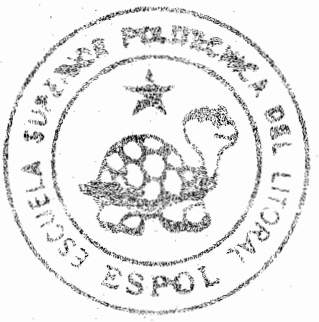
ESCUELA SUPERIOR POLITECNICA DEL LITORAL



CENTRO DE EDUCACION CONTINUA

Diplomado en Auditoría Informática

III / V PROMOCION

PROYECTO

Tesis Previo la Obtención del Diplomado en Auditoría Informática

T E M A :

"Auditoría a la Adquisición y Procesamiento de Datos del Área de Telemetría para la Empresa Eléctrica de Guayaquil Utilizando ISO 27002"

A U T O R E S :

Christian Cascante Caballero
Iván Coronel Arellano

Año 2011

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

CENTRO DE EDUCACIÓN CONTINUA

DIPLOMADO EN AUDITORÍA INFORMÁTICA

III / V PROMOCIÓN

PROYECTO

TESIS PREVIO LA OBTENCIÓN DEL DIPLOMADO EN AUDITORÍA INFORMÁTICA.

TEMA

"AUDITORÍA A LA ADQUISICIÓN Y PROCESAMIENTO DE DATOS DEL AREA DE TELEMETRÍA PARA LA EMPRESA ELÉCTRICA DE GUAYAQUIL UTILIZANDO ISO 27002"

AUTORES

CHRISTIAN CASCANTE CABALLERO
IVÁN CORONEL ARELLANO

AÑO

2011

Agradecimiento.

A las autoridades de la Eléctrica de Guayaquil

por la apertura brindada en la realización de este trabajo,

a Jorge Olaya y las personas que aportaron con su colaboración.

Dedicatoria.

A Dios

a mi madre, a Geovanny, mi hermano Walter,

a mi esposa Delia

por su apoyo incondicional

y a mis hijos Lucas e Isabela.

Christian Cascante Caballero

A Dios,

a mi padre, madre y hermana,

a mi esposa,

a mi hija.

Iván Coronel Arellano

INDICE

Capítulo 1

1. Introducción.

1.1 Antecedentes.

Los temas relativos a la auditoría informática cobran cada vez más relevancia, debido a que la información se ha convertido en el activo más importante de las empresas, representando su principal ventaja estratégica, por lo que estas invierten enormes cantidades de dinero y tiempo en la creación de sistemas de información, con el fin de obtener la mayor productividad y calidad posibles.

A partir de este siglo, los cambios adoptados por las organizaciones en el ámbito económico, industrial y social cambian de forma apresurada, debido a esto es necesario que las tecnologías de información que soportan los procesos de las organizaciones se adapten rápidamente a los nuevos requerimientos.

En base a lo antes citado, es fundamental que los procesos cuenten con los controles necesarios y que los mismos se estén cumpliendo para garantizar de forma razonable la seguridad de la información; la Unidad Eléctrica de Guayaquil se encuentra automatizando su sistema de adquisición de datos de consumo eléctrico (telemetría) por lo cual es importante revisar las actividades del proceso para determinar alguna vulnerabilidad que pueda comprometer la confidencialidad, integridad de la información y que esta esté disponible.

Hoy en día, los ataques a los sistemas de gestión de información se dan con mayor frecuencia lo que nos expone a nuevas amenazas, por lo que es necesario conocer qué vulnerabilidades podrían existir en nuestro sistema, y con ello tomar acciones que puedan mitigar o aislar su acción en el caso que se lleguen a materializar.

1.2 Introducción a la Auditoría Informática.

En la actualidad, las tecnologías de la información están presentes en todas las áreas de las organizaciones soportando sus procesos. Esta implantación generalizada de SI se ha realizado en muchos casos sin la necesaria planificación, en parte por el desconocimiento de los conceptos por el personal de TI. La tendencia hacia los sistemas abiertos, la interconexión global y el deseo por parte de los consumidores de independizarse de los fabricantes traen consigo la necesidad de un estudio más profundo de los SI antes de tomar decisiones. Por lo tanto, se hace necesario mejorar la planificación de futuras implementaciones, la compatibilidad entre sistemas y la organización del personal y de la empresa.

En las organizaciones modernas, tanto públicas como privadas, la misión de las tecnologías de la información es facilitar la consecución de sus objetivos estratégicos. Para ello, es necesario que se invierta una considerable cantidad de recursos en personal, equipos y tecnología, además de los costos derivados de la posible organización estructural que muchas veces conlleva la introducción de estas tecnologías. Esta importante inversión debe ser constantemente justificada en términos de eficacia y eficiencia. Por tanto, el propósito a alcanzar por una organización que contrata la auditoria de cualquier parte de sus SI es asegurar que sus objetivos estratégicos son los mismos que los de la propia organización y que los sistemas prestan el apoyo adecuado a la consecución de estos objetivos, tanto en el presente como en su evolución futura.

La Auditoría en Informática es la revisión y evaluación de los controles, sistemas, procedimientos de informática, de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a de lograr una utilización más eficiente y segura de la información que servirá para la adecuada toma de decisiones.

Los objetivos de la auditoría Informática son:

- El control de la función informática.
- El análisis de la eficiencia de los Sistemas Informáticos.
- La verificación del cumplimiento de la Normativa en este ámbito.
- La revisión de la eficaz gestión de los recursos informáticos.

La auditoría informática sirve para mejorar ciertas características en la empresa como:

- Eficiencia
- Eficacia
- Rentabilidad
- Seguridad

Generalmente se puede desarrollar en alguna o combinación de las siguientes áreas:

- Gobierno corporativo.
- Administración del Ciclo de vida de los sistemas.
- Servicios de Entrega y Soporte.
- Protección y Seguridad.
- Planes de continuidad y Recuperación de desastres.

La necesidad de contar con lineamientos y herramientas estándar para el ejercicio de la auditoría informática ha promovido la creación y desarrollo de mejores prácticas como COBIT, ISO y COSO

1.3 Objetivo del Proyecto de Auditoria.

- Evaluar la adquisición y el procesamiento automatizado de datos del área de Telemetría de la empresa Eléctrica de Guayaquil, basado en el análisis y revisión de la documentación y actividades mediante la utilización de herramientas y conocimientos adquiridos durante el curso de Diplomado de Auditoria Informática.

- Dar a conocer la importancia de realizar revisiones regulares de las tecnologías de la información en su fase de planeación, desarrollo, implementación y control; con el fin de cumplir con los objetivos y metas de negocio.

1.4 Alcance.

El alcance de este trabajo comprende la revisión de los recursos y actividades de TI que intervienen en el proceso de adquisición de datos que utiliza el área de Telemetría para generar información que influye directamente en las actividades de facturación, cortes y reconexión del servicio eléctrico.

En la documentación entregable se emitirá un informe final donde se incluirán las debidas recomendaciones para contribuir con la mejora del proceso.

Cabe indicar que en el presente trabajo no se incluirá diseño, ni implementación de los controles sugeridos.

1.5 Información Institucional.

1.5.1 Reseña histórica.

En 1905 se crea la Empresa "Luz y Fuerza Eléctrica" para la prestación del servicio eléctrico en la ciudad de Guayaquil.

El 29 de octubre de 1925, la Municipalidad del Cantón Guayaquil celebró con la Empresa Eléctrica del Ecuador Inc., constituida en el Estado de Maine de los Estados Unidos de América, un contrato de concesión para la producción, transmisión, distribución, uso y suministro de electricidad para el mencionado cantón.

El Consejo Nacional de Electricidad, CONELEC y Electroecuador Inc. celebraron el 16 de agosto de 1999 el contrato de concesión específica para la generación de energía eléctrica en Guayaquil, posteriormente, este contrato fue terminado por el Consejo de modo unilateral y anticipadamente mediante resolución 208/03 de fecha 17 de septiembre del 2003, en vista de que Electroecuador Inc. no se encontraba cumpliendo el objeto del contrato de concesión suscrito, al no mantener a su cargo las actividades de generación, establecidas en el mismo y éstas estaban siendo realizadas por terceras personas, lo que significó que la concesionaria Electroecuador Inc. había dejado de cumplir con sus obligaciones, ocasionando inclusive que se encuentren pendientes varias actividades de mantenimiento preventivo y correctivo.

El Consejo Nacional de Electricidad, CONELEC, el 23 de marzo del 2000, dictó la Resolución #0034/00, por la que se dispone convocar a licitación pública disponiendo la iniciación del procedimiento para la selección de la empresa que prestaría el servicio público de distribución y comercialización de energía eléctrica en área de concesión Guayaquil y consecuentemente declaró terminada en forma definitiva la operación del referido servicio que venía suministrando la Empresa Eléctrica del Ecuador Inc. y asumió por delegación, a través de un tercero, denominado Administrador Temporal la continuidad de la provisión del mismo utilizando para ello los bienes afectos al servicio de Distribución.

Mediante Decreto Ejecutivo No. 712, publicado en el Registro Oficial No. 149 del 18 de agosto del 2003 se crea la "CORPORACIÓN PARA LA ADMINISTRACIÓN TEMPORAL ELÉCTRICA DE GUAYAQUIL" como una persona jurídica de derecho privado, con finalidad pública, sin fines de lucro, con patrimonio y fondos propios.

Mediante Decreto Ejecutivo No. 1786, de junio 18 del 2009, publicado mediante Registro Oficial No. 625 de julio 2 de 2009, la Corporación para la Administración Temporal Eléctrica de Guayaquil, se convierte en la UNIDAD DE GENERACIÓN, DISTRIBUCIÓN Y COMERCIALIZACIÓN DE ENERGÍA ELÉCTRICA DE GUAYAQUIL -ELÉCTRICA DE GUAYAQUIL-.

1.5.2 Rol de la Empresa Eléctrica de Guayaquil.

La ELÉCTRICA DE GUAYAQUIL, con sede en la ciudad de Guayaquil, Provincia del Guayas, tiene como rol principal asumir la prestación de los servicios de generación, distribución y comercialización de la energía eléctrica en el área de servicio pudiendo participar para su gestión en empresas mixtas y en compañías de economía mixta, de conformidad con la Constitución y la ley.

Los ingresos económicos con los que opera la Unidad Eléctrica de Guayaquil provienen principalmente de la generación, distribución y comercialización de energía eléctrica a los usuarios, otros servicios y de las asignaciones del Presupuesto General del Estado.

1.5.3 Situación Jurídica.

Con la expedición del Decreto Ejecutivo No. 1786 de fecha 18 de junio se convierte la "Corporación para la Administración Temporal Eléctrica de Guayaquil" en la Unidad de Generación, Distribución y Comercialización de Energía Eléctrica de Guayaquil -Eléctrica de Guayaquil- como organismo de la Función Ejecutiva del Estado, que conforma la administración pública central, adscrito al Ministerio de Electricidad y Energía Renovable, regulada

en consecuencia por normas, leyes, reglamentos, regulaciones, estatutos y demás cuerpos legales concernientes al Derecho Público, y que además forma parte del sector estratégico del Estado, teniendo como eje de acción la eficiencia en la prestación del servicio público de generación, distribución y comercialización de energía eléctrica, mediante la optimización de los recursos, y regida por principios de eficacia, eficiencia, calidad, coordinación, participación, desconcentración, planificación, transparencia y evaluación.

Los bienes e instalaciones con los que cuenta la Unidad Eléctrica de Guayaquil, de conformidad al Decreto Ejecutivo No. 1786, Art. 4 No. 1, son los bienes e instalaciones afectos a los servicios públicos de generación, distribución y comercialización de la fuerza eléctrica en Guayaquil, que deberán ser transferidos al Estado por la terminación del contrato concesivo celebrado con Electroecuador Inc., y la Empresa Eléctrica del Ecuador Inc. de conformidad al Art. 43 de la Ley de Régimen del Sector Eléctrico, así como los bienes adquiridos por la "CORPORACIÓN PARA LA ADMINISTRACIÓN TEMPORAL ELÉCTRICA DE GUAYAQUIL" desde el inicio de sus operaciones.

Con respecto al recurso humano que venía laborando en la Ex CATEG, se mantuvo la continuidad de las relaciones laborales de todos los trabajadores que prestaban sus servicios en relación de dependencia con las limitaciones legales y constitucionales del régimen de Derecho Público, siendo el Ministerio de Relaciones Laborales el encargado de determinar quiénes son los servidores que se regirán por la Ley Orgánica de Servicio Civil y Carrera Administrativa y de Unificación y Homologación de las Remuneraciones del Sector Público y obreros sujetos al Código de Trabajo.

1.5.4 Visión.

Ser una empresa líder en el sector eléctrico en el Ecuador, reconocida por la comunidad en función a la calidad y confiabilidad del servicio, con la generación de energía eficiente, limpia y sustentable.

1.5.5 Misión.

Brindar el servicio público de generación, distribución y comercialización de energía eléctrica, con estándares de calidad y confiabilidad, cultura organizacional orientada a la satisfacción del cliente, que garantice el desarrollo económico y social de la ciudad de Guayaquil.

1.5.6 Situación actual.

La Eléctrica de Guayaquil actualmente brinda el servicio Generación de Distribución y Comercialización de energía eléctrica a 586.539 abonados (junio de 2011) tanto residenciales como comerciales. Para poder brindar una atención ágil y óptima, la empresa cuenta con 7 agencias alrededor de la ciudad.

A continuación una proyección de su crecimiento en abonados:

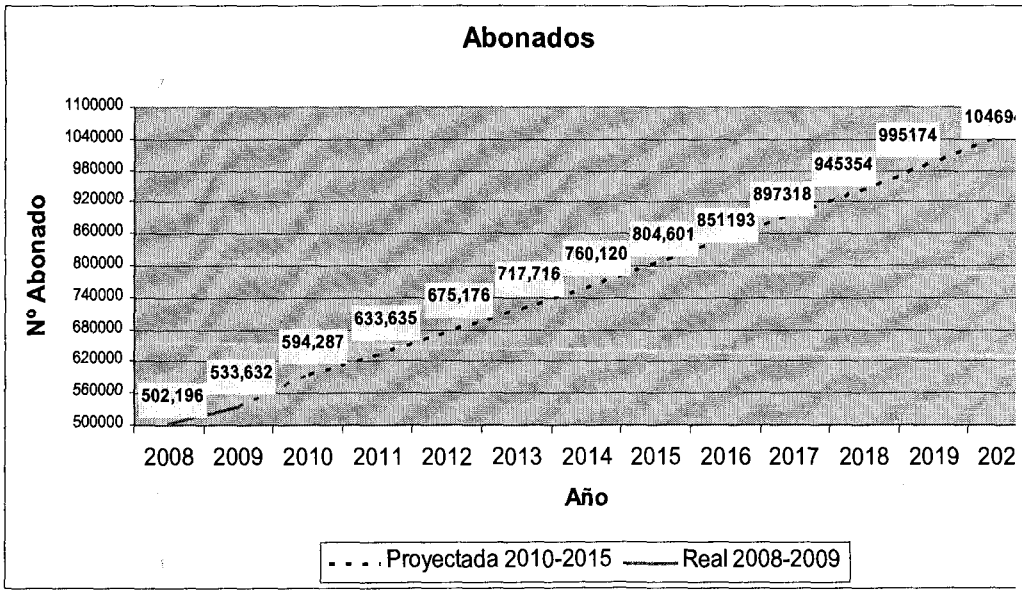


Figura 1.1 Proyección de crecimiento de abonados.

1.5.7 Objetivos estratégicos - Eléctrica de Guayaquil.

- Consolidar la empresa con una estructura organizacional de administración por procesos.
- Desarrollar el talento humano capacitándolo, comprometiéndolo y motivándolo.
- Ser calificada por nuestros usuarios como una empresa orientada al servicio al cliente.
- Ampliar cobertura dentro de nuestra área de servicio.
- Desarrollar un sistema eléctrico de confiabilidad con tecnologías de punta.
- Operar sobre las bases de indicadores nacionales e internacionales de calidad en materia de productividad, competitividad y tecnología.
- Optimizar la distribución de energía eléctrica con la reducción de pérdidas técnicas y comerciales.
- Mejorar los índices de cobrabilidad y recuperación de cartera vencida.
- Transparentar la gestión mediante la rendición de cuentas.

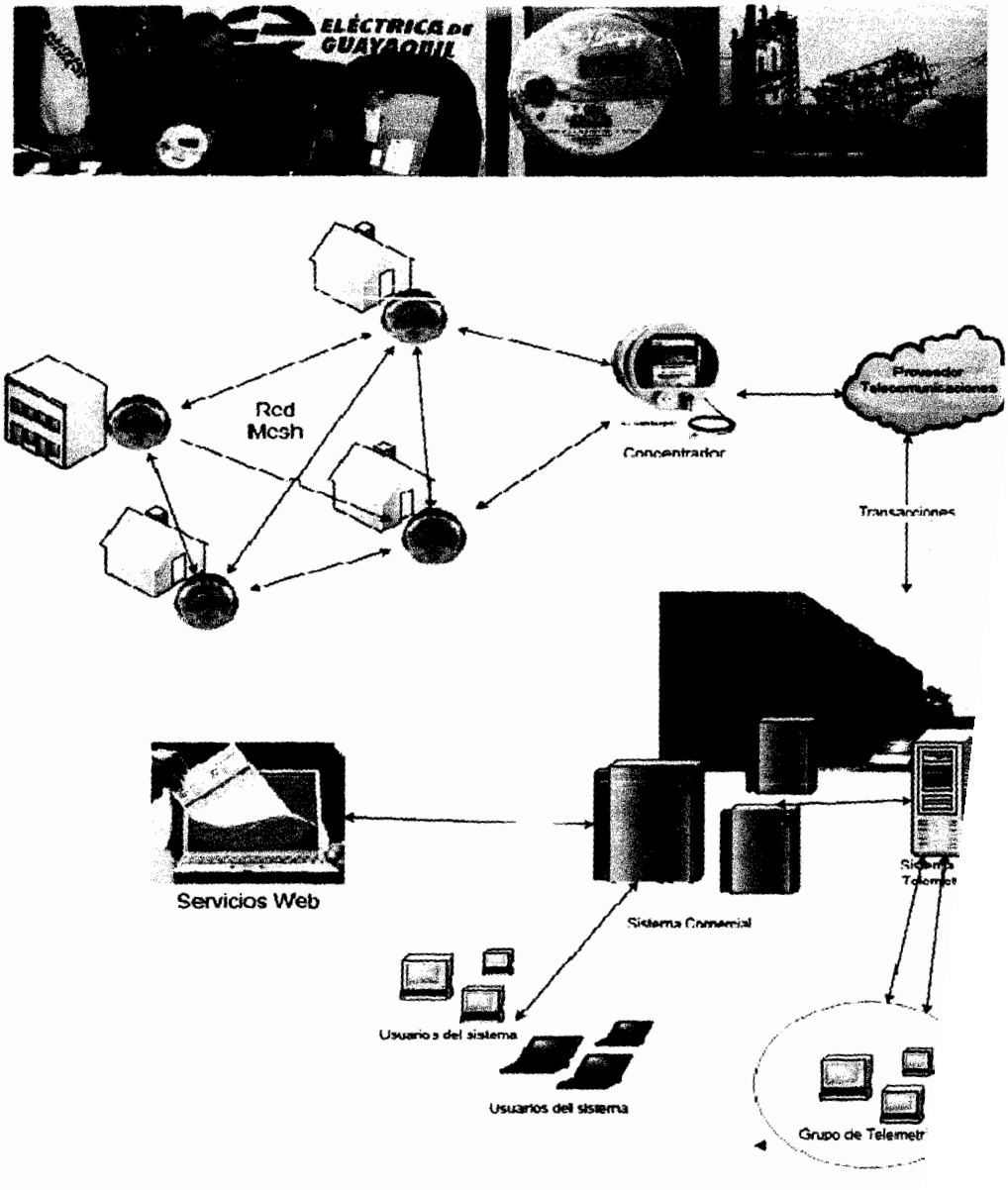
1.5.8 Organigrama de la Eléctrica de Guayaquil.

