Una Metodología para Auditar Normas de Calidad Orientada a la Gestión de Clientes en una Empresa Proveedora de Internet

A Methodology To Audit Quality Standards Oriented Towards Customer Management In An Internet Service Provider

Jack Daniel Cáceres Meza[1]

Facultad de Ingeniería Electrónica y Eléctrica, Universidad Nacional Mayor de San Marcos, Lima, Perú

***Resumen*— Se plantea una metodología específica para auditar empresas de tamaño medio que proveen servicios de Internet, cuyos resultados puedan apoyar la gestión de los clientes, y evitar utilizar una de las muchas metodologías existentes que se enfocan exclusivamente en los sistemas de información.**

Palabras clave—auditoría, ISO20000, ISO27000, efectividad, TIC.

Abstract- We propose a specific methodology to audit midsize companies that provide Internet services, whose results can support the management of customers, and avoid using one of the many existing methodologies that focus exclusively on information systems.

Key words—audit, ISO20000, ISO27000, effectiveness, ICT.

I. INTRODUCCIÓN

Una parte importante de la infraestructura de un Proveedor de Servicios Internet (ISP, por sus siglas en inglés) se relaciona con su gestión, control y mejora, así como la manera en que se solucionan problemas y se provee seguridad a la información.

En este contexto consideraremos dos tipos de infraestructura: la física implementada por empresas operadoras a las que denominaremos Telco 1.0; y la virtual, implementada por empresas que entregan servicios de valor agregado a las que denominaremos Telco 2.0. Las Telco 2.0 sub-arriendan los recursos de las Telco 1.0 para entregar sus servicios.

Por mucho tiempo las Telco 1.0 han seguido estándares que, en muchos casos, son diferentes a los que se utilizan en el ámbito de las Tecnologías de la Información y las Comunicaciones (TIC).

Sin embargo, conforme anota Nolle [1], la aplicación de buenas prácticas y normas internacionales del mundo de las TIC es perfectamente pertinente en el mundo de las telecomunicaciones de hoy. La explicación es que la fusión de las infraestructuras de red con las tecnologías de la información es un hecho natural ya que todo equipo moderno se basa en estándares de la Arquitectura Orientada a Servicios (SOA, por sus siglas en inglés).

En la actualidad, independiente del tipo de infraestructura que se gestione, los servicios que se entregan por su intermedio son críticos para los usuarios por tanto, la aplicación de buenas prácticas en la industria y normativas internacionales como ISO es una obligación, si se busca garantizar la calidad del servicio entregado, así como su efectividad. y así lo confirma la norma ISO 27011 [2], enfocada en las empresas de telecomunicaciones, al recordarnos que la información y los procesos de apoyo, instalaciones, redes y líneas son activos importantes y que la gestión de la seguridad de la información es sumamente necesaria, con la finalidad de manejar los activos de manera apropiada y continuar con las actividades de forma correcta y satisfactoria.

En general, una empresa necesita realizar auditorías porque debe justificar la inversión que realiza en tecnología (eficiencia y eficacia) y asegurar que ésta apoye sus objetivos estratégicos en todo momento, porque en la actualidad los resultados de las empresas son evaluados por los clientes en términos de efectividad en la entrega y valor de su utilización.

Como ejemplo, la International Civil Aviation Organization (ICAO) [3] considera crítica una adecuada metodología de auditoría, y desarrolla su propio manual con base en la ISO 19011.

La metodología de auditoría propuesta es uno de varios apoyos para lograr el alineamiento estratégico.

[1]Jack Daniel Caceres Meza, e-mail: jack_caceres@hotmail.com.

El resto de este trabajo está organizado de la manera descrita a continuación. En laS ección 2 se desarrolla el Marco Teórico respectivo, donde diferenciamos la orientación de la auditoría para una empresa de telecomunicaciones de la empleada regularmente para los sistemas de información. La Sección 3 describe el Método que se seguirá en la Sección 4. Finalmente, tras utilizar esta metodología en un caso real, los resultados se muestran en la Sección 5, y en la Sección 6 presentamos las Conclusiones.

