría Nacional de la Administración Pública, <<**Anexo 1 del Acuerdo No. 166 del 19 de septiembre de 2013.** Esquema Gubernamental de la Seguridad de la Información (EGSI)>>, Versión 1.0, Septiembre de 2013.

[9] iso27002.es, <<El Anexo de ISO 27001 en español>> [En línea] Disponible en: http://www.iso27002.es/ [Último ingreso: 07/12/2014].

[10] SANS, <<SANS Institute>> [En línea] Disponible en: http://www.sans.org [Último ingreso: 07/12/2014].

[11] SANS, <<Critical Security Controls>> [En línea] Disponible en: http://www.sans.org/critical-security-controls [Último ingreso: 07/12/2014].

[12] ISO, <<ISO/IEC 27002:2005>> [En línea] Disponible en: http://www.iso.org/iso/catalogue_detail?csnumber=50297 [Último ingreso: 22/02/2015].

[13] Empresa Eléctrica Quito "E.E.Q. S.A.", <<EQUIPOS ACTIVOS EN LA EMPRESA ELÉCTRICA>> [Documento digital], Fecha de consulta: 29/01/2015.

[14] Empresa Eléctrica Quito "E.E.Q. S.A.", <<Inventario de Plataforma>> [Documento digital], Fecha de consulta: 22/02/2015.

[15] Empresa Eléctrica Quito "E.E.Q. S.A.", << SISTEMA DE GESTIÓN DE LA CALIDAD – Procedimiento para control de bienes. (GR-GBB-P003)>>, Revisión 08. [Documento digital].

[16] Empresa Eléctrica Quito "E.E.Q. S.A.", <<SISTEMA DE GESTIÓN DE LA CALIDAD - Políticas para el uso y manejo de los recursos informáticos de la EEQ. (TI-D001)>>, Revisión 02. [Documento digital].

[17] Empresa Eléctrica Quito "E.E.Q. S.A.", << SISTEMA DE GESTIÓN DE LA CALIDAD - Procedimiento para administración de redes y comunicaciones (TI-GRC-P001)>>, Revisión 03. [Documento digital].

[18] Empresa Eléctrica Quito "E.E.Q. S.A.", << SISTEMA DE GESTIÓN DE LA CALIDAD - Procedimiento para la gestión del portal web empresarial (TI-GDS-P003)>>, Revisión 00. [Documento digital].

[19] Empresa Eléctrica Quito "E.E.Q. S.A.", << SISTEMA DE GESTIÓN DE LA CALIDAD - Procedimiento administración de servicios Internet y Correo (TI-GBD-P004)>>, Revisión 02. [Documento Digital].

[20] Empresa Eléctrica Quito "E.E.Q. S.A.", << SISTEMA DE GESTIÓN DE LA CALIDAD - Procedimiento para administración de seguridades y accesos (TI-GBD-P003)>>, Revisión 02. [Documento Digital].

[21] Empresa Eléctrica Quito “E.E.Q. S.A.”, << SISTEMA DE GESTIÓN DE LA CALIDAD – Instructivo para Control Bienes (GR-GBB-P003-I001)>>, Revisión 08. [Documento Digital].

[22] Secretaría Nacional de la Administración Pública, <<Quipux Gestión Documental>> [En línea] Disponible en: http://www.gestiondocumental.gob.ec/ [Último ingreso 27/04/2015].

[23] Systems Experts, <<Looking at the SANS 20 Critical Security Controls – Mapping de SANS 20 to NIST 800-53 to ISO 27002 by Brad C. Jhonson>> [En línea] Disponible en: http://systemexperts.com/media/pdf/SystemExperts-SANS20-1.pdf [Último ingreso: 26/07/2015].

[24] INEN Instituto Ecuatoriano de Normalización, <<NORMA TÉCNICA ECUATORIANA NTE INEN-ISO/IEC 27002:2009>>, Primera edición, Quito-Ecuador. [Documento Digital], [Último ingreso: 06/08/2015].

[25] INEN Instituto Ecuatoriano de Normalización, <<NORMA TÉCNICA ECUATORIANA NTE INEN-ISO/IEC 27004:2012>>, Primera edición, Quito-Ecuador. [Documento Digital], [Último ingreso: 21/09/2015].