Ver Anexo 1

1.6 Área de Telemetría.

Su función principal es diseñar e implementar soluciones para una mejor gestión de lectura de datos y automatización de servicios. Son los encargados de administrar los equipos de recolección de lecturas del consumo eléctrico de forma automatizada y ponerla a disposición de las diferentes áreas de la empresa, para ejecutar sus procesos correspondientes.

Esquema de Masificación del Proceso de Telemetria para la ciudad de Guayaquil



1.6.1 Organización del área de telemetría.

El área de telemetría está organizada de la siguiente forma:

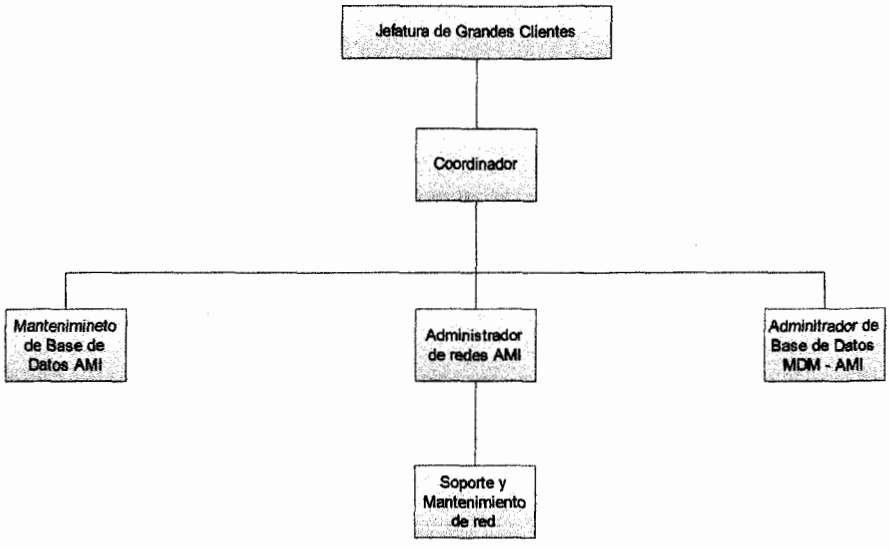


Figura 1.2 Organigrama de telemetría.

1.6.2 Descripción del proceso de telemetría.

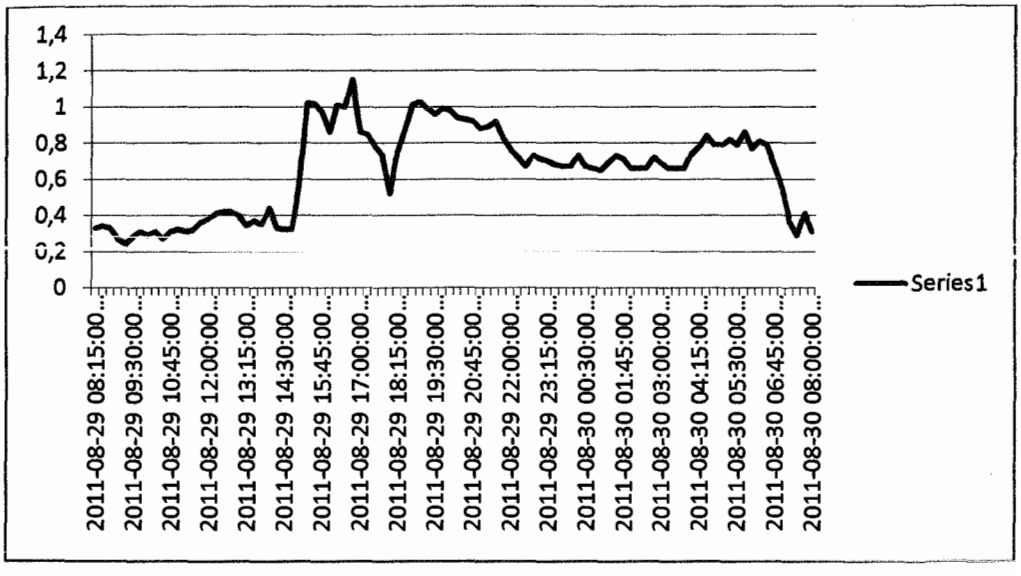
En la actualidad las Empresas se proyectan a un gran crecimiento de su plataforma tecnológica sin tomar en cuenta la importancia del control y revisión de las tecnologías de la información para la ejecución de proyectos, por lo cual las Organizaciones requieren de revisiones que les permita evaluar sus procedimientos y desempeño.

La Telemetría es un conjunto de procedimientos para medir magnitudes físicas y químicas desde una posición distante al lugar donde se producen los fenómenos cuando existen limitaciones de acceso y el posterior envío de la información hacia el operador del sistema.

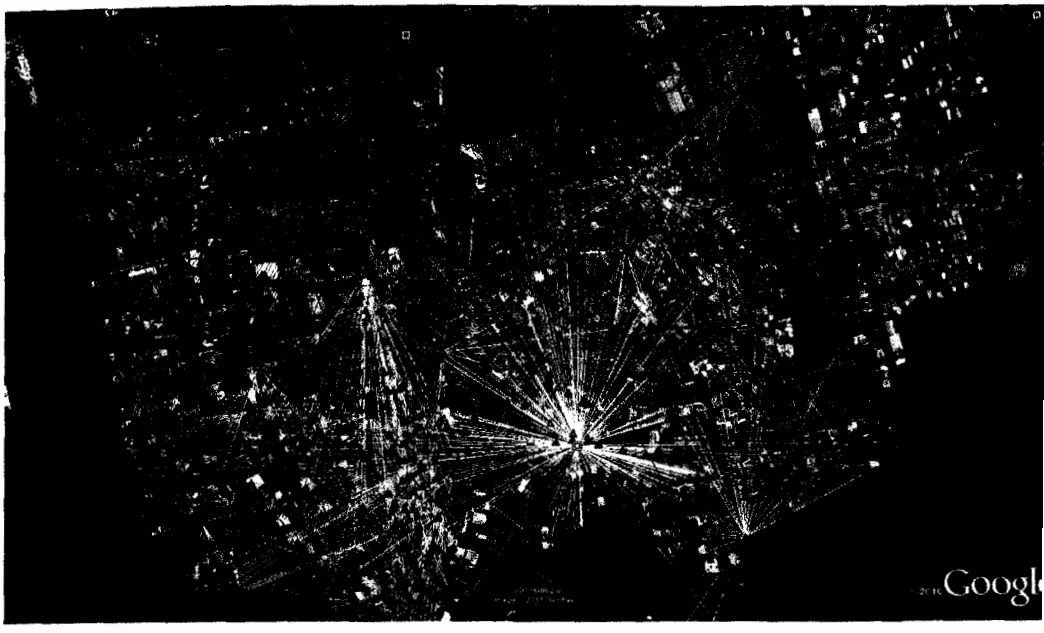
La palabra telemetría procede de las palabras griegas τηλε (tele), que quiere decir a distancia, y la palabra μετρον (metron), que quiere decir medida.

El envío de información hacia el operador en un sistema de telemetría se realiza típicamente mediante comunicación inalámbrica, aunque también se puede realizar por otros medios (teléfono, redes de ordenadores, enlace de fibra óptica, etcétera). Los sistemas de telemetría reciben las instrucciones y los datos necesarios para operar mediante desde el Centro de Control.

En la "Eléctrica de Guayaquil", los procesos de Telemetría soportados por la tecnología AMI (Infraestructura de Medición Avanzada) está orientada a la adquisición de lecturas de consumo eléctrico de 4,517 para clientes con tarifa Industrial, Comercial y Residencial.



La implementación del Sistema de Telemetría AMI cuya cobertura por medio de red inalámbrica está orientada a clientes ubicados en el sector vía a la costa, distribuidos en 405 Clientes con tarifa Industrial y Comercial, y 3,852 Clientes con tarifa residencial o masiva.



Los datos de lectura de consumo eléctrico pasa a ser procesada por el sistema comercial de la empresa con el fin de realizar los cortes y re conexión del servicio en línea además de a un futuro ofrecer la modalidad de energía eléctrica prepago. En su primera fase, este servicio se encuentra implementado en el sector de vía a la costa en el área de concesión (desde el Km 10 hasta el km 32), donde se encuentran clientes corporativos de gran demanda y consumo de energía eléctrica.

El proyecto contempla masificar de forma sostenible el uso de estos medidores AMI, que son la base para la automatización de varios procesos comerciales que inciden directamente en el servicio al cliente.

Esta importante inversión realizada por la Eléctrica de Guayaquil le permite tomar ventaja y marcar el liderazgo en el sector eléctrico a nivel nacional y en la región por lo que es necesaria la revisión de los controles implementados al proceso a fin de poder evaluar los procedimientos y desempeño del mismo.

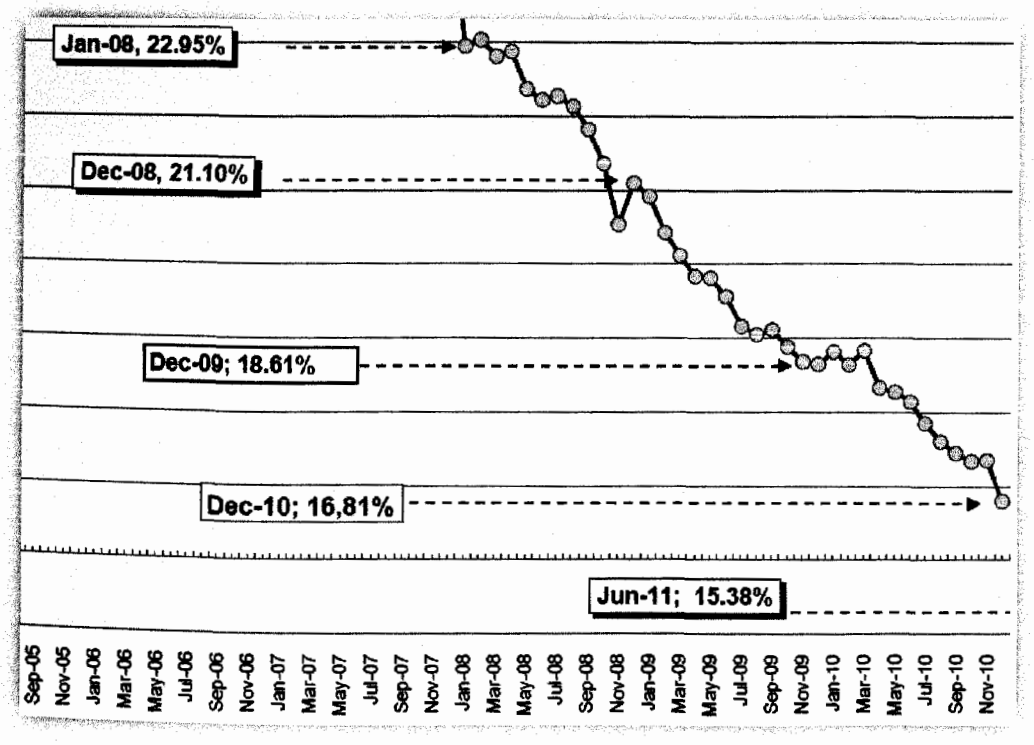
Se debe mencionar también que la información recibida a través de la red de telemetría, es de carácter confidencial, por lo que cualquier filtración no autorizada podría ser mal utilizada por terceros; de ocurrir dicho evento se afectaría directamente a la información que es el activo más importante de la

empresa, su imagen y la privacidad del usuario por lo cual se debe preservar su confidencialidad, integridad y disponibilidad.

1.6.3 Índice de recuperación de pérdidas con la automatización del proceso de telemetría.

El evento más común al que se encuentra expuesta la empresa Eléctrica de Guayaquil es el hurto de energía, manipulación de sus equipos de medición y manipulación de la información de lectura tomada de forma manual. Aunque actualmente se ha iniciado con la automatización de la lectura de consumo eléctrico, la cobertura del mismo es mínima (0.62%) de los abonados pero debido a los resultados obtenidos en este ultimo año el proyecto se masificara en toda la ciudad y con proyección nacional a mediano plazo.

En los tres últimos años la Eléctrica de Guayaquil ha reducido el índice de pérdidas del 22.95% al 16.81% hasta finales del 2010 y en el transcurso del presente año hasta mayo del 2011 el porcentaje de pérdidas se ha reducido hasta el 15.38%.



La necesidad de la Eléctrica de Guayaquil de contar con un sistema confiable de gestión de información en línea de sus clientes requiere la revisión constante de sus prácticas y actividades a fin de poder monitorear y evaluar el fiel cumplimiento del proceso establecido y garantizar una gestión confiable a sus clientes y a la vez incrementar el índice de cumplimiento de las normativas de calidad impuestas por los entes reguladores del país.

Capítulo 2

2. Auditoría Informática.

La auditoría informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un Sistema de Información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.

Auditar consiste principalmente en estudiar los mecanismos de control que están implantados en una empresa u organización, determinando si los mismos son adecuados y cumplen unos determinados objetivos o estrategias, estableciendo los cambios que se deberían realizar para la consecución de los mismos.

2.1 Seguridad de la información.

La Seguridad de la Información determina que la información es el activo más crítico de las empresas y por ende es indispensable preservar su integridad, confidencialidad y disponibilidad razonablemente, ya que es imposible eliminar completamente los riesgos; pero si se puede reducirlos considerablemente mediante la implementación de controles para estar protegidos contra eventos externos y/o interno que pueden representar amenazas y vulnerabilidades.

Figura 2.1 Características de la información segura.

- **Confidencialidad.**
  La información que se cambia entre individuos y empresas no siempre deberá ser conocida por todo el mundo. Mucha de la información generada por las personas se destina a un grupo específico de individuos y muchas veces a una única persona. Eso significa que esos datos deberán ser conocidos solo por un grupo controlado de personas.

- **Integridad.**
  La integridad de la información se logra al asegurar que la misma no ha sido alterada de forma indebido o no autorizada; para que la información se pueda utilizar, deberá esta integra, cuando ha existido una alteración no autorizada quiere decir que ha perdido su integridad.

- **Disponibilidad.**
  La disponibilidad permite que la información se la pueda utilizar; para que esto se cumpla, toda la estructura física y tecnológica que permite el acceso, transito y almacenamiento. La disponibilidad de la información permite:
  - ✓ Se utilice cuando sea necesario.
  - ✓ Se encuentre al alcance de los usuarios y destinatarios.

Los procesos, sistemas y redes constituyen los recursos de las empresas para la obtención de la información por lo que es necesario asegurar la confidencialidad, integridad y disponibilidad de la misma a fin de generar una ventaja competitiva, incrementar el índice de recaudación y disminuir las perdidas y mejorar la imagen comercial de la organización; hay que tener en cuenta que gran parte del éxito de una empresa dependerá de la calidad de la información que esta genere y gestiona.

Para lograr lo antes expuesto es necesario que se implementen controles que contenga políticas, prácticas, procedimientos, estructuras organizacionales para garantizar que los riesgos dentro del proceso a auditar sean reducidos a un nivel aceptable y se cumpla con la recuperación de pérdidas. La falta de controles expone a la empresa a pérdidas no monetarias pero de gran importancia como lo es el daño a la reputación de la institución.

2.2 Estándares relacionados a la seguridad de la información.

En la actualidad diferentes organizaciones han desarrollado varios marcos de referencia relacionados con la seguridad de la información entre los que podemos mencionar los más conocidos:

- International Standards Organization: ISO 17799:2000, ISO 17799:2005, ISO 27000:2005.
- IT Governance Institute and Information System and Audit Control Association – ISACA: Marco de Referencia COBIT. Última versión 4.1.

2.2.1 ISO – International Organization for Standardization.

La Organización de Estándares Internacionales (ISO) es el organismo líder a nivel mundial en el desarrollo de estándares, los cuales especifican los requerimientos de los productos, servicios, procesos, materiales, sistemas; su administración y prácticas organizacionales.

Entre los estándares más conocidos tenemos:

- ISO 9000 – Orientado a Sistemas de Gestión de Calidad.
- ISO 14001 – Enfocada a Administración Ambiental.
- ISO 17700 – Brinda buena prácticas de Seguridad de la Información basada en la BS 7799 Parte 1.

El alcance del presente trabajo se enfoca exclusivamente en la revisión de los recursos y actividades de TI que intervienen en el proceso de adquisición de datos que utiliza el área de Telemetría y la seguridad de la información; basándonos directamente en la norma ISO 27002:2005.

2.2.2 Information System and Audit Control Association – ISACA.

ISACA (Asociación de Auditoría y Control de Sistemas de Información) es una asociación de profesionales y universitarios que se dedican a la práctica y estudio de la auditoría, el control y la seguridad informática.

El Marco de Referencia de buenas prácticas denominado Metodología COBIT, (Control Objectives Information Technologies) Objetivos de Control para la Información y Tecnologías, está enfocada a la seguridad de la información.

COBIT 4.1 tiene una estructura estándar de 34 procesos u Objetivos de Control en cuatro dominios perfectamente definidos:

- Planeamiento y Organización.
- Adquisición e Implementación.
- Entrega y Soporte.
- Monitoreo.

2.3 La Serie ISO 27000

La norma ISO 27000 difiere en el resto de normas pues esta es una recopilación de estándares. Su numeración se reservó para todas aquellas normas relacionadas con los sistemas de gestión de seguridad de la información. Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044.

La serie de estándares 27000 pueden ser mencionados de la siguiente manera:

- **ISO 27000 (términos y definiciones):** Contiene todo el vocabulario perfecta y concisamente definido para toda la serie 27000. Su objetivo es evitar las distintas interpretaciones entre los conceptos técnicos y de gestión.

- **ISO 27001 (requerimientos de un SGSI):** Es la norma principal de las serie y contiene los requisitos del sistema de gestión de seguridad de la información.

- **ISO 27002 (objetivos de control y controles):** Corresponde a una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. Esta norma no es certificable. Contiene 39 objetivos de control y 133 controles agrupados en 11 dominios.

- **ISO 27003 (guía de implantación de un SGSI):** Constituye otra guía de implementación de Seguridad de Información pero esta vez orientada al uso del PDCA y de sus requerimientos.

- **ISO 27004 (métricas y técnicas de medida de la efectividad de un SGSI):** Se especificará las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados.

- **ISO 27005 (guía para la gestión del riesgo de seguridad de la información):** Establece las directrices para la gestión del riesgo en la seguridad de la información, apoyando los conceptos generales de la norma 27001. Su diseño está enfocado a la aplicación satisfactoria de la seguridad de la información en la gestión de riesgos.