II. Marco Teórico

A. *Definición de auditoría*

La auditoria constituye una herramienta de control y supervisión que contribuye a la creación de una cultura de la disciplina de la organización, al ocuparse "fundamentalmente del conjunto de medidas, políticas y procedimientos establecidos en las empresas para proteger el activo, minimizar las posibilidades de fraude, incrementar la eficiencia operativa y optimizar la calidad de la información en general" Morell [4].

Según Hevia [5], una auditoría "ayuda a la organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la efectividad de los procesos de gestión de riesgos, control y dirección".

La normatécnica peruana NTP 19011 [6], define auditoría como: "Un proceso sistemático, independiente y documentado para obtener evidencia capaz de ser interpretada y evaluada objetivamente para determinar la extensión en la que el criterio auditor ha sido cumplido".

El Instituto de Auditores Internos [7] ha definido a la auditoría interna como: "Una actividad de consultoría independiente, que establece una confianza objetiva, y que está diseñada para añadir valor y mejorar las operaciones de una organización. Apoya a que una organización logre sus objetivos, al brindar un acercamiento sistemático y disciplinado para evaluar y mejorar la eficacia del riesgo administrativo, el control y los procesos de gobierno"

1) Auditoría de telecomunicaciones

Una auditoría de telecomunicaciones es una evaluación del ambiente de telecomunicaciones de una organización. Sus objetivos son: la seguridad; cumplimiento de la política establecida; eficiencia de procesos; eficacia de costos; efectividad del servicio; apoyo de las telecomunicaciones a los objetivos del negocio; cumplimiento legal y regulatorio; comprobación del cumplimiento de las condiciones de uso y otros.

Según la empresa Audit Telecom [8], una apropiada auditoría de telecomunicaciones debería incluir todos los tipos de telecomunicaciones: voz, vídeo, y datos, y abarcar todo el equipo de telecomunicaciones, servicios, seguridad, políticas, planes de desarrollo y capacidad, política de continuidad del negocio, gastos utilizados por la organización, otros.

2) Auditoría en Informática

La literatura relacionada con el tema en cuestión es abundante pero podemos resumir que, en Informática, una auditoría implica la revisión y evaluación de los procesos, sus controles (preventivos, de detección, correctivos, alternativos o compensatorios), sistemas, procedimientos de informática, seguridad de datos y de la red, continuidad, aplicaciones, disponibilidad, confidencialidad e integridad de los datos, mapeo de datos, análisis de necesidades, inventario de los equipos de cómputo, gestión, utilización y eficiencia, que participan en el procesamiento de la información de la organización a fin de que, una vez evaluado el nivel de exposición (cuantitativa y cualitativamente), por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

3) Auditoría de la calidad

Mora [9] sostiene que "la auditoría de la calidad es una herramienta de gestión empleada para verificar y evaluar las actividades relacionadas con la calidad en el seno de una organización".

Se conoce que aquí se audita el Sistema de calidad de una empresa. El sistema se basa en dos manuales que una empresa establece para llevar a cabo la gestión de la calidad: el manual de calidad, que sintetiza la política de la empresa en cuanto a la calidad; y el manual de procedimientos, que detalla los procedimientos operativos con actores, y cuya redacción debe ser correcta, precisaclara, comple ta, pertinente, objetiva, concisa, constructiva, y oportuna.

Desde el punto de vista del aseguramiento de la calidad, se deberá auditar la observación de las consabidas competencias, "saber hacer" y "hacer bien" las cosas:

- Documentar las tareas que se realizan, ya que si no estamos en capacidad de describir claramente un trabajo, difícilmente podremos mejorarlo de forma consistente.
- Realizar las tareas conforme a lo documentado, ya que tenemos una referencia; si algo cambia en la ejecución, ésta se debe documentar y por tanto, se debe actualizar la documentación original.

- Registrar lo realizado, con la finalidad de examinar la calidad de lo ejecutado e identificar las causas de los problemas, si hubieran.
- Verificar, de modo periódico, que se estén alcanzando los objetivos previstos por la organización. No es extraña la siguiente frase entre auditores: "en Dios confío; del resto, dudo".
- Actuar sobre la diferencia es decir, cuando detectemos un problema existente o potencial, se actúa sobre él: se investigan las causas y se registra el resultado de la investigación. Se toman medidas para solucionarlo y para evitar que se repita, se comprueba la eficacia de las medidas correctivas, y se apropia y difunde clara y detalladamente el proceso completo incorporándolo a la documentación como lecciones aprendidas.