- **ISO 27006 (proceso de acreditación de entidades de certificación y el registro de PGSI's):** Esta norma tiene la finalidad de interpretar los criterios de acreditación de las diferentes normas ISO cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma.

2.4 ISO 27002:2005

Es un estándar de seguridad de la información publicado por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), titulada Tecnología de la información - Técnicas de seguridad - Código de buenas prácticas para la gestión de seguridad de la información.

ISO / IEC 27002:2005 se ha convertido de BS7799, publicado a mediados de la década de 1990. La norma británica fue adoptada por la norma ISO / IEC como ISO / IEC 17799:2000, revisado en 2005, y pasa a ser (pero por lo demás sin cambios) en 2007 para alinear con la otra la norma ISO / IEC 27000 de la serie de normas.

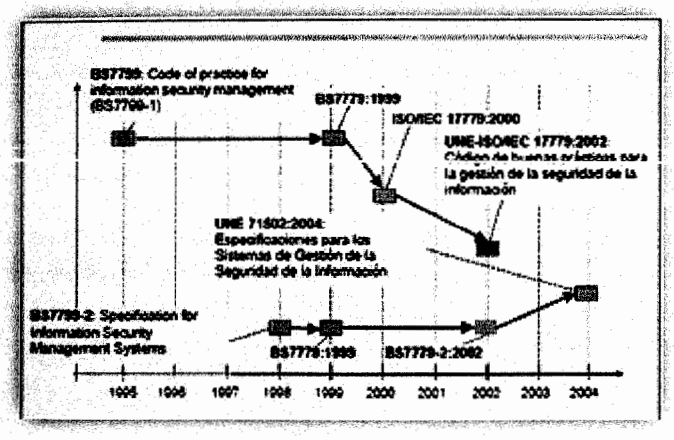


Figura 2.2 Evolución de la norma ISO 2700

ISO / IEC 27002 proporciona las mejores prácticas, recomendaciones sobre la gestión de seguridad de la información para su utilización por los responsables de iniciar, implementar o mantener la seguridad de la información, se define como: la preservación de la confidencialidad (asegurando que la información sea accesible a las personas autorizadas a tener acceso), integridad (protección de la exactitud e integridad de la información y los métodos de procesamiento) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y los activos asociados cuando sea necesario).

Consta de 11 dominios (Áreas de actuación) y 39 objetivos de control y 133 controles para asegurar los distintos objetivos de control.

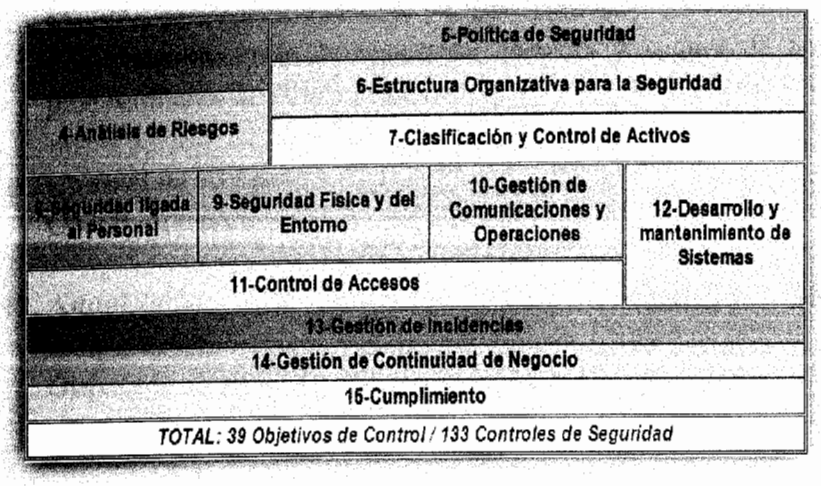


Figura 2.3 Dominios de la norma ISO 27002:2005

5. **Política de Seguridad de la información.**
   Objetivo: Proporcionar la guía y apoyo de la Dirección para la seguridad de la información en relación a los requisitos del negocio y a las leyes y regulaciones relevantes.

6. **Organización de la Seguridad de la información.**
   Objetivo: Manejar la seguridad de la información dentro de la organización.

7. **Gestión de Activos.**
   Objetivo: Lograr y mantener una apropiada protección de los activos organizacionales.

8. **Seguridad de Recursos Humanos.**
   Objetivo: Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados; reducir el riesgo de robo fraude y mal uso de los medios.

9. **Seguridad Física y Ambiental.**
   Objetivo: Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización.

10. **Gestión de Comunicaciones y Operaciones.**
    Objetivo: Asegurar la operación correcta y segura de los medios de procesamiento de la información.

11. **Control de Accesos.**
    Objetivo: Controlar el acceso a la información.

12. **Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.**
    Objetivo: Garantizar que la seguridad sea una parte integral de los sistemas de información.

13. **Gestión de Incidentes de la Seguridad de la Información.**
    Objetivo: Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva oportuna.

14. **Gestión de Continuidad del Negocio.**
    Objetivo: Contraatacar las interrupciones a las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

15. **Cumplimiento.**
    Objetivo: Evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad.

Capítulo 3

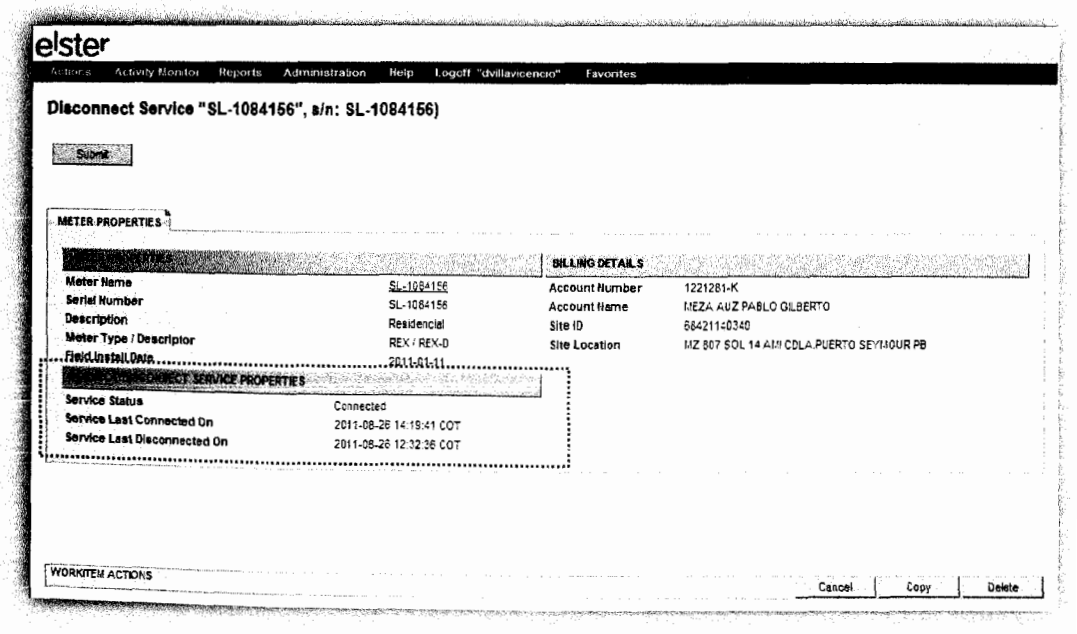
3. Alcance y definición de proyecto de tesis.

3.1 Objetivo del trabajo.

Revisar las actividades y controles implementados en el Proceso de Telemetría perteneciente a la Empresa Eléctrica de Guayaquil, identificar los riesgos y emitir recomendaciones para uso de la entidad.

El siguiente trabajo pondrá a disposición de la empresa lo siguiente:

- Identificación de las vulnerabilidades existentes en la gestión del Área de Telemetría y Tecnología.
- Registro de riesgos y su análisis de impacto al negocio.
- Tabla de recomendaciones para mitigar los riesgos existentes.



El objetivo de la realización de este trabajo es alertar a la Eléctrica de Guayaquil de las amenazas existente en el proceso a revisar, para que se tomen medidas correctivas y mitigar su impacto en el caso que se materialicen; esto servirá de guía previo a la implementación del proyecto de

automatización de lecturas de consumo eléctrico, cortes y reconexiones en toda la ciudad.

3.2 Alcance.

El presente trabajo consiste en la revisión de las actividades del proceso de telemetría en la que tenemos la adquisición de data de lecturas del consumo eléctrico, procesamiento de la data para poner a disposición de los procesos de facturación y la ejecución de cortes y reconexión automática del servicio eléctrico.

Como consta en nuestra propuesta inicial la cual fue aceptada por el Gerente del Área Operativa Comercial (Anexo 2), utilizaremos como marco de referencia la "Guía de mejores prácticas" ISO 27002:2005 y abarcaremos los siguientes dominios:

- Seguridad física y ambiental.
- Gestión de comunicaciones y operaciones.
- Control de acceso.

Detallaremos los hallazgos encontrados en la revisión y si cumplen con el control de referencia, en el caso de no cumplir se detallara el riesgo que existe y la recomendación correspondiente.

Es necesario indicar que en el presente proyecto de no se detallarán controles especifico a aplicar ni su implementación.

3.3 Equipo de Auditoría.

El equipo de trabajo está conformado por:

- ✓ Christian Giovanni Cascante Caballero
- ✓ Álvaro Iván Coronel Arellano

3.3.1 Nomenclatura de responsables utilizada en la tabla del plan de trabajo.

Participante.	*Nomenclatura*
Christian Cascante	CC
Iván Coronel	IC

3.4 Plan de trabajo.

El plan de trabajo aplicado en el presente proyecto, se describe las etapas, actividades y asignación de responsabilidades.

Etapa.	Tares a Realizar	Responsable	
		IC	CC
1	**Entendimiento de la Empresa.**		
	Reunión con el Gerente del Área Operativo Comercial.	X	X
	Reunión con el Jefe del Departamento de Telemetría.	X	X
	Reunión con el Jefe de TI - Telemetría.	X	
	Entrevista con el personal que interviene en el proceso de telemetría	X	X
2	**Reconocimiento del Proceso de Telemetría.**		
	Reconocimiento del Proceso de Telemetría y visitas de campo.	X	X
	Levantamiento de información relacionada a la adquisición de datos del Proceso de Telemetría.		X
	Revisión de la Documentación existente	X	
3	**Definición del Alcance**		
	Definición del Marco de Referencia.	X	X
	Selección de los dominios aplicables al trabajo de auditoría.	X	X
	Análisis de las entrevistas con el personal que intervienen en el proceso.	X	X
4	**Ejecución del trabajo de auditoría.**		
	Revisar los controles existentes en la adquisición de datos.	X	X
	Definición de los dominios aplicables al trabajo.	X	X
	Elaboración de Checklist	X	X
	Revisión de los controles existentes en las actividades del proceso	X	X
	Descripción de los hallazgos	X	X
	Elaboración de sugerencias	X	X
	Documentación.	X	X
	Elaboración de las conclusiones.	X	X
	Documentación.	X	X

Tabla 3.1 Plan de trabajo

3.5 Actividades a realizarse según plan de trabajo.

Etapa.	Descripción de Tareas.	
1	**Entendimiento de la Empresa.**	
	Reunión con el Gerente del Área Operativo Comercial.	Entrevista con el Ing. Diego Sánchez para conocer acerca de la seguridad de la información que se gestiona.
	Reunión con el Jefe del Departamento de Telemetría.	Entrevista con el Ing. Geovanny Ramírez a fin de determinar la actividad del Departamento de Telemetría.
	Reunión con el Jefe de TI - Administrador del sistema Energy Axis	Conocer el entorno informático donde se gestiona la información y los controles que se aplican para garantizar la seguridad de la información.
	Entrevista con el personal que interviene en el proceso de telemetría	Conocer a las actividades que se ejecutan en el proceso de Telemetría.
2	**Reconocimiento del Proceso de Telemetría.**	
	Reconocimiento del Proceso de Telemetría y visitas de campo.	Conocer como se obtienen los datos que van a ser procesados.
	Levantamiento de información relacionada al Proceso de Telemetría.	Determinar los servicios que ofrece el proceso a auditar a las otras áreas de la empresa.
	Revisión de la Documentación existente	Determinar si las actividades y procedimientos se encuentran debidamente documentados.
3	**Definición del Alcance**	
	Definición del Marco de Referencia.	Investigar sobre los dominios, controles de ISO 27002:2005.
	Selección de los dominios aplicables al trabajo de auditoría.	Investigar sobre los dominios, controles de ISO 27002:2005.
	Reunión con el Gerente del Área Operativo Comercial.	Poner a conocimiento del Ing. Diego Sánchez el alcance del trabajo de auditoría.

4	**Ejecución del trabajo de auditoría.**	
	Definición de los dominios aplicables al trabajo.	Determinar los dominios aplicables para revisar la seguridad física de los equipos de cómputo y la seguridad de la información en la gestión de TI.
	Elaboración del Checklist	
		Elaborar un Checklist en base a los dominios seleccionados en ISO 27002:2005 para revisar la seguridad de la información en la adquisición y procesamiento de datos.
	Aplicación del Checklist	Revisar las actividades y controles en base al Checklist y describir los hallazgos.
	Determinar los riesgos existentes.	Revisar la información obtenida en el Checklist y determinar los posibles riesgos.
	Evaluación del Riesgo	Tasar los riesgos encontrados y determinar su criticidad.
	Recomendaciones.	Emitir recomendaciones en base a los hallazgos que no cumplen con los controles de referencia aplicados en la revisión.
	Documentación.	Realizar matriz de resumen de las revisiones. Elaborar documentos a incluir en los anexos.
	Elaboración de las conclusiones.	Elaborar las conclusiones en base a la revisión del proceso.
	Documentación.	Elaborar la documentación entregable. (Tesis)

Tabla 3.2 Actividades a realizarse

3.6 Justificación de aplicabilidad de los controles de ISO 27002:2005 en la revisión del proceso de telemetría.

La aplicabilidad de los dominios de ISO 27002:2005 ha sido determinada en base a la información facilitada por el personal de la Empresa Electica de Guayaquil y el Alcance del proyecto de Auditoria. ***(Anexo 2)***

Dominio: Seguridad Física y Ambiental.

9 Seguridad Física y Ambiental.					
Estándar	**Objetivo**		**Controles**	**Aplica (Si/No)**	**Justificación de la Ejecución**
9.1	Áreas Seguras	9.1.1	Perímetro de Seguridad Física	No	No se define en el alcance
		9.1.2	Controles Físicos de Entrada	No	No se define en el alcance
		9.1.3	Seguridad de oficinas, despachos e instalaciones.	No	No se define en el alcance
		9.1.4	Protección contra las amenazas externas y de origen ambiental	No	Preocupación por la integridad de los equipos de recolección y transmisión de datos.
		9.1.5	Trabajo en áreas seguras.	No	No se define en el alcance
		9.1.6	Áreas de acceso al público y de carga y descarga	No	No se define en el alcance
9.2	Seguridad de los Equipos.	9.2.1	Ubicación y protección de los equipos	Si	Posible manipulación de los equipos por terceros.
		9.2.2	Instalación de suministro	Si	Asegurar el funcionamiento de los equipos de transmisión de datos ante cortes de energía eléctrica
		9.2.3	Seguridad del cableado	Si	Preocupación de la Gerencia por la pérdida de enlace con los equipos recolectores de información.
		9.2.4	Mantenimiento de los equipos	Si	Mantener la continuidad de los servicios que ofrece.
		9.2.5	Seguridad de los equipos fuera de las instalaciones	No	No se define en el alcance
		9.2.6	Reutilización o retirada segura de los equipos	No	No se define en el alcance
		9.2.7	Retirada de materiales propiedad de la empresa	No	No se define en el alcance

Dominio: Gestión de las comunicaciones y operaciones.

10 Gestión de las comunicaciones y operaciones					
Estándar	**Objetivo**		**Controles**	**Aplica (Si/No)**	**Justificación de la Ejecución**
10.1	Procedimientos Operacionales y Responsabilidades	10.1.1	Documentos de procedimientos de operación.	Si	Revisar la documentación de la operación del sistema Energy Axis.
		10.1.2	Gestión de Cambios	Si	Revisar procedimientos para gestionar los cambios.
		10.1.3	Segregación de funciones	Si	No se define en el alcance
		10.1.4	Separación de las instalaciones de desarrollo, prueba y operación	Si	No hay ambiente de desarrollo, ni pruebas.
10.2	Gestión de la entrega del servicio de terceros.	10.2.1	Provisión del servicio	Si	Revisar los controles de seguridad, definiciones y niveles de servicio del proveedor de enlace de datos.
		10.2.2	Monitoreo y revisión de los servicios de terceros	Si	Revisar los niveles de servicios, revisar los aspectos de seguridad.
		10.2.3	Manejo de cambios en los servicios de terceros	Si	Revisar la coordinación de los cambios de ubicación entre la organización y terceros.
10.3	Planeación y aceptación del sistema	10.3.1	Gestión de la capacidad	No	No se define en el alcance
		10.3.2	Aceptación del sistema	No	No se define en el alcance
10.4	Protección contra el código malicioso y móvil	10.4.1	Controles contra códigos maliciosos	Si	Revisar la protección contra riesgos asociados a archivos maliciosos.
		10.4.2	Controles contra códigos móviles	Si	Revisar la integridad de la información que pasa de la Base de Datos de Telemetría a la Base de Datos del Sistema Comercial de la Empresa.
10.5	Respaldo o Back-Up	10.5.1	Copias de seguridad de información	Si	Revisar los controles para asegurar la disponibilidad de la información.
10.6	Gestión de seguridad de la red	10.6.1	Controles de redes	Si	Revisar el control de accesos a los servicios de la red.
		10.6.2	Seguridad de los servicios de red	Si	Revisar le ancho de banda y equipos de seguridad.

10 Gestión de las comunicaciones y operaciones					
Estándar	**Objetivo**		**Controles**	**Aplica (Si/No)**	**Justificación de la Ejecución**
10.7	Gestión de medios	10.7.1	Gestión de medios removibles	No	No se define en el alcance
		10.7.2	Retirada de Soportes	No	No se define en el alcance
		10.7.3	Procedimientos de manipulación de la información.	No	No se define en el alcance
		10.7.4	Seguridad de la documentación del sistema.	No	No se define en el alcance
10.8	Intercambio de información.	10.8.1	Políticas y procedimientos de intercambio de información.	No	No se define en el alcance
		10.8.2	Acuerdos de intercambio.	No	No se define en el alcance
		10.8.3	Soportes físicos en tránsito.	No	No se define en el alcance
		10.8.4	Mensajería electrónica.	No	No se define en el alcance
		10.8.5	Sistemas de información empresariales.	No	No se define en el alcance
10.9	Servicios de comercio electrónico.	10.9.1	Comercio electrónico.	No	No se define en el alcance
		10.9.2	Transacciones en línea.	Si	
		10.9.3	Información públicamente disponible.	No	No se define en el alcance
10.10	Supervisión.	10.10.1	Registros de auditoría.	Si	Revisar si el proceso cuenta con registros para revisiones en caso de un incidente.
		10.10.2	Supervisión del uso del sistema.	Si	Revisar el correcto uso de los recursos del sistema.
		10.10.3	Protección de la información de los registros.	Si	Revisión considerada en el alcance.
		10.10.4	Registros de administración y operación.	Si	Revisión considerada en el alcance.
		10.10.5	Registro de fallos.	Si	Revisión considerada en el alcance.
		10.10.6	Sincronización del reloj.	Si	Revisión considerada en el alcance.

Dominio: Control de Acceso.

11 Control de Acceso					
Estándar	**Objetivo**		**Controles**	**Aplica (Si/No)**	**Justificación de la Ejecución**
11.1	Requisitos de negocio para el control de acceso.	11.1.1	Política de control de acceso.	Si	
11.2	Gestión de acceso de usuario.	11.2.1	Registro de usuario.	No	No se define en el alcance
		11.2.2	Gestión de privilegios.	Si	Verificar la existencia de perfiles de uso establecidos.
		11.2.3	Gestión de contraseñas de usuario.	Si	Verificar la existencia de políticas en el uso de contraseñas.
		11.2.4	Revisión de los derechos de acceso de usuario.	Si	Verificar la existencia de perfiles de uso establecidos.
11.3	Responsabilidades de usuario.	11.3.1	Uso de contraseñas.	No	No se define en el alcance
		11.3.2	Equipo de usuario desatendido.	No	No se define en el alcance
		11.3.3	Política de puesto de trabajo despejado y pantalla limpia.	No	No se define en el alcance
11.4	Control de acceso a la red.	11.4.1	Política de uso de los servicios en red.	Si	Revisar las actividades existentes para el control del uso de la red.
		11.4.2	Autenticación de usuario para conexiones externas.	Si	Verificar los controles para permitir la conexión de usuarios vía VPN
		11.4.3	Identificación de los equipos en las redes.	No	No se define en el alcance
		11.4.4	Protección de los puertos de diagnóstico y configuración remotos.	Si	Confirmar que solo se encuentren habilitados los puertos requeridos por los sistemas de gestión.
		11.4.5	Segregación de las redes.	No	No se define en el alcance
		11.4.6	Control de la conexión a la red.	No	No se define en el alcance
		11.4.7	Control de encaminamiento (routing) de red.	No	No se define en el alcance

11 Control de Acceso					
Estándar	**Objetivo**		**Controles**	**Aplica (Si/No)**	**Justificación de la Ejecución**
11.5	Control de acceso al sistema operativo.	11.5.1	Procedimientos seguros de inicio de sesión.	Si	Verificar la existencia de procedimientos.
		11.5.2	Identificación y autenticación de usuario.	Si	Constatar la existencia de procedimientos y controles.
		11.5.3	Sistema de gestión de contraseñas.	Si	Revisar el procedimiento para asignación de contraseñas.
		11.5.4	Uso de los recursos del sistema.	No	No se define en el alcance
		11.5.5	Desconexión automática de sesión.	No	No se define en el alcance
		11.5.6	Limitación del tiempo de conexión.	No	No se define en el alcance
11.6	Control de acceso a las aplicaciones y a la información.	11.6.1	Restricción del acceso a la información.	Si	Revisar si existen restricciones a la información que se maneja en telemetría.
		11.6.2	Aislamiento de sistemas sensibles.	Si	Verificar el ambiente de procesamiento de los sistemas de telemetría.
11.7	11.7 Ordenadores portátiles y teletrabajo.	11.7.1	Ordenadores portátiles y comunicaciones móviles.	No	No se define en el alcance
		11.7.2	Teletrabajo.	No	No se define en el alcance

Tabla 3.3 Justificación de aplicabilidad

Los parámetros establecidos en las tablas de aplicabilidad se han definidos en base a los requerimientos de las Gerencia Comercial Operativa y al alcance del proyecto.

Capítulo 4

4. Análisis de riesgo.

4.1 Definición de análisis de riesgo.

Es el estudio de las causas de las posibles amenazas y probables eventos no deseados y los daños y consecuencias que éstas puedan producir.

Este tipo de análisis es ampliamente utilizado como herramienta de gestión y de seguridad para identificar riesgos ya sean con métodos cualitativo y cuantitativos.

El primer paso del análisis es identificar los activos a proteger o evaluar. La evaluación de riesgos involucra comparar el nivel de riesgo detectado durante el proceso de análisis con criterios de riesgo establecidos previamente.

La función de la evaluación consiste en ayudar a alcanzar un nivel razonable de consenso en torno a los objetivos en cuestión, y asegurar un nivel mínimo que permita desarrollar indicadores operacionales a partir de los cuales medir y evaluar.

Los resultados obtenidos del análisis, van a permitir aplicar alguno de los métodos para el tratamiento de los riesgos, que involucra identificar el conjunto de opciones que existen para tratar los riesgos, evaluarlas, preparar planes para este tratamiento y ejecutarlos.

4.2 Objetivos del análisis del riesgo.

El objetivo del análisis de de riesgo enfocado en las tecnologías de la información:

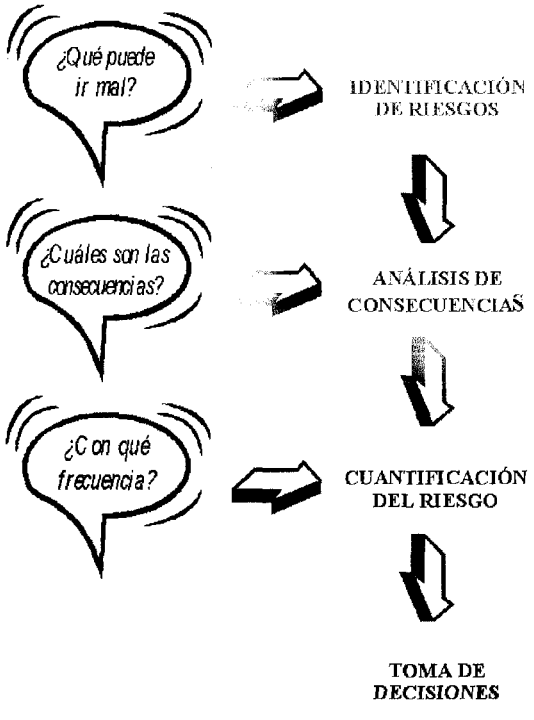
- Identificar y medir los riesgos que representa una instalación industrial para las personas, el medio ambiente y los bienes materiales.
- Deducir los posibles eventos graves que pudieran materializarse.

- Determinar las consecuencias en el espacio y el tiempo de las amenazas, aplicando determinados criterios de vulnerabilidad.
- Analizar las causas de las amenazas.
- Definir medidas y procedimientos de prevención y protección para evitar que una amenaza se materialice o limitar las consecuencias de las mismas.

4.3 Aspectos a tratar en los análisis de riesgos.

Los aspectos de un análisis de riesgos implica desde el punto de vista de la prevención de incidentes, están íntimamente relacionados con los siguientes ítems:

- Identificación de sucesos no deseados, que pueden conducir a la materialización de una amenaza.
- Análisis de las vulnerabilidades.
- Valoración de las consecuencias y de la frecuencia con que estos sucesos pueden producirse.



4.4 Clasificación de riesgos de TI.

4.4.1 Riesgo de integridad.

Son los riesgos que inciden en la exactitud de la información, trasmisión, recepción, procesamiento y emisión de reportes que se realizan a través de las aplicaciones utilizadas por las organizaciones. Es necesario revisar lo siguiente:

- Usuarios: riesgo en mala asignación de perfiles individuales y de grupo según sus funciones y obligaciones.
- Procesamiento: controles inadecuados tanto preventivos como detectivos que ponen en riesgo el procesamiento de la data y posterior obtención de información confiable.
- Cambios: La falta de control en cambios a realizarse en aplicativos o infraestructura puede derivar en fallas o colapso del sistema.

4.4.2 Riesgo de acceso.

El inapropiado control de acceso al sistema e infraestructura que comprometen la integridad de la información poniendo en riesgo la integridad, confiabilidad y disponibilidad de la información.

- Entorno de procesamiento: mal manejo de los accesos inapropiados en aplicativos e información.
- Redes: acceso no autorizado a la red de datos y riesgo de cambios o daños el sistema o información.
- Físico: falta de protección a los equipos que intervienen en lo procesos.

4.4.3 Riesgo de utilidad.

Se debe tener en cuenta lo siguiente:

- Técnicas de recuperación de incidentes para minimizar el impacto en el caso de que un evento se materialice.
- Procedimientos para respaldos y planes de contingencia para recuperación en casos de desastres.

4.4.4 Riesgo de infraestructura.

Falta de infraestructura para soportar adecuadamente las necesidades actuales y futuras de una organización entre estos comprenden: hardware, software, redes y la administración de estos recursos.

4.5 Estructura del análisis de riesgo.

La realización de un análisis de riesgos implica componentes básicos: identificación de peligros, evaluación de riesgos (que puede realizarse desde un punto de vista cuantitativo o cualitativo), gestión de riesgo y comunicación de riesgos, debemos que tener en cuenta los siguientes puntos:

- Identificar de riesgos de la organización.
- Determinar los riesgos de mayor severidad y que puedan derivar en mayor impacto sobre los activos de la organización.
- Establecer controles que permitan mitigar los riesgos más severos.

Identificación de los peligros: hay que conocer las amenazas en el proceso que se revisa y este trabajo se lo debe hacer de forma permanente debido a que todos los días nos exponemos a nuevos riesgos internos, externos o inherentes.

Evaluación de los riesgos: se tiene que determinar y clasificar el riesgo de acuerdo a su severidad, calcular la probabilidad de que ocurra y finalmente determinar su impacto.

Controles: después de la evaluación de los riesgos hay que desarrollar controles e implementarlos con el fin de mitigar o aislar su impacto en la organización.

4.6 Análisis de riesgo para la Empresa Eléctrica de Guayaquil – Proceso de Telemetría.

Una vez establecidos los controles que son aplicables al proceso de telemetría, las mismas que han sido aceptadas por el gerente de la Gerencia Comercial Operativa Ing. Diego Sánchez y el jefe del Área de Telemetría Ing. Geovanny Ramírez procederemos con la revisión, identificación, análisis y evaluación de los riesgos en base a los siguientes dominios de la norma ISO 27002:2005:

- Seguridad física y ambiental.
- Gestión de comunicación y operaciones.
- Control de acceso.

4.6.1 Objetivos del análisis de riesgo.

Determinar los riesgos y nivel de criticidad existentes en las TI que intervienen en el proceso de telemetría basados en los dominios aplicados en la revisión de seguridades de la información.

4.6.2 Identificación de los riesgos.

Los riegos son identificados en base a los hallazgos del Checklist elaborado para la revisión de las actividades del proceso de telemetría en las cuales intervienen las tecnologías de información.

Dentro de los dominios seleccionados se establecieron cubrir 35 de 133 controles existentes y que son aplicables en la revisión a realizarse.

Dominios	Controles
Seguridad física y ambiental	4
Gestión de comunicaciones y operaciones	19
Control de accesos	12
Total	**35**

Tabla 4.1 Controles aplicados en la revisión

Dominio:	9 SEGURIDAD FÍSICA Y AMBIENTAL.			
Objetivo:	Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización.			
Control:	9.2 SEGURIDAD DE LOS EQUIPOS.			
Controles	**Preguntas de Auditoria**	**Cumple (Si/No)**	**Hallazgos**	**Riesgo**
Instalación de suministro	¿Los equipos de recolección de datos (transceiv*ers*) cuentan con un respaldo de energía en caso de falta del suministro eléctrico Ej. UPS?	Si	Cada tranceivers se encuentra respaldado con un UPS de 750 VA con una autonomía de 18 a 25 minutos.	
	¿Los equipos de recolección de datos (*gatekeepers*) cuentan con un respaldo de energía en caso de falta del suministro eléctrico Ej. UPS?	Si	Cada equipo posee su propio sistema de respaldo de energía con una autonomía de 10 horas.	
Seguridad del cableado	¿El cableado de fibra óptica que da enlace a los gatekeepers tiene un adecuado tendido Ej. Tensión correcta del cable, tendido subterráneo, etc.?	No	El tendido de fibra óptica de la empresa que provee el servicio de enlace de datos pasa por postes de alumbrado público.	Existe el riesgo de que le poste pueda ser derribado por colisión de un vehículo o la caída de un árbol ya que se encuentran a lado de las calles.
Mantenimiento de los equipos	¿Se cuenta con un documento del cronograma detallado de actividades y tiempos de mantenimiento de los equipos?	No	No existe el documento ni el plan de mantenimiento de los equipos.	Existe el riesgo de falla o avería de los equipos por falta de mantenimiento.

Dominio:	9 SEGURIDAD FISICA Y AMBIENTAL.			
Objetivo:	Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización.			
Control:	9.2 SEGURIDAD DE LOS EQUIPOS.			
Controles	**Preguntas de Auditoria**	**Cumple (Si/No)**	**Hallazgos**	**Riesgo**
Ubicación y protección de los equipos	¿Se encuentran los equipos de conversión de medios (*transceivers Ethernet - Fibra óptica*) instalados en una ubicación segura?.	No	Los tranceivers se encuentran instalados sobre los postes de alumbrado público a 9 metros de altura en cajas anti-hurto eléctricas, sin embargo existen riesgos implícitos.	Existe el riesgo de acceso por parte de personas no autorizadas. Existe el riesgo de que el poste pueda ser derribado por colisión de un vehículo o la caída de un árbol ya que se encuentran a lado de las calles.
	¿Se encuentran los equipos de recolección de datos (*gatekeepers*) instalados en una ubicación segura?.	No	Los gatekeepers se encuentran instalados sobre los postes de alumbrado público a 18 metros de altura.	Existe el riesgo de que el poste pueda ser derribado por colisión de un vehículo o la caída de un árbol ya que se encuentran a lado de las calles.
	¿Se encuentran los equipos de recolección de datos (gatekeepers) protegidos de amenazas potenciales como: los efectos del entorno (Sol, viento, lluvia), manipulación, robo, vandalismo, etc.?	Si	Los gatekeepers han sido diseñados para funcionar en entornos hostiles, tiene una caja de protección de sus partes sensibles de fábrica y a la altura que se encuentran solo se puede acceder con carro canasta. *Anexo 3.*	
	¿Se encuentran los equipos de conversión de medios (transceivers Ethernet - Fibra óptica) protegidos de amenazas potenciales como: los efectos del entorno (Sol, viento, lluvia), manipulación, robo, vandalismo, etc.?	Si	Los tranceivers se encuentran protegidos dentro de una caja metálica y con cerradura anti-hurto, lo cual la protege contra amenazas del medioambiente.	

Objetivo:	Asegurar la operación correcta y segura de los medios de procesamiento de la información.			
Control:	10.1 RESPONSABILIDADES Y PROCEDIMIENTOS DE OPERACIÓN.			
Controles	**Preguntas de Auditoria**	**Cumple (Si/No)**	**Hallazgos**	**Riesgo**
Documentación de procedimientos de operación.	¿Se cuenta con documentación con procedimientos de reinicio y recuperación del sistema para su uso en el evento de una falla en el sistema?	No	No existe documentación de los procedimientos.	En caso de que falten las personas que conocen el procedimiento, no se tendrá información de cómo hacerlo.
	¿Se cuenta con la documentación de los procedimientos y manejo de información?	No	No existe documentación de los procedimientos, la información la maneja una sola persona.	Se dependería de una sola persona en el proceso.
	¿Se cuenta con documentación de contactos de soporte en el evento de dificultades operacionales o técnicas?	Si	Si se cuenta con la documentación de contactos de personal de las empresas proveedoras del servicio.	
Gestión de cambios.	¿Se tiene un control del procedimiento de aprobación formal de cambios de equipos o de configuración?	No	Existe un procedimiento pero no se encuentra documentado, y los cambios se dan en función de la demanda de equipos.	En caso de que falten las personas que conocen el procedimiento, no se tendrá información de cómo hacerlo.
Segregación de funciones.	¿Se tiene una segregación de funciones del personal perteneciente al proceso de telemetría?	Si	Existe segregación de funciones y responsabilidades mediante perfiles de cada persona incluyendo al administrador del Servidor EA_MS (Energy Axis). *Anexo 4.*	
Separación de las instalaciones de desarrollo, prueba y operación	¿La organización posee secciones de desarrollo, pruebas y producción las cuales se encuentren separadas física y funcionalmente?	No	No existen ambientes de desarrollo, pruebas y producción separada. El desarrollo es in-house y las pruebas se la realizan en el servidor de producción.	Existe el riesgo de falla en las pruebas lo cual podría comprometer la operación del proceso.

Dominio:	10 GESTIÓN DE COMUNICACIONES Y OPERACIONES.			
Control:	10.2 GESTIÓN DE LA PROVISIÓN DE SERVICIOS POR TERCEROS.			
Objetivo:	Implementar y mantener el nivel apropiado de seguridad de la información y la entrega del servicio en línea con los acuerdos de entrega de servicios de terceros.			
Controles	**Preguntas de Auditoria**	**Cumple (Si/No)**	**Hallazgos**	**Riesgo**
Provisión del servicio	¿Se tienen establecidos en los contratos con las empresas proveedora de enlace de datos acuerdos de seguridad y niveles de calidad del servicio?	Si	Actualmente se tienen acuerdos de servicio, sin embargo se tienen enlaces de contingencia para superar los inconvenientes que se presenten.	
Monitoreo y revisión de los servicios de terceros	¿Se tiene implementado en la empresa un sistema de monitoreo para verificar niveles de desempeño?	Si	Existen registros históricos de monitoreo de incidentes con el enlace de datos.	
	¿Se revisa los rastros de auditoría y registros de eventos relacionadas con el servicio entregado por proveedor del enlace de datos?.	Si	Se utiliza un software para el monitoreo y emisión de alarmas.	
	¿La empresa proveedora del servicio de enlace de datos a designado a una persona responsable de la revisión y cumplimiento de requerimientos del contrato?.	Si	Se tiene un ejecutivo de cuenta y un técnico personalizados que atienden todos los requerimientos.	
Manejo de cambios en los servicios de terceros	¿Se tienen establecidos procedimientos para manejar cambios en la provisión del servicio de enlace de datos con el proveedor. Ej.: aumento de ancho de banda, reubicación de gatekeepers, cambios y mejoras en las redes, cambios a implementar por parte del proveedor, etc.?.	Si	Existen procedimientos que se siguen con el proveedor principal de enlaces, pero con el proveedor de contingencia no se lo tiene documentado.	

Dominio:	10 GESTIÓN DE COMUNICACIONES Y OPERACIONES.			
Control:	10.4 PROTECCIÓN CONTRA CODIGO MALICIOSO Y DESCARGABLE.			
Objetivo:	Proteger la integridad del software y la integración.			
Controles	**Preguntas de Auditoria**	**Cumple (Si/No)**	**Hallazgos**	**Riesgo**
Controles contra códigos maliciosos	¿Se tiene instalado software de prevención, detección y reparación o eliminación de código malicioso debidamente actualizado en los computadores de la empresa?	Si	Se tiene un servidor de antivirus, y el software está instalado en servidores y computadores con parametrización de las políticas de protección por parte del administrador del servicio vía consola.	
Controles contra códigos móviles	¿Se valida la integridad de los archivos XML en la transferencia de los mismos entre los servidores de Telemetría y Sistema Comercial?	Si	Los archivos son tomados directamente del servidor, además de tener controles internos para seguridad. Anexo 5.	