4) Otros conceptos de auditoría

De Di Bello [10] y otros autores, podemos resumir que toda auditoría interna:

- Debe agregar valor: es decir, debe ser capaz de aportar comentarios que permitan a nuestras organizaciones ganar en productividad, mejorar procesos, disminuir costos, mejorar los servicios para contar con clientes satisfechos y aumentar la relación riesgo/retorno.
- Debe ser pro-activa: de compromiso con un doble propósito de prevención y docencia; prevención a través de la docencia.
- Tiene el propósito de prevención: al asegurar a la empresa que sus colaboradores no ocasionen daño o pérdida patrimonial o sean objeto de instancias disciplinarias por desconocimiento de normativas legales y /o reglamentarias, o de otra índole. El aseguramiento debe darse, entre otras opciones, mediante inducción, definición clara de funciones y método de evaluación del desempeño, difusión y capacitación continua, apropiada, clara, correcta, suficiente, y completa con manuales y procedimientos de los procesos y operativa de la empresa.
- Es una actividad de consultoría: porque asesora y provee servicios relacionados, de naturaleza y alcances diversos, previamente acordados y dirigidos a añadir valor y a mejorar las operaciones, los procesos de gobierno y gestión de riesgos.
- Es una responsabilidad de todo el personal de la organización. El auditor interno solo evalúa la efectividad de los sistemas de control de la organización. Es un fotógrafo y no el arquitecto.

III. MÉTODO

Se desarrollará una metodología que permita a la empresa de telecomunicaciones una adecuada auditoría interna de cumplimiento, con miras a una futura certificación. Esta metodología abarcará los procesos, políticas, normas y procedimientos internos que hayan sido desarrollados empleando las normas peruanas NTP ISO 9001:2000, Gestión de la mejora continua; NTP ISO/IEC 27002, Gestión de la seguridad de la información, y la aplicación específica ISO/IEC 27011:2008, Directrices de seguridad de la información para empresas de telecomunicaciones teniendo como base la norma ISO/IE 27002 (ITU-T X.1051); NTP ISO/IEC 20000 2, Gestión de servicios de TI; y sistemas de gestión como ISO/IEC 27001 e ISO/IEC 20000-1.

Con la finalidad de asegurar los aspectos de imparcialidad, competencia y proceso de la auditoría, temas de preocupación particular para los gobiernos y autoridades reglamentarias a nivel internacional, utilizaremos los lineamientos establecidos por la norma internacional ISO/IEC 17021:2006, requisitos para los organismos que realizan la auditoría y la certificación de sistemas de gestión.

Para ejecutar la auditoría propuesta emplearemos la norma NTP 19011:2003, Directrices para la auditoría de los sistemas de gestión, aplicable a todas las organizaciones que tienen que realizar auditorías internas o externas de sistemas de gestión o que gestionan un programa de auditoría.

IV. METODOLOGÍA PROPUESTA

En primer lugar, los auditores deben satisfacer los requerimientos de la ISO 17021 y demostrar experiencia. Como aporte, podemos identificar algunos atributos importantes para esta norma que están directamente relacionados con la calidad del servicio prestado y son los siguientes: responsabilidad, transparencia, confidencialidad, receptividad, y respuesta oportuna a las reclamos.

Consideraremos las cualidades personales fundamentales de un auditor de proyectos de acuerdo con las normas UNE 166.000 y UNE 166.001 [11], las que son:

- Ético (imparcial, sincero, honesto, discreto, prudente, reservado).
- Diplomático (relaciones con las personas).
- Observador (activamente consciente del entorno físico y las actividades).
- Perceptivo (instintivamente consciente y capaz de entender las situaciones).

- Versátil (para adaptarse a diferentes situaciones).
- Tenaz (consecución de objetivos).
- Decidido (conclusiones basadas en el análisis y razonamientos lógicos).
- De mentalidad abierta (puntos de vista alternativos).
- Seguro de sí mismo (actúa y funciona independiente a la vez que