Dominio:	10 GESTIÓN DE COMUNICACIONES Y OPERACIONES.			
Control:	10.5 COPIAS DE SEGURIDAD.			
Objetivo:	Mantener la integridad y disponibilidad de la información y los medios de procesamiento de información.			
Controles	**Preguntas de Auditoria**	**Cumple (Si/No)**	**Hallazgos**	**Riesgo**
Copias de seguridad de información	¿Se realizan respaldos (*verificación del mismo*) de la data de telemetría en cintas y se los almacena en un lugar apartado a la distancia suficiente en caso de desastre en el local principal?	No	No existe una política definida para el respaldo para la información de telemetría en medios magnéticos.	Existe el riesgo de afectar la continuidad del negocio en el posible evento de un desastre en el edificio principal.

Dominio:	10 GESTIÓN DE COMUNICACIONES Y OPERACIONES.			
Control:	10.6 GESTIÓN DE LA SEGUIRIDAD DE LAS REDES.			
Objetivo:	Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.			
Controles	**Preguntas de Auditoria**	**Cumple (Si/No)**	**Hallazgos**	**Riesgo**
Controles de redes	¿Se tiene separada las responsabilidades de redes y operaciones?	Si	Existe una separación definida la separación de operaciones de redes y computacionales tanto en personal como en funciones.	
	¿Los datos que se adquieren y se transmiten a los equipos de telemetría a través de la red LAN y WAN guardan su confidencialidad e integridad?	Si	Se utiliza un algoritmo de encriptación avanzado AES-128. Se encripta la data en el gatekeeper y se lo desencripta en el servidor Energy Axis. Anexo 6.	
	¿Se han establecido acuerdos de seguridad con el proveedor del servicio de transmisión de datos?.	Si	Los datos encapsulados y aislados por medio de VRF - MPLS.	
Seguridad de los servicios de red	¿Se tienen protecciones contra accesos no autorizados y/o ataques de terceros?.	Si	Se tiene implementado un sistema de prevención y detección de intrusos IDS e IPS con equipos de borde de la red local para la protección de accesos externos e internos además de 2 firewalls. *Anexo 7.*	

Control:	*10.9 SERVICIOS DE COMERCIO ELECTRÓNICO.*			
Objetivo:	Asegurar la seguridad de los servicios de comercio electrónico y su uso seguro.			
Controles	**Preguntas de Auditoria**	**Cumple (Si/No)**	**Hallazgos**	**Riesgo**
Transacciones en línea.	¿Los equipos que intervienen en las transacciones ejecutados por el proceso de telemetría, utilizan protocolos de comunicación seguros?.	Si	Toda información y transacción hacia o desde el medidor del servicio eléctrico utiliza el protocolo ANSI C12.22 y utiliza el cifrado AES-128. (Anexo 3)	

Dominio:	10 GESTIÓN DE COMUNICACIONES Y OPERACIONES.			
Control:	10.10 SERVICIOS DE COMERCIO ELECTRÓNICO.			
Objetivo:	Detectar las actividades de procesamiento de información no autorizadas.			
Controles	**Preguntas de Auditoria**	**Cumple (Si/No)**	**Hallazgos**	**Riesgo**
Registros de auditoría.	¿El sistema de gestión de telemetría (Energy Axys) guarda registros de auditoría de las actividades excepciones y eventos de seguridad de la información por un periodo de tiempo?	Si	Los registros son permanentes, pero no se los está respaldando, al momento está utilizado el 20% de espacio de almacenamiento total, y la tasa de crecimiento anual es del 5% del total utilizado (20%). *Anexo 8.*	
	¿El administrador del sistema Energy Axys tiene privilegios para borrar o desactivar los registros de sus propias actividades?	Si	No hay manera de alterar los registros desde la aplicación, todo queda registrado.	

Control:	10.10 SERVICIOS DE COMERCIO ELECTRÓNICO.			
Objetivo:	Detectar las actividades de procesamiento de información no autorizadas.			
Controles	**Preguntas de Auditoria**	**Cumple (Si/No)**	**Hallazgos**	**Riesgo**
Supervisión del uso del sistema.	¿Se tiene procedimientos de monitoreo para asegurar que los usuarios realicen solo realicen las actividades que ha sido autorizados hacer?	Si	La aplicación tiene perfiles de usuario, y autorizaciones para cada tipo; por lo que solo pueden realizar lo que tengan autorizado.	
Protección de la información de los registros.	¿Se protegen los registros contra manipulación y acceso no autorizado?	Si	Todo cambio y/o modificación se la tiene que gestionar con el proveedor y realizarla vía remota desde Estados Unidos. No hay manera de manipular los registros desde la aplicación.	
Registros de administración y operación.	¿Se registran las actividades del administrador y operador del sistema?.	Si	Si se guardan los registros de las actividades de todos los usuarios del Energy Axis y se los puede revisar con la opción de Auditoria que se encuentra embebido en el aplicativo e gestión. *Anexo 9.*	
Registro de fallos.	¿Se encuentra activada la función de registro de errores?.	Si	Si se encuentra activada esta función, el personal es notificado mediante aviso y proceden con la solución de la falla.	
Sincronización del reloj.	¿Los equipos de telemetría se encuentran sincronizados con la hora del servidor?	Si	Todos los equipos se encuentran sincronizados con el servidor.	

Dominio:	11 CONTROL DE ACCESO.			
Control:	11.1 REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO.			
Objetivo:	Controlar el acceso a la información.			
Controles	**Preguntas de Auditoria**	**Cumple (Si/No)**	**Hallazgos**	**Riesgo**
Política de control de acceso.	¿Se cuenta con políticas debidamente documentadas para el control de acceso lógicos y el detalle de los perfiles de usuarios?	No	Se aplican políticas y criterios para el control de acceso, pero no existen documentos de respaldo.	Existe el riesgo de no establecer correctamente los perfiles de acceso.
	¿Los equipos de procesamiento de telemetría están protegidos por controles de acceso físicos?	Si	Los equipos se encuentran en el Centro de Cómputo dentro del Departamento de Tecnología. Hay dos controles de acceso de validación con tarjeta magnética uno en la entrada al área de tecnología y otro en la puerta blindada del Centro de Computo.	

Dominio:	11 CONTROL DE ACCESO.			
Control:	11.2 GESTIÓN DE ACCESO DE USUARIO.			
Objetivo:	Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información.			
Controles	**Preguntas de Auditoria**	**Cumple (Si/No)**	**Hallazgos**	**Riesgo**
Gestión de privilegios.	Se debiera restringir y controlar la asignación y uso de privilegios sobre la base de "solo lo que necesita saber" y los requerimientos mínimos para su rol funcional.	Si	Se asigna perfiles a los usuarios de los servicios de la aplicación de forma individual.	
Gestión de contraseñas de usuario.	¿En la asignación de contraseñas, se controla a través de un proceso de gestión en la que el usuario tenga que firmar un enunciado para mantener la confidencialidad de las claves secretas que se les proporciona temporalmente y estar obligados a cambiarla inmediatamente?	No	La solicitud de contraseñas se las realiza vía correo electrónico desde la Jefatura de Telemetría al administrador del aplicativo y la respuesta es por la misma vía, el usuario no firma documentos de confidencialidad.	Se podría hacer mal uso de las credenciales de autenticación por parte de personal mal intencionado o no pertenecientes a la empresa.
Revisión de los derechos de acceso de usuario.	¿Los derechos de usuario se los revisa regularmente, después de una modificación de privilegios o terminación del empleo de la persona?	No	No existe un proceso establecido	Existe el riesgo que ese acceso este siendo utilizado por otro usuario.

Dominio:	11 CONTROL DE ACCESO.			
Control:	11.4 CONTROL DE ACCESO A LA RED.			
Objetivo:	Evitar el acceso no autorizado a los servicios de la red.			
Controles	**Preguntas de Auditoria**	**Cumple (Si/No)**	**Hallazgos**	**Riesgo**
Política de uso de los servicios en red.	¿Se ha establecido perfiles a los usuarios de telemetría por parte del administrador del directorio activo para acceder a los servicios de red?	Si	Se asigna perfiles a los usuarios de los servicios de red de forma individual y por grupos.	
Autenticación de usuario para conexiones externas.	¿La autenticación de las conexiones vía VPN son validadas?.	Si	Se realiza por medio de Firewall principal y software cliente para conexión.	
Protección de los puertos de diagnóstico y configuración remotos.	¿Se tienen definidos los puertos de configuración para equipos de telemetría?	Si	Se tiene bloqueado todos los puertos y excepto lo habilitados para el uso exclusivo del aplicativo.	

Dominio:	11 CONTROL DE ACCESO.			
Control:	11.5 CONTROL DE ACCESO AL SISTEMA OPERATIVO.			
Objetivo:	Evitar el acceso no autorizado a los sistemas operativos.			
Controles	**Preguntas de Auditoria**	**Cumple (Si/No)**	**Hallazgos**	**Riesgo**
Procedimientos seguros de inicio de sesión.	¿Se cuenta con un procedimiento de autenticación de usuarios con controles de intentos fallidos y su debido registro?.	Si	Todas las maquinas están bajo dominio y son administradas por directorio activo en donde se encuentran parametrizadas las opciones de seguridad.	
Identificación y autenticación de usuario.	¿Se utiliza ID diferente para cado uno de los usuarios?	Si	Cada usuario tiene un ID único.	
Sistema de gestión de contraseñas.	¿Cada usuario tiene asignada una contraseña única junto con su ID?	Si	Cada usuario tiene un ID y contraseña única.	

Dominio:	11 CONTROL DE ACCESO.			
Control:	11.6 CONTROL DE ACCESO A LAS APLICACIONES Y A LA INFORMACIÓN.			
Objetivo:	Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.			
Controles	**Preguntas de Auditoria**	**Cumple (Si/No)**	**Hallazgos**	**Riesgo**
Restricción del acceso a la información.	¿Se establecen los accesos al sistema de telemetría a través de una política de accesos en base a perfiles de usuario?.	Si	Se asigna perfiles a los usuarios de la aplicación de forma individual.	
Aislamiento de sistemas sensibles.	¿El sistema de telemetría comparte el ambiente de procesamiento con otros sistemas?	Si	El sistema EA_MS tiene su propio ambiente de procesamiento de forma individual.	

4.6.3 Evaluación del riesgo.

La evaluación de riesgos es una herramienta indispensable en la actividad preventiva, mediante la cual se obtiene la información precisa para determinar las decisiones apropiadas en orden a adoptar las medidas necesarias de prevención de riesgos, estableciendo las prioridades que correspondan.

La evaluación de riesgos es en sí misma una actividad preventiva, debido a que se identifica los factores de riesgo para prever los posibles daños y su magnitud y así poder elegir los medios para eliminarlos o minimizarlos.

4.6.4 Probabilidad de ocurrencia.

La asignación de un valor definido para el cálculo de la probabilidad no se encuentra definido pero para nuestro trabajo estableceremos los siguientes valores en la tabla detallada a continuación.

Clasificación	Probabilidad
Muy Alto	4
Medio Alto	3
Medio Bajo	2
Muy bajo	1

Tabla 4.2 Clasificación de Probabilidad

4.6.5 Nivel de impacto.

No existe un estándar definido para establecer el impacto de un riesgo pero asignaremos una escal de valores los cuales serán asignados en nuestro trabajo dependiendo de la magnitud del riesgo como afecte este al proceso.

Clasificación	Probabilidad
Alta	3
Media	2
Baja	1

Tabla 4.3 Clasificación del Impacto.

4.6.6 Criticidad.

El valor de la criticidad será el resultado de la probabilidad de ocurrencia por el nivel de impacto, como se detalla a continuación:

Criticidad = Probabilidad x Impacto

Para asignar el nivel de criticidad estableceremos un rango una vez que sabemos que la puntuación máxima es 12 y la mínima 1, el rango para la criticad baja estará en desde el 9% al 35% del valor máximo, el valor medio se lo asignara desde el 36% al 70% y la alta criticidad a partir del 71 % al 100%.

Nivel de Criticidad	Nomenclatura	Mínimo	Máximo
Alta	A	8	12
Media	M	5	7
Baja	B	1	4

Tabla 4.4 Niveles de Criticidad

4.6.7 Calculo y asignacion del nivel de riesgo y criticidad.

En las tablas que a continuación se detallan procedemos a valorar los riesgos y determinar el nivel de criticidad.

Dominio:	9 SEGURIDAD FÍSICA Y AMBIENTAL.				
Objetivo:	Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización.				
Control:	9.2 SEGURIDAD DE LOS EQUIPOS.				
Controles	**Riesgo**	**Probabilidad**	**Impacto**	**Nivel de Riesgo**	**Criticidad**
Ubicación y protección de los equipos	Existe el riesgo de acceso por parte de personas no autorizadas.	2	3	**3**	**Media**
	Existe el riesgo de que el poste pueda ser derribado por colisión de un vehículo o la caída de un árbol ya que se encuentran a lado de las calles.	2	3	**6**	**Media**
	Existe el riesgo de que el poste pueda ser derribado por colisión de un vehículo o la caída de un árbol ya que se encuentran a lado de las calles.	2	3	**6**	**Media**
Seguridad del cableado	Existe el riesgo de que le poste pueda ser derribado por colisión de un vehículo o la caída de un árbol ya que se encuentran a lado de las calles.	2	3	**6**	**Media**
Mantenimiento de los equipos	Existe el riesgo de falla o avería de los equipos por falta de mantenimiento.	3	3	**9**	**Alta**

Dominio:	10 GESTIÓN DE COMUNICACIONES Y OPERACIONES.				
Objetivo:	Asegurar la operación correcta y segura de los medios de procesamiento de la información.				
Control:	10.1 RESPONSABILIDADES Y PROCEDIMIENTOS DE OPERACIÓN.				
Controles	**Riesgo**	**Probabilidad**	**Impacto**	**Nivel de Riesgo**	**Criticidad**
Documentación de procedimientos de operación.	En caso de que falten las personas que conocen el procedimiento, no se tendrá información de cómo hacerlo.	3	3	9	**Alta**
	Se dependería de una sola persona en el proceso.	4	3	12	**Alta**
Gestión de cambios.	En caso de que falten las personas que conocen el procedimiento, no se tendrá información de cómo hacerlo.	3	3	9	**Alta**
Separación de las instalaciones de desarrollo, prueba y operación	Existe el riesgo de falla en las pruebas lo cual podría comprometer la operación del proceso.	4	3	12	**Alta**

Dominio:	10 GESTIÓN DE COMUNICACIONES Y OPERACIONES.				
Control:	10.5 COPIAS DE SEGURIDAD.				
Objetivo:	Mantener la integridad y disponibilidad de la información y los medios de procesamiento de información.				
Controles	**Riesgo**	**Probabilidad**	**Impacto**	**Nivel de Riesgo**	**Criticidad**
Copias de seguridad de información	Existe el riesgo de afectar la continuidad del negocio en el posible evento de un desastre en el edificio principal.	3	3	9	**Alta**

Dominio:	11 CONTROL DE ACCESO.				
Control:	11.1 REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO.				
Objetivo:	Controlar el acceso a la información.				
Controles	**Riesgo**	**Probabilidad**	**Impacto**	**Nivel de Riesgo**	**Criticidad**
Política de control de acceso.	Existe el riesgo de no establecer correctamente los perfiles de acceso.	3	3	9	**Alta**

Dominio:	11 CONTROL DE ACCESO.				
Control:	11.2 GESTIÓN DE ACCESO DE USUARIO.				
Objetivo:	Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información.				
Controles	**Riesgo**	**Probabilidad**	**Impacto**	**Nivel de Riesgo**	**Criticidad**
Gestión de contraseñas de usuario.	Se podría hacer mal uso de las credenciales de autenticación.	2	3	6	**Media**
Revisión de los derechos de acceso de usuario.	Existe el riesgo que ese acceso este siendo utilizado por otro usuario.	4	3	9	**Alta**

Capitulo 5

5. Conclusiones y Recomendaciones.

5.1 Conclusiones

Durante la revisión efectuada al proceso de Telemetría se evidenció falta de documentación en cuanto a políticas y procedimientos.

También llamó la atención que en los procedimientos de operación para la configuración de medidores AMI, hay un nivel de riesgo Alto, debido a que una sola persona conoce las claves de acceso, configuración y procedimientos para hacerlo.

Según la evaluación, se tuvo como resultado un riesgo medio (con valor de 5 puntos en una escala del 1 al 12).

Sería importante que se determine en una revisión posterior el nivel de riesgo que la Eléctrica de Guayaquil asumirá en el proyecto de Telemetría, a fin de que cuando se concrete el plan de expansión se asegure de forma razonable la operatividad del proceso de Telemetría y sus actividades de lectura, corte y reconexión, y facturación remota.

Cabe indicar que se evidencio falta de personal en el área de telemetría para cumplir eficaz y eficientemente las actividades que intervienen en el proceso revisado, lo cual incide directamente en el cumplimiento de los objetivos establecidos, lo cual podría afectar la credibilidad e imagen de la empresa ante sus clientes. Adicionalmente se recomienda que la capacitación del personal que actualmente interviene en el proceso deba ser constante a fin de mantener el éxito del proyecto y su futura expansión.

Finalmente se debería enfocar esfuerzos en los riesgos de mayor criticidad e impacto detallados en el informe, para lo cual se exponen las recomendaciones a seguir con el objeto de mitigar los riesgos y su impacto.

Dominio:	9 SEGURIDAD FÍSICA Y AMBIENTAL.	
Objetivo:	Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización.	
Control:	9.2 SEGURIDAD DE LOS EQUIPOS.	
Controles	**Riesgo**	**Recomendación**
Ubicación y protección de los equipos	Existe el riesgo de acceso por parte de personas no autorizadas.	Reubicar los equipos a una mayor altura para minimizar el riesgo de manipulación o hurto de los equipos.
	Existe el riesgo de que el poste pueda ser derribado por colisión de un vehículo o la caída de un árbol ya que se encuentran a lado de las calles.	Reubicar los equipos en postes alejados de la vía pública (calles), a fin de evitar daño temporal o permanente de los equipos en caso de un accidente de tránsito en el cual el poste sea derribado.
	Existe el riesgo de que el poste pueda ser derribado por colisión de un vehículo o la caída de un árbol ya que se encuentran a lado de las calles.	Reubicar los equipos en postes alejados de la vía pública (calles), a fin de evitar daño temporal o permanente de los equipos en caso de un accidente de tránsito en el cual el poste sea derribado.
Seguridad del cableado	Existe el riesgo de que le poste pueda ser derribado por colisión de un vehículo o la caída de un árbol ya que se encuentran a lado de las calles.	Reubicar los equipos en postes alejados de la vía pública (calles), a fin de evitar daño temporal o permanente de los equipos en caso de un accidente de tránsito en el cual el poste sea derribado.
Mantenimiento de los equipos	Existe el riesgo de falla o avería de los equipos por falta de mantenimiento.	Elaborar un plan de mantenimiento anual.

Objetivo:	Asegurar la operación correcta y segura de los medios de procesamiento de la información.	
Control:	10.1 RESPONSABILIDADES Y PROCEDIMIENTOS DE OPERACIÓN.	
Controles	**Riesgo**	**Recomendación**
Documentación de procedimientos de operación.	En caso de que falten las personas que conocen el procedimiento, no se tendrá información de cómo hacerlo.	Elaborar documentación de los procedimientos de reinicio y recuperación del sistema, además de políticas para el manejo de la información. Capacitar constantemente al personal que interviene en estas actividades.
	Se dependería de una sola persona en el proceso.	Asegurar la información a fin de mitigar el riesgo de pérdida de la misma. Elaborar documentación de los procedimientos y manejo de información para que esta actividad no dependa de una sola persona. Revisar la segregación de funciones establecidas actualmente en la empresa y tomar las medidas correctivas necesarias.
Gestión de cambios.	En caso de que falten las personas que conocen el procedimiento, no se tendrá información de cómo hacerlo.	Elaborar e implementar un procedimiento para controlar los cambios en los equipos y/o su configuración a fin de no comprometer la confiabilidad del proceso.
Separación de las instalaciones de desarrollo, prueba y operación	Existe el riesgo de falla en las pruebas lo cual podría comprometer la operación del proceso.	Separar los ambientes de desarrollo, prueba y producción a fin de tener independencia en el momento de evaluar una nueva aplicación, además de no comprometer la continuidad del negocio debido a posibles errores en caso de que una prueba sea fallida.

Control:	10.5 COPIAS DE SEGURIDAD.
Objetivo:	Mantener la integridad y disponibilidad de la información y los medios de procesamiento de información.

Controles	Preguntas de Auditoria	Recomendación
Copias de seguridad de información	Existe el riesgo de afectar la continuidad del negocio en el posible evento de un desastre en el edificio principal.	Implementar políticas de respaldos de la información y de ser posible un entorno de alta disponibilidad, implementar políticas basándose en un marco de referencia de Guías de Buenas Prácticas para almacenar los respaldos a fin de asegurar razonablemente la integridad, confidencialidad y disponibilidad de la información.

Dominio:	11 CONTROL DE ACCESO.
Control:	11.1 REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO.
Objetivo:	Controlar el acceso a la información.

Controles	Riesgo	Recomendación
Política de control de acceso.	Existe el riesgo de no establecer correctamente los perfiles de acceso.	Elaborar la documentación correspondiente a las políticas establecidas para asignar los accesos lógicos a los usuarios además de un registro documentado y actualizado de los perfiles de usuario y cambios realizados.

Dominio:	11 CONTROL DE ACCESO.
Control:	11.2 GESTIÓN DE ACCESO DE USUARIO.
Objetivo:	Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información.

Controles	Riesgo	Recomendación
Gestión de contraseñas de usuario.	La solicitud de contraseñas se las realiza vía correo electrónico desde la Jefatura de Telemetría al administrador del aplicativo y la respuesta es por la misma vía, el usuario no firma documentos de confidencialidad.	Elaborar un acuerdo de confidencialidad para asignación de credenciales y definir tiempos de expiración en aplicativo, capacitar a los usuarios acerca de la importancia de la confidencialidad de las contraseñas y los riesgos existentes.
Revisión de los derechos de acceso de usuario.	Existe el riesgo que ese acceso este siendo utilizado por otro usuario.	Realizar un procedimiento en el cual se establezca una revisión regular cada 3 a 6 meses.

BIBLIOGRAFÍA

Documentación interna de la Eléctrica de Guayaquil

Documentación interna del Área de Telemetría – Energy Axis, Elster.

Manuales de Energy Axis.

Norma ISO 27001:2005

Norma ISO 27002:2005

Manual Cobit 4.1

Material de estudio CEC – Diplomado de Auditoría Informática

Brochure ISO 17799 – BSI Management System

ENLACES DE INTERNET.

http://www.electricaguayaquil.gob.ec

http://www.energyaxis.com/

http://www.iso27000.es/

http://www.bsigroup.com.mx/es-mx/Auditoria-y-Certificacion/Sistemas-d
Gestion/Normas-y-estandares/ISO-27001/

http://www.iso.org

http://www.isaca.org.ec

GLOSARIO.

AMI: Son los sistemas que miden, recolectan y analizan el uso de la energía, e interactúan con dispositivos como los medidores inteligentes de electricidad, de gas, o de agua.

CONELEC: Consejo Nacional de Electricidad, es un ente regulador y controlador, a través del cual el Estado Ecuatoriano puede delegar las actividades de generación, transmisión, distribución y comercialización de energía eléctrica, a empresas concesionarias.

COBIT: Es una metodología aceptada mundialmente para el adecuado control de proyectos de tecnología, los flujos de información y los riesgos que éstas implican. La metodología COBIT se utiliza para planear, implementar, controlar y evaluar el gobierno sobre TIC; incorporando objetivos de control, directivas de auditoría, medidas de rendimiento y resultados, factores críticos de éxito y modelos de madurez.

COSO: Es un documento que contiene las principales directivas para la implantación, gestión y control de un sistema de Control Interno. Debido a la gran aceptación de la que ha gozado, desde su publicación en 1992, el Informe COSO se ha convertido en el estándar de referencia en todo lo que concierne al Control Interno.

EA_MS: Energy Axis Management System, es el administrador del sistema de la red inteligente de toma de lectura de los medidores eléctricos.

FIREWALL: Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

GATEKEEPERS: Es la unidad central de control que gestiona las prestaciones en una red de datos, proporcionan la inteligencia de red, incluyendo servicios de resolución de direcciones, autorización, autenticación, registro de lectura para su tarifación y comunicación con el sistema de gestión de la red.

IDS: Es un aplicativo usado para detectar accesos no autorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos hackers, o de Script Kiddies que usan herramientas automáticas. El IDS suele tener sensores virtuales (por ejemplo, un sniffer de red) con los que el núcleo del IDS puede obtener datos externos (generalmente sobre el tráfico de red). El IDS detecta, gracias a dichos sensores, anomalías que pueden ser indicio de la presencia de ataques o falsas alarmas.

ISACA: (Asociación de Auditoría y Control de Sistemas de Información) es una asociación de profesionales y universitarios que se dedican a la práctica y estudio de la auditoría, el control y la seguridad informática.

ISO: Es una organización no gubernamental establecida en 1947. La misión de la ISO es promover el desarrollo de la estandarización y las actividades con ella relacionada en el mundo con la mira en facilitar el intercambio de servicios y bienes, y para promover la cooperación en la esfera de lo intelectual, científico, tecnológico y económico.

Red MESH: Se define como una aplicación inalámbrica en la cual se tiene una amplia flexibilidad en los enlaces que se pueden ofrecer con esta tecnología pudiendo ser Punto a Punto, Punto a Multipunto y Multipunto a Multipunto.

SI: Un sistema de información es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su posterior uso, generados para cubrir una necesidad.

TELEMETRÍA: Es una tecnología que permite la medición remota de magnitudes físicas y el posterior envío de la información hacia el operador del sistema.

TI: Tecnologías de la información, agrupan los elementos y las técnicas utilizadas en el tratamiento y la transmisión de las informaciones.

TRANSCEIVER: Es un dispositivo que realiza, dentro de una misma caja o chasis, funciones tanto de trasmisión como de recepción, utilizando componentes de circuito comunes para ambas funciones.

UPS: Uninterruptible Power Supply, es una fuente de suministro eléctrico que posee una batería con el fin de seguir dando energía a un dispositivo en el caso de interrupción eléctrica.

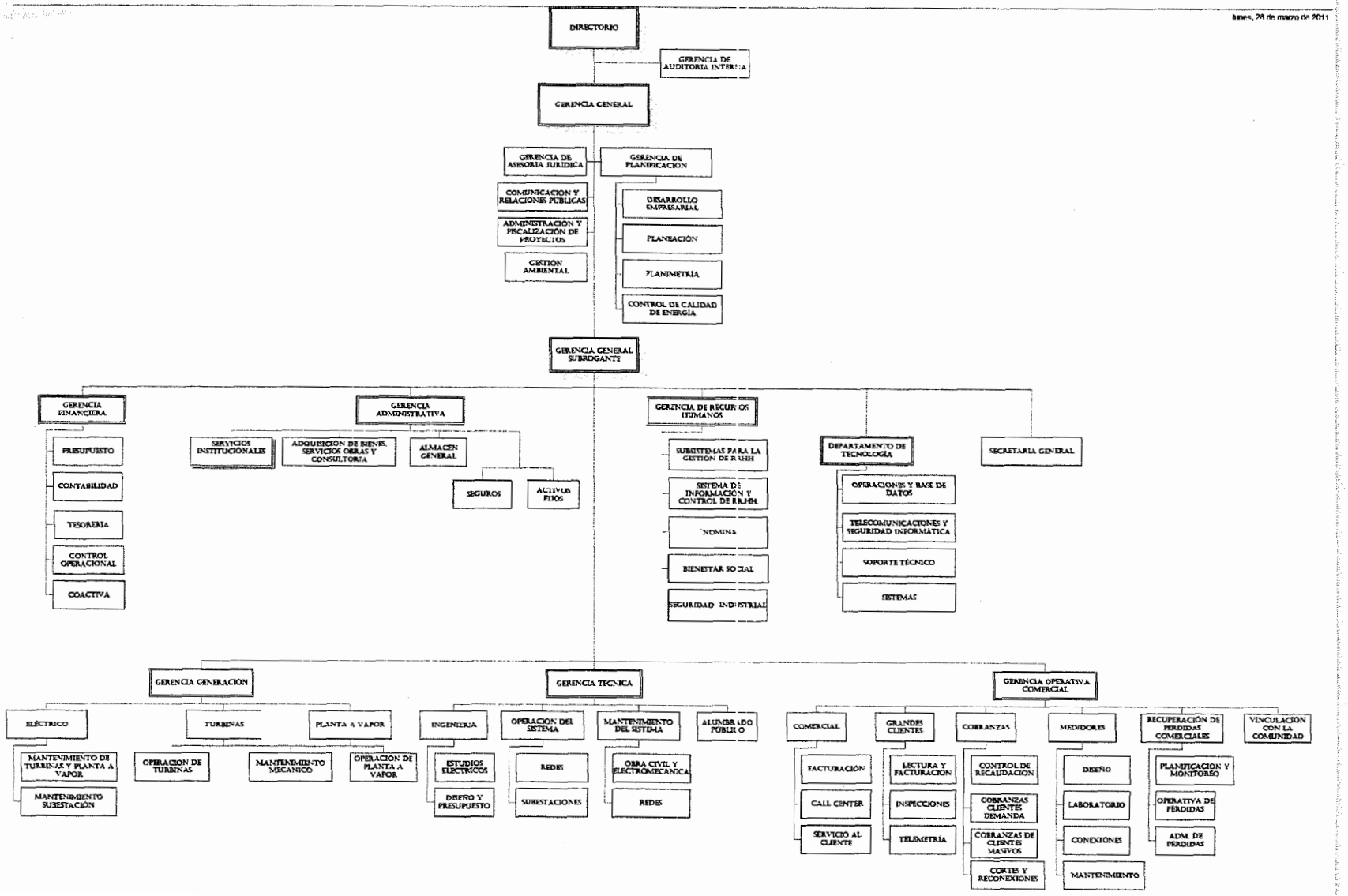
XML: Son las siglas de *Extensible Markup Language,* una especificación/lenguaje de programación desarrollada por el W3C. XML es una versión de SGML, diseñado especialmente para los documentos de la web. Permite que los diseñadores creen sus propias etiquetas, permitiendo la definición, transmisión, validación e interpretación de datos entre aplicaciones y entre organizaciones.

ANEXOS

ANEXO 1

UNIDAD DE GENERACIÓN, DISTRIBUCIÓN Y COMERCIALIZACIÓN DE ENERGÍA ELÉCTRICA DE GUAYAQUIL

lunes, 28 de marzo de 2011



ANEXO 2

Guayaquil 18 de julio de 2011.

Oficio# AE-01

Estimado

Ing. Daniel Pesantez.

Ciudad.

De mis consideraciones.

Por medio de la presente solicitamos realizar una reunión de trabajo para el día jueves, 21 de Julio de 2011 a partir de las 10h00, con el fin de revisar el alcance y elaborar la lista de aplicabilidad de controles a considerar en el Proyecto de Auditoria del Proceso de Telemetría.

Agradezco su respuesta oportuna.

Atentamente

Christian Cascante

Iván Coronel

Aprobado
Daniel Pesantez
18/07/2011
1:54 pm

ACTA DE TRABAJO N°1

Asunto de la Reunión:	Revisión del alcance y controles que se revisarán en el proyecto de Auditoría Proceso de Telemetría.
Fecha de Reunión:	21-Julio-2011
Hora:	Desde: 10h00 Hasta: 12h00
Revisión:	0
Fecha Elaboración:	22-Julio-2011
Convocatoria a reunión de trabajo :	La convocatoria a la reunión de trabajo fue realizada por personal a cargo de Auditoría: Christian Cascante e Iván Coronel, mediante oficio # AE-01 con fecha 18 de julio de 2011 el cual se adjunta.

Asistentes:

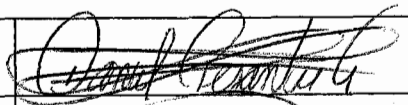
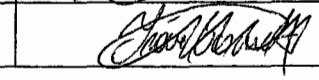
1. Daniel Pesantez – Telemetría
2. Christian Cascante – Auditor Informático del DAI-ESPOL
3. Iván Coronel – Auditor Informático del DAI-ESPOL

Temas tratados:

1. Revisión del plan de trabajo y alcance de la Auditoría a realizar.
   1.1. Todos los presentes están de acuerdo con el plan de trabajo y alcance presentado.
2. Revisión y análisis de los dominios que aplican al proyecto de auditoría.
   2.1. Se indica que los dominios a cubrir serán: Seguridad Física y Ambiental, Gestión de Comunicaciones y Operaciones, y Control de Accesos.
3. Determinación de los controles que serán revisados en el proyecto.
   3.1. Se acordó realizar la revisión de los controles que cubre el alcance los mismos que fueron puestos a conocimiento de los presentes, se adjunta listado de controles a revisar.
4. Detalles de aplicabilidad del proyecto.
   4.1. Se realizó explicación de los controles aplicables según el alcance del proyecto.
5. Definir protocolo para solicitar futuras revisiones.
   5.1. Previa coordinación se brindarán todas las facilidades (campo y oficina) para el desarrollo del proyecto.
6. Información del sistema de Telemetría – EnergyAxis.
   6.1. Se entregan manuales y se facilita usuario para revisión del sistema.
7. Revisión de la arquitectura del proceso de Telemetría.

Conclusiones:

De los temas tratados se ha quedado de acuerdo, para constancia y conformidad los intervinientes suscriben presente acta de trabajo.

Daniel Pesantez – Ingeniero de Telemetría	
Christian Cascante – Auditor Informático del DAI-ESPOL	
Iván Coronel – Auditor Informático del DAI-ESPOL	

ISO 27002:2005

Análisis de aplicabilidad.

I. Coronel, C. Cascante
Julio 26 de 2011

Dominios	Objetivos	Si	No
Política de Seguridad de la información.	Proporcionar la guía y apoyo de la Dirección para la seguridad de la información en relación a los requisitos del negocio y a las leyes y regulaciones relevantes.		X
Organización de la Seguridad de la información.	Manejar la seguridad de la información dentro de la organización.		X
Gestión de Activos.	Lograr y mantener una apropiada protección de los activos organizacionales.		X
Seguridad de Recursos Humanos.	Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados; reducir el riesgo de robo fraude y mal uso de los medios.		X
Seguridad Física y Ambiental.	Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización.	✓	
Gestión de Comunicaciones y Operaciones.	Asegurar la operación correcta y segura de los medios de procesamiento de la información.	✓	
Control de Accesos.	Controlar el acceso a la información.	✓	
Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.	Garantizar que la seguridad sea una parte integral de los sistemas de información.		X
Gestión de Incidentes de la Seguridad de la Información.	Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva oportuna.		X
Gestión de Continuidad del Negocio.	Contraatacar las interrupciones a las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.		X
Cumplimiento.	Evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad.		X

Dominio: Seguridad Física y Ambiental.

9 Seguridad Física y Ambiental.					
Estándar	**Objetivo**		**Controles**	**Aplica (Si/No)**	**Justificación de la Ejecución**
9.1	Áreas Seguras	9.1.1	Perímetro de Seguridad Física	No	No se define en el alcance
		9.1.2	Controles Físicos de Entrada	No	No se define en el alcance
		9.1.3	Seguridad de oficinas, despachos e instalaciones.	No	No se define en el alcance
		9.1.4	Protección contra las amenazas externas y de origen ambiental	No	Preocupación por la integridad de los equipos de recolección y transmisión de datos.
		9.1.5	Trabajo en áreas seguras.	No	No se define en el alcance
		9.1.6	Áreas de acceso al público y de carga y descarga	No	No se define en el alcance
9.2	Seguridad de los Equipos.	9.2.1	Ubicación y protección de los equipos	Si	Posible manipulación de los equipos por terceros.
		9.2.2	Instalación de suministro	Si	Asegurar el funcionamiento de los equipos de transmisión de datos ante cortes de energía eléctrica
		9.2.3	Seguridad del cableado	Si	Preocupación de la Gerencia por la pérdida de enlace con los equipos recolectores de información.
		9.2.4	Mantenimiento de los equipos	Si	Mantener la continuidad de los servicios que ofrece.
		9.2.5	Seguridad de los equipos fuera de las instalaciones	No	No se define en el alcance
		9.2.6	Reutilización o retirada segura de los equipos	No	No se define en el alcance
		9.2.7	Retirada de materiales propiedad de la empresa	No	No se define en el alcance

Dominio: Gestión de las comunicaciones y operaciones.

10 Gestión de las comunicaciones y operaciones					
Estándar	**Objetivo**		**Controles**	**Aplica (Si/No)**	**Justificación de la Ejecución**
10.1	Procedimientos Operacionales y Responsabilidades	10.1.1	Documentos de procedimientos de operación.	Si	Revisar la documentación de la operación del sistema Energy Axis.
		10.1.2	Gestión de Cambios	Si	Revisar procedimientos para gestionar los cambios.
		10.1.3	Segregación de funciones	Si	No se define en el alcance
		10.1.4	Separación de las instalaciones de desarrollo, prueba y operación	Si	No hay ambiente de desarrollo, ni pruebas.
10.2	Gestión de la entrega del servicio de terceros.	10.2.1	Provisión del servicio	Si	Revisar los controles de seguridad, definiciones y niveles de servicio del proveedor de enlace de datos.
		10.2.2	Monitoreo y revisión de los servicios de terceros	Si	Revisar los niveles de servicios, revisar los aspectos de seguridad.
		10.2.3	Manejo de cambios en los servicios de terceros	Si	Revisar la coordinación de los cambios de ubicación entre la organización y terceros.
10.3	Planeación y aceptación del sistema	10.3.1	Gestión de la capacidad	No	No se define en el alcance
		10.3.2	Aceptación del sistema	No	No se define en el alcance
10.4	Protección contra el código malicioso y móvil	10.4.1	Controles contra códigos maliciosos	Si	Revisar la protección contra riesgos asociados a archivos maliciosos.
		10.4.2	Controles contra códigos móviles	Si	Revisar la integridad de la información que pasa de la Base de Datos de Telemetría a la Base de Datos del Sistema Comercial de la Empresa.
10.5	Respaldo o Back-Up	10.5.1	Copias de seguridad de información	Si	Revisar los controles para asegurar la disponibilidad de la información.
10.6	Gestión de seguridad de la red	10.6.1	Controles de redes	Si	Revisar el control de accesos a los servicios de la red.
		10.6.2	Seguridad de los servicios de red	Si	Revisar le ancho de banda y equipos de seguridad.

10 Gestión de las comunicaciones y operaciones					
Estándar	**Objetivo**		**Controles**	**Aplica (Si/No)**	**Justificación de la Ejecución**
10.7	Gestión de medios	10.7.1	Gestión de medios removibles	No	No se define en el alcance
		10.7.2	Retirada de Soportes	No	No se define en el alcance
		10.7.3	Procedimientos de manipulación de la información.	No	No se define en el alcance
		10.7.4	Seguridad de la documentación del sistema.	No	No se define en el alcance
10.8	Intercambio de información.	10.8.1	Políticas y procedimientos de intercambio de información.	No	No se define en el alcance
		10.8.2	Acuerdos de intercambio.	No	No se define en el alcance
		10.8.3	Soportes físicos en tránsito.	No	No se define en el alcance
		10.8.4	Mensajería electrónica.	No	No se define en el alcance
		10.8.5	Sistemas de información empresariales.	No	No se define en el alcance
10.9	Servicios de comercio electrónico.	10.9.1	Comercio electrónico.	No	No se define en el alcance
		10.9.2	Transacciones en línea.	Si	
		10.9.3	Información públicamente disponible.	No	No se define en el alcance
10.10	Supervisión.	10.10.1	Registros de auditoría.	Si	Revisar si el proceso cuenta con registros para revisiones en caso de un incidente.
		10.10.2	Supervisión del uso del sistema.	Si	Revisar el correcto uso de los recursos del sistema.
		10.10.3	Protección de la información de los registros.	Si	Revisión considerada en el alcance.
		10.10.4	Registros de administración y operación.	Si	Revisión considerada en el alcance.
		10.10.5	Registro de fallos.	Si	Revisión considerada en el alcance.
		10.10.6	Sincronización del reloj.	Si	Revisión considerada en el alcance.

Dominio: Control de Acceso.

11 Control de Acceso					
Estándar	**Objetivo**		**Controles**	**Aplica (Si/No)**	**Justificación de la Ejecución**
11.1	Requisitos de negocio para el control de acceso.	11.1.1	Política de control de acceso.	Si	
11.2	Gestión de acceso de usuario.	11.2.1	Registro de usuario.	No	No se define en el alcance
		11.2.2	Gestión de privilegios.	Si	Verificar la existencia de perfiles de uso establecidos.
		11.2.3	Gestión de contraseñas de usuario.	Si	Verificar la existencia de políticas en el uso de contraseñas.
		11.2.4	Revisión de los derechos de acceso de usuario.	Si	Verificar la existencia de perfiles de uso establecidos.
11.3	Responsabilidades de usuario.	11.3.1	Uso de contraseñas.	No	No se define en el alcance
		11.3.2	Equipo de usuario desatendido.	No	No se define en el alcance
		11.3.3	Política de puesto de trabajo despejado y pantalla limpia.	No	No se define en el alcance
11.4	Control de acceso a la red.	11.4.1	Política de uso de los servicios en red.	Si	Revisar las actividades existentes para el control del uso de la red.
		11.4.2	Autenticación de usuario para conexiones externas.	Si	Verificar los controles para permitir la conexión de usuarios vía VPN
		11.4.3	Identificación de los equipos en las redes.	No	No se define en el alcance
		11.4.4	Protección de los puertos de diagnóstico y configuración remotos.	Si	Confirmar que solo se encuentren habilitados los puertos requeridos por los sistemas de gestión.
		11.4.5	Segregación de las redes.	No	No se define en el alcance
		11.4.6	Control de la conexión a la red.	No	No se define en el alcance
		11.4.7	Control de encaminamiento (routing) de red.	No	No se define en el alcance

11 Control de Acceso					
Estándar	**Objetivo**		**Controles**	**Aplica (Si/No)**	**Justificación de la Ejecución**
11.5	Control de acceso al sistema operativo.	11.5.1	Procedimientos seguros de inicio de sesión.	Si	Verificar la existencia de procedimientos.
		11.5.2	Identificación y autenticación de usuario.	Si	Constatar la existencia de procedimientos y controles.
		11.5.3	Sistema de gestión de contraseñas.	Si	Revisar el procedimiento para asignación de contraseñas.
		11.5.4	Uso de los recursos del sistema.	No	No se define en el alcance
		11.5.5	Desconexión automática de sesión.	No	No se define en el alcance
		11.5.6	Limitación del tiempo de conexión.	No	No se define en el alcance
11.6	Control de acceso a las aplicaciones y a la información.	11.6.1	Restricción del acceso a la información.	Si	Revisar si existen restricciones a la información que se maneja en telemetría.
		11.6.2	Aislamiento de sistemas sensibles.	Si	Verificar el ambiente de procesamiento de los sistemas de telemetría.
11.7	11.7 Ordenadores portátiles y teletrabajo.	11.7.1	Ordenadores portátiles y comunicaciones móviles.	No	No se define en el alcance
		11.7.2	Teletrabajo.	No	No se define en el alcance

Tabla 3.3 Justificación de aplicabilidad

Los parámetros establecidos en las tablas de aplicabilidad se han definidos en base a los requerimientos de las Gerencia Comercial Operativa y al alcance del proyecto.

Guayaquil 26 de julio de 2011

Oficio# AE-02

Estimado

Ing. Oswaldo Alarcón

Ciudad.

De mis consideraciones.

Por medio de la presente solicitamos realizar una reunión de trabajo para el día miércoles 27 de Julio de 2011 a partir de las 14h30, con el fin de revisar la inter-operación entre e sistema de telemetría y el sistema Comercial con medidores AMI.

Agradezco su respuesta oportuna.

Atentamente

Christian Cascante

Iván Coronel

Ing. Oswaldo Alarcón
26/07/2011

ACTA DE TRABAJO N°2

Asunto de la Reunión:	Revisión de la inter-operación entre el sistema de Telemetría y el sistema Comercial con medidores AMI.
Fecha de Reunión:	27-Julio-2011
Hora:	Desde: 14h30 Hasta: 16h30
Revisión:	0
Fecha Elaboración:	28-Julio-2011
Convocatoria a reunión de trabajo :	La convocatoria a la reunión de trabajo fue realizada por personal a cargo de la Auditoría: Christian Cascante e Iván Coronel, mediante oficio # AE-02 con fecha 26 de julio de 2011 el cual se adjunta.

Asistentes:

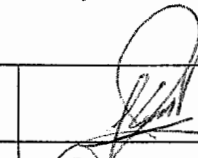
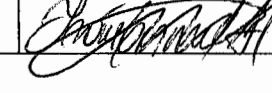
1. Oswaldo Alarcón – Tecnología
2. Christian Cascante – Auditor Informático del DAI-ESPOL
3. Iván Coronel – Auditor Informático del DAI-ESPOL

Temas tratados:

1. Revisión de los datos que se adquieren desde los medidores AMI.
    1.1. Se revisó los archivos en formato xml, se revisó la estructura de directorios y el almacenamiento de estos archivos.
2. Revisión de la interface para el intercambio de datos entre ambos sistemas.
    2.1. Se revisa la forma de transferencia y validación de datos.
3. Verificación de la información que se procesa en el sistema comercial.
    3.1. Se hizo la verificación del subproceso automatizado de corte y reconexión.
4. Revisión de perfiles de usuarios.
    4.1. Se revisaron los perfiles de usuarios que están definidos en el sistema EnergyAxis.
5. Verificar privilegios de acuerdo a los perfiles.
    5.1. Se crearon usuarios de prueba con distintos perfiles para validación.
6. Revisión de topología de la red de datos del proceso de Telemetría.

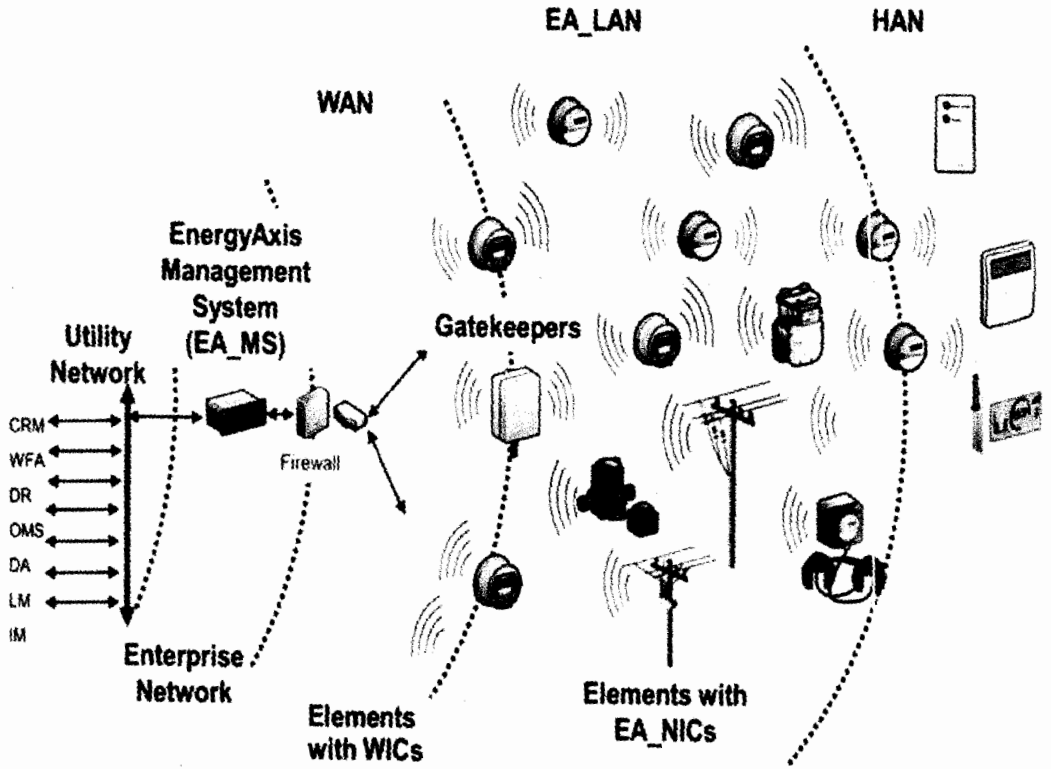
Conclusiones:

De los temas tratados se ha quedado de acuerdo, para constancia y conformidad los intervinientes suscriben la presente acta de trabajo.

Oswaldo Alarcón – Ingeniero de Tecnología	
Christian Cascante – Auditor Informático del DAI-ESPOL	
Iván Coronel – Auditor Informático del DAI-ESPOL	

ANEXO 3

GateKeeper.


EA_LAN
HAN
WAN
EnergyAxis
Management
System
(EA_MS)
Utility
Network
Gatekeepers
CRM
WFA
DR
OMS
DA
LM
IM
Firewall
Enterprise
Network
Elements
with WICs
Elements with
EA_NICs

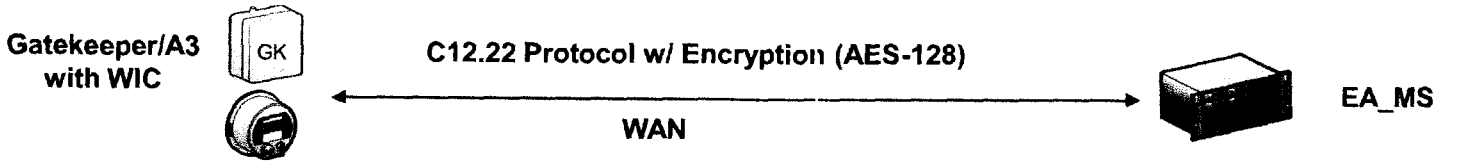
ANEXO 4

User Profiles – Actions > Schedule

elster

Report Only User	Billing and CIS Services	Meter Services	System Admin
View Reports	•View All •Resubmit •Modify Information •Create new schedule	•Exchange •Delete	•Same as Meter Services

ANEXO 5



AES-128

Es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. El AES fue anunciado por el Instituto Nacional de Estándares y Tecnología (NIST) como FIPS PUB 197 (Federal Information Processing Standards) de los Estados Unidos (FIPS 197) el 26 de noviembre de 2001 después de un proceso de estandarización que duró 5 años. Se transformó en un estándar efectivo el 26 de mayo de 2002.

1. Categoría del Estándar: Estándar de Seguridad Informática, Criptografía.
2. Explicación: El estándar de cifrado avanzado (AES) especifica un algoritmo criptográfico que se puede utilizar para proteger los datos electrónicos. El algoritmo AES es capaz de utilizar las claves de cifrado de 128, 192 y 256 bits para cifrar y descifrar los datos en bloques de 128 bits.

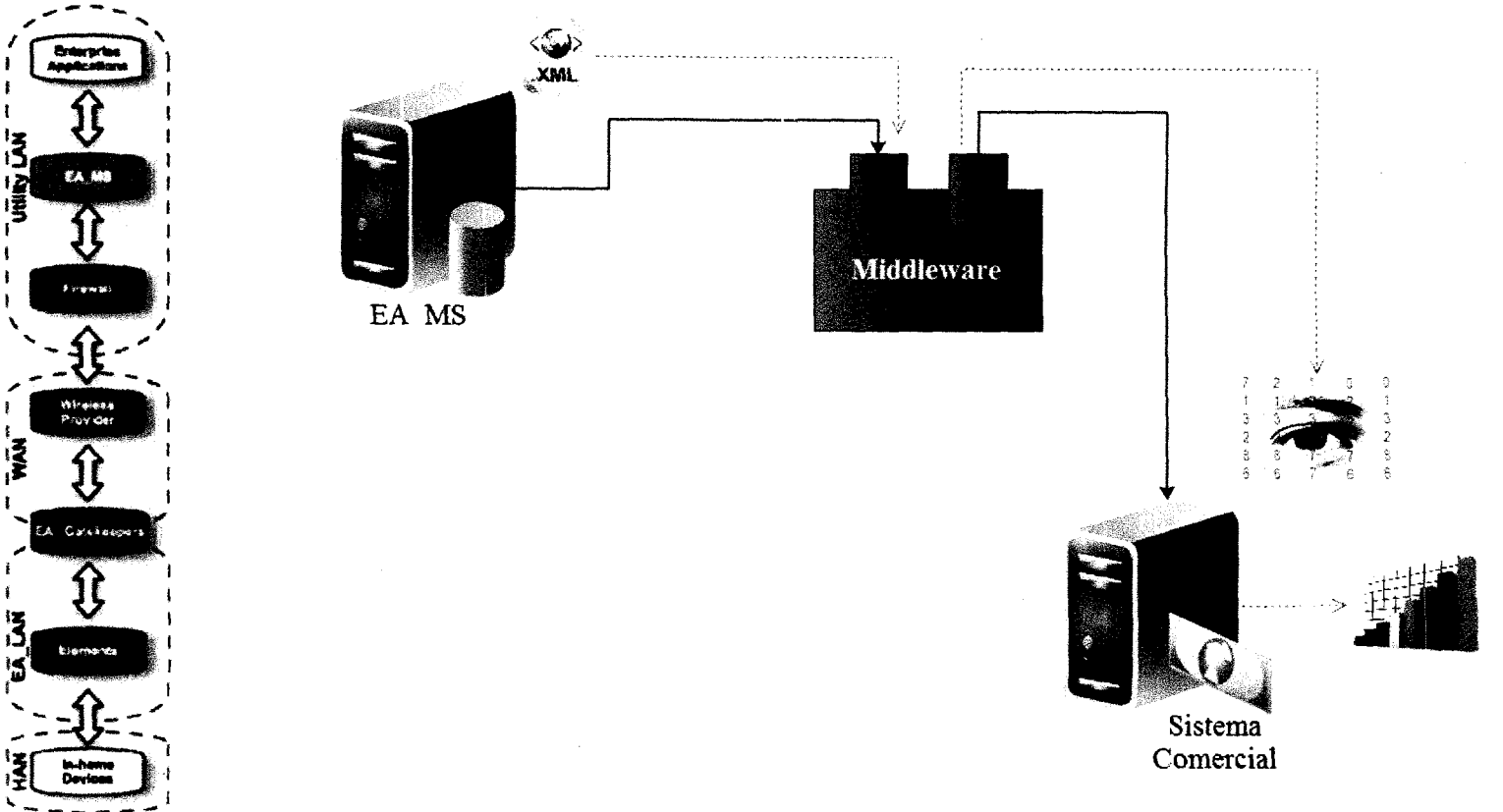
ANSI C12.22

C12.22 describe un protocolo para el transporte de ANSI C12.19 la tabla de datos a través de redes, con el propósito de la interoperabilidad entre los módulos de comunicaciones y metros. AES Esta norma utiliza AES de cifrado para permitir las comunicaciones sólida y segura, incluyendo confidencialidad e integridad de los datos. Es el modelo de seguridad es extensible para soportar nuevos mecanismos de seguridad.

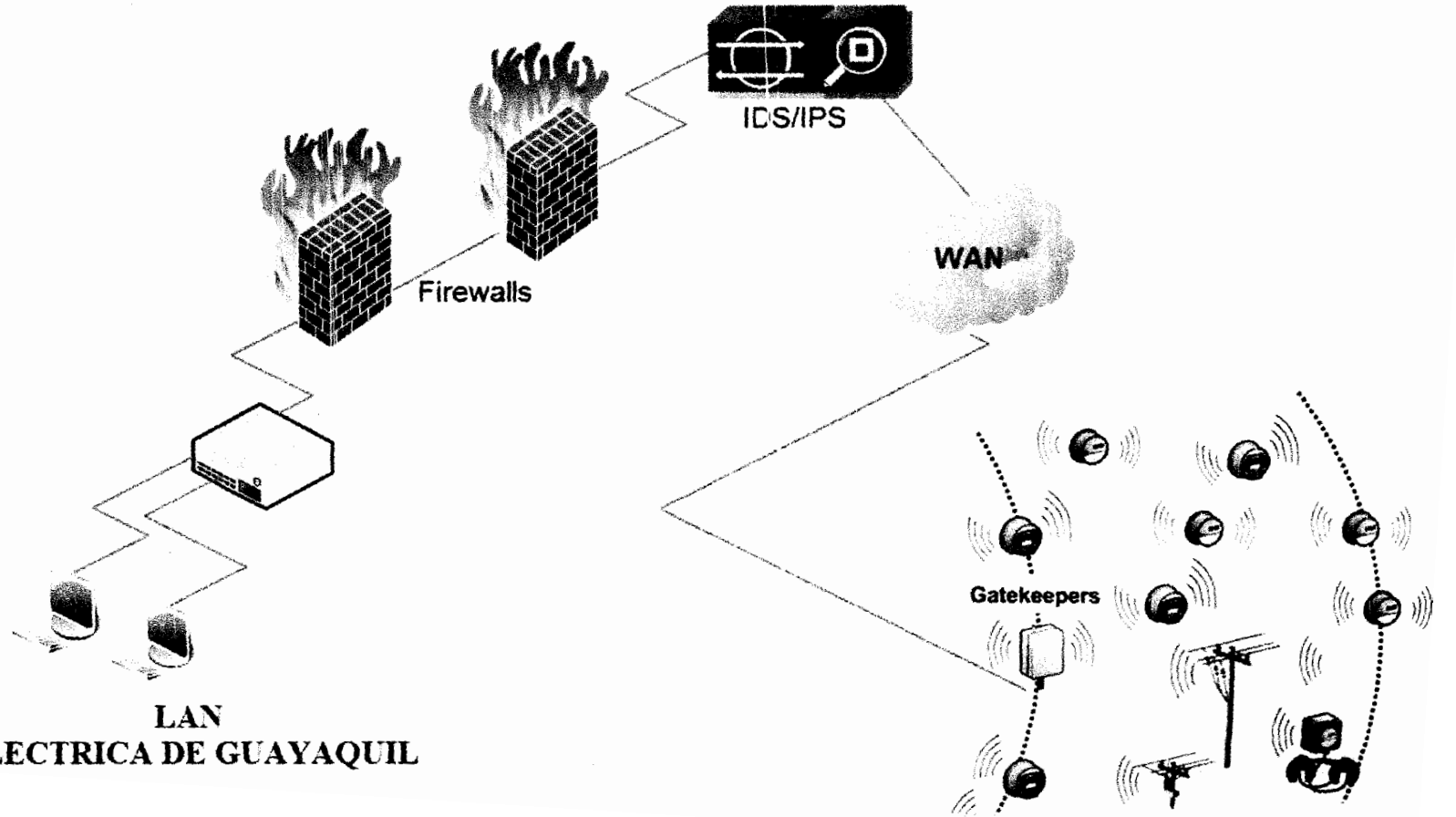
C12.22 define los servicios de mensaje que son componentes de una Infraestructura de Medición Avanzada (AMI) para el SmartGrid.

ANEXO 6

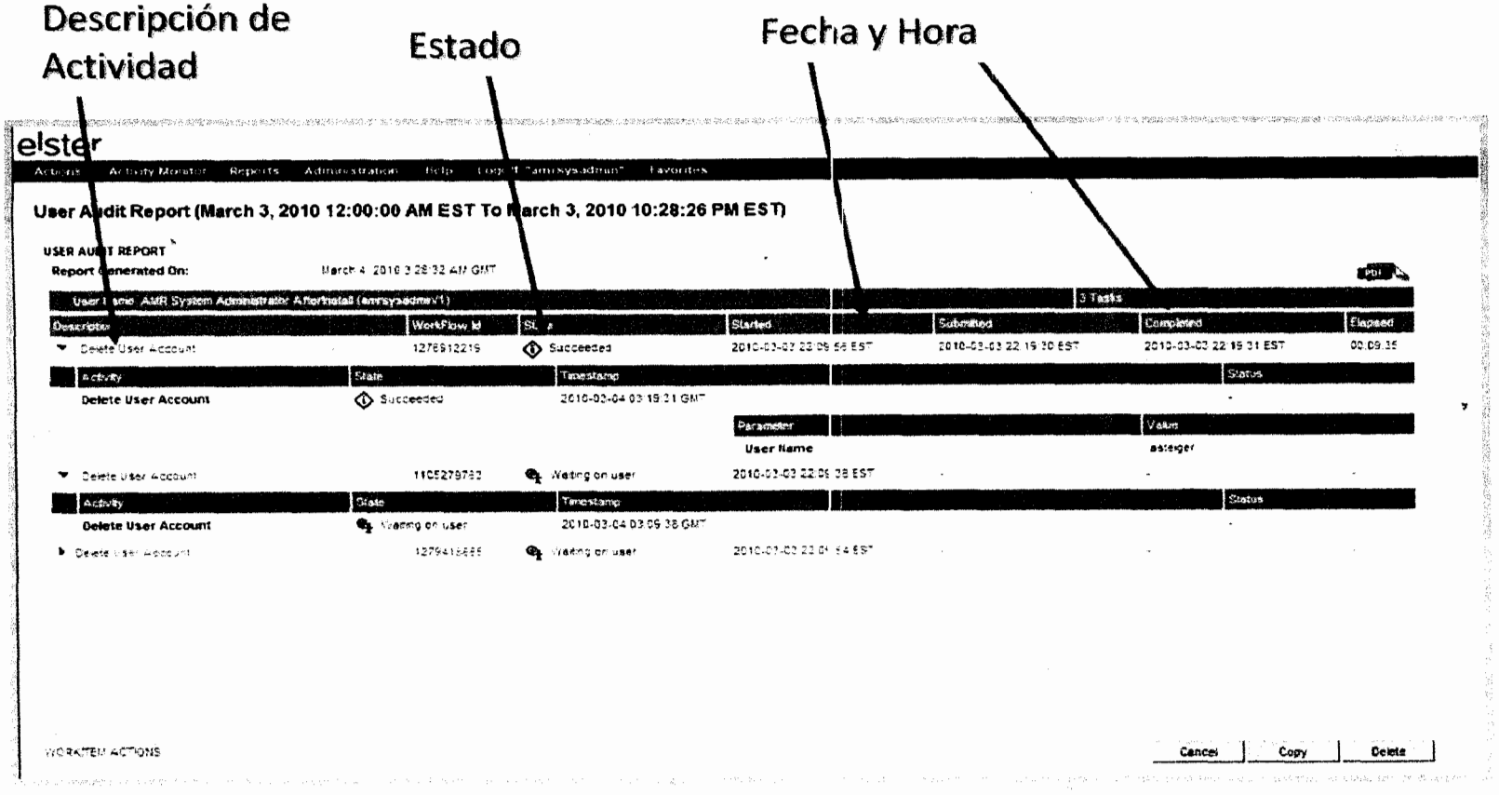
Transferencia de archivos XML desde EA MS al Sistema Comercial.



ANEXO 7

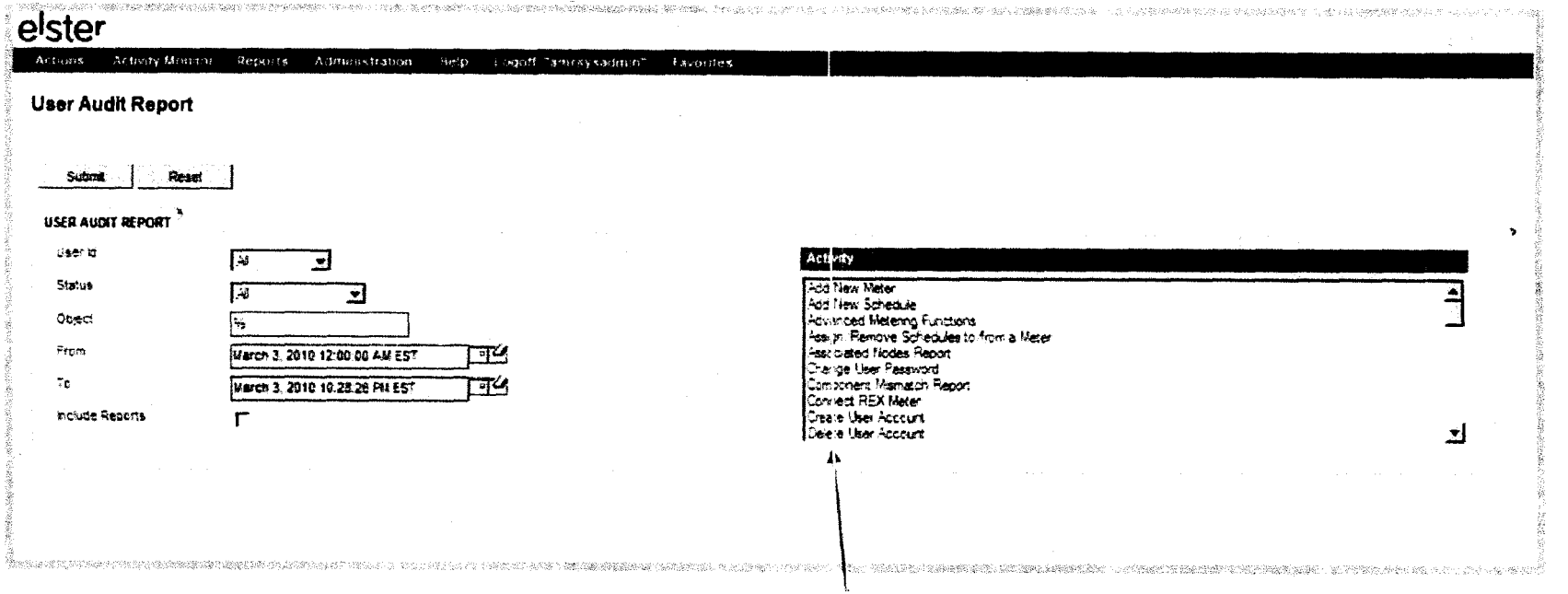

IDS/IPS
Firewalls
WAN
Gatekeepers
LAN
ELECTRICA DE GUAYAQUIL

ANEXO 8


Descripción de Actividad
Estado
Fecha y Hora
elster
Actions
Activity Monitor
Reports
Administration
Help
Favorites
User Audit Report (March 3, 2010 12:00:00 AM EST To March 3, 2010 10:28:26 PM EST)
USER AUDIT REPORT
Report Generated On:
March 4, 2010 3:28:32 AM GMT
3 Tasks
Description
WorkFlow Id
State
Started
Submitted
Completed
Elapsed
Delete User Account
1276912219
Succeeded
2010-03-03 22:09:56 EST
2010-03-03 22:19:30 EST
2010-03-03 22:19:31 EST
00:09:35
Activity
State
Timestamp
Status
Delete User Account
Succeeded
2010-03-04 03:19:21 GMT
Parameter
Value
User Name
asteger
Delete User Account
1105279782
Waiting on user
2010-03-03 22:09:38 EST
Activity
State
Timestamp
Status
Delete User Account
Waiting on user
2010-03-04 03:09:38 GMT
Delete User Account
1279416885
Waiting on user
2010-03-03 22:01:54 EST
WORKITEM ACTIONS
Cancel
Copy
Delete

ANEXO 9

Filtrado por – ID de Usuario, estado, Actividad, Objeto, Rango de tiempo, etc.



Actividades a seleccionar para emitir Reportes de

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

CENTRO DE EDUCACIÓN CONTINUA

DIPLOMADO EN AUDITORÍA INFORMÁTICA

III / V PROMOCIÓN

INFORME DE AUDITORÍA

AUDITORIA A LA ADQUISICION Y PROCESAMIENTO DE DATOS DEL AREA DE TELEMETRIA.
ENTIDAD: EMPRESA ELECTRICA DE GUAYAQUIL.
FECHA DE FINALIZACIÓN: 26 DE AGOSTO DE 2011.

AUTORES

CHRISTIAN CASCANTE CABALLERO
IVÁN CORONEL ARELLANO

AÑO

2011

INFORME DE AUDITORÍA

AUDITORIA A LA ADQUISICION Y PROCESAMIENTO DE DATOS DEL AREA DE TELEMETRIA.
ENTIDAD: EMPRESA ELECTRICA DE GUAYAQUIL.
FECHA DE FINALIZACIÓN: 26 DE AGOSTO DE 2011.

I. RESUMEN EJECUTIVO.

Una vez realizada la revisión de los procedimientos y actividades ejecutadas en la adquisición y procesamiento de los datos del proceso de telemetría con la finalidad de verificar la existencia y cumplimiento de los controles que actualmente existen, hemos determinado como resultado del trabajo de auditoría que el proceso se halla expuesto a un Riesgo Medio, lo que puede afectar significativamente a la obtención oportuna de los datos y su procesamiento lo cual derivaría en el retraso de los demás procesos dependientes (Lectura, Cortes y Reconexiones, Facturación) de la información que genera el Área de Telemetría.

II. OBSERVACIONES

➢ Seguridad Física y Ambiental.

9.2.1 (Criticidad Baja). Los tranceivers se encuentran instalados sobre los postes de alumbrado público a 9 metros de altura en cajas anti-hurto eléctricas, sin embargo existen riesgos implícitos.	
Riesgo: Existe el riesgo de acceso por parte de personas no autorizadas, además existe el riesgo de que el poste pueda ser derribado por colisión de un vehículo o la caída de un árbol ya que se encuentran a lado de las calles.	**Recomendación:** Reubicar los equipos a una mayor altura para minimizar el riesgo de manipulación o hurto de los equipos.

9.2.1 (Criticidad Media). Los gatekeepers se encuentran instalados sobre los postes de alumbrado público a 18 metros de altura.	
Riesgo: Existe el riesgo de que el poste pueda ser derribado por colisión de un vehículo o la caída de un árbol ya que se encuentran a lado de las calles.	**Recomendación:** Reubicar los equipos a una mayor altura para minimizar el riesgo de manipulación o hurto de los equipos, reubicar los equipos en postes alejados de la vía pública (calles), a fin de evitar daño temporal o permanente de los equipos en caso de un accidente de tránsito en el cual el poste sea derribado.

9.2.3 (Criticidad Media). El tendido de fibra óptica de la empresa que provee el servicio de enlace de datos pasa por postes de alumbrado público.	
Riesgo: Existe el riesgo de que le poste pueda ser derribado por colisión de un vehículo o la caída de un árbol ya que se encuentran a lado de las calles.	**Recomendación:** Reubicar los equipos en postes alejados de la vía pública (calles), a fin de evitar daño temporal o permanente de los equipos en caso de un accidente de tránsito en el cual el poste sea derribado.

9.2.4 (Criticidad Baja). No existe el documento ni el plan de mantenimiento de los equipos.	
Riesgo: Existe el riesgo de falla o avería de los equipos por falta de mantenimiento.	**Recomendación:** Elaborar un plan detallado de las actividades y frecuencia del mantenimiento de los equipos.

➢ Gestión de las comunicaciones y operaciones.

10.1.1 (Criticidad Media). No existe documentación en donde se detallen los procedimientos de reinicio y recuperación del sistema en el caso de una falla, así como del manejo de la información.	
Riesgo: En caso de que falten las personas que conocen el procedimiento, no se tendrá información de cómo hacerlo.	**Recomendación:** Elaborar documentación de los procedimientos de reinicio y recuperación del sistema, además de políticas para el manejo de la información. Capacitar constantemente al personal que interviene en estas actividades.

10.1.1 (Criticidad Alta). El procedimiento para la operación (cambios de configuración) de los medidores es manejado por una persona.	
Riesgo: Se dependería de una sola persona en el proceso.	**Recomendación:** Asegurar la información a fin de mitigar el riesgo de pérdida de la misma. Elaborar documentación de los procedimientos y manejo de información para que esta actividad no dependa de una sola persona. Revisar la segregación de funciones establecidas actualmente en la empresa y tomar las medidas correctivas necesarias.

10.1.2 (Criticidad Media). Existe un procedimiento de aprobación formal de cambios o configuración de equipos, pero no se encuentra documentado, y los cambios se dan en función de la demanda de equipos.	
Riesgo: En caso de que falten las personas que conocen el procedimiento, no se tendrá información de cómo hacerlo.	**Recomendación:** Elaborar e implementar un procedimiento para controlar los cambios en los equipos y/o su configuración a fin de no comprometer la confiabilidad del proceso.

10.1.4 (Criticidad Baja). No existen ambientes de desarrollo, pruebas y producción separada. El desarrollo es in-house y las pruebas se la realizan en el servidor de producción.	
Riesgo: Existe el riesgo de falla en las pruebas lo cual podría comprometer la operación del proceso.	**Recomendación:** Separar los ambientes de desarrollo, prueba y producción a fin de tener independencia en el momento de evaluar una nueva aplicación, además de no comprometer la continuidad del negocio debido a posibles errores en caso de que una prueba sea fallida.

10.5.1 (Criticidad Baja). No existe una política definida para el respaldo y verificación de la información de telemetría en medios magnéticos.	
Riesgo: Existe el riesgo de afectar la continuidad del negocio en el posible evento de un desastre en el edificio principal.	**Recomendación:** Implementar políticas de respaldos de la información y de ser posible un entorno de alta disponibilidad, implementar políticas basándose en un marco de referencia de Guías de Buenas Prácticas para almacenar los respaldos a fin de asegurar razonablemente la integridad, confidencialidad y disponibilidad de la información.

➢ Control de Acceso.

11.1.1 (Criticidad Alta). Se aplican políticas y criterios para el control de acceso lógicos a través de perfiles de usuarios, pero no existe documentación que respalde este control.	
Riesgo: Existe el riesgo de no establecer correctamente los perfiles de acceso.	**Recomendación:** Elaborar la documentación correspondiente a las políticas establecidas para asignar los accesos lógicos a los usuarios además de un registro documentado y actualizado de los perfiles de usuario y cambios realizados.

11.2.3 (Criticidad Media). La solicitud de contraseñas se las realiza vía correo electrónico desde la Jefatura de Telemetría al administrador del aplicativo y la respuesta es por la misma vía, el usuario no firma documentos de confidencialidad.	
Riesgo: Se podría hacer mal uso de las credenciales de autenticación por parte de personal mal intencionado o no pertenecientes a la empresa.	**Recomendación:** Elaborar un acuerdo de confidencialidad para asignación de credenciales y definir tiempos de expiración en aplicativo, capacitar a los usuarios acerca de la importancia de la confidencialidad de las contraseñas y los riesgos existentes.

11.2.4 (Criticidad Alta). No existe un procedimiento establecido para realizar modificaciones o eliminación de privilegios de usuarios según demande el caso.	
Riesgo: Existe el riesgo que ese acceso este siendo utilizado por otro usuario.	**Recomendación:** Realizar un procedimiento en el cual se establezca una revisión regular cada 3 a 6 meses.

III. MATRIZ DE EVALUACIÓN DEL RIESGO

9 SEGURIDAD FÍSICA Y AMBIENTAL.				
Riesgo	Probabilidad	Impacto	Nivel de Riesgo	Criticidad
Existe el riesgo de que el poste pueda ser derribado por colisión de un vehículo o la caída de un árbol ya que se encuentran a lado de las calles.	2	3	**6**	**Media**
Existe el riesgo de acceso por parte de personas no autorizadas.	2	3	**6**	**Media**
Existe el riesgo de falla o avería de los equipos por falta de mantenimiento.	3	3	**9**	**Alta**

10 GESTIÓN DE COMUNICACIONES Y OPERACIONES.				
Riesgo	Probabilidad	Impacto	Nivel de Riesgo	Criticidad
Se dependería de una sola persona en el proceso.	4	3	**12**	**Alta**
En caso de que falten las personas que conocen el procedimiento, no se tendrá información de cómo hacerlo.	3	3	**9**	**Alta**
Existe el riesgo de falla en las pruebas lo cual podría comprometer la operación del proceso.	4	3	**12**	**Alta**
Existe el riesgo de afectar la continuidad del negocio en el posible evento de un desastre en el edificio principal.	3	3	**9**	**Alta**

11 CONTROL DE ACCESO

Riesgo	Probabilidad	Impacto	Nivel de Riesgo	Criticidad
Existe el riesgo de no establecer correctamente los perfiles de acceso.	3	3	**9**	**Alta**
Existe el riesgo que ese acceso este siendo utilizado por otro usuario.	3	3	**9**	**Alta**
Se podría hacer mal uso de las credenciales de autenticación.	4	3	**12**	**Media**

Elaborado por:	*Christian Cascante*	
Elaborado por:	*Iván Coronel*	
Revisado por:	*Jorge Olaya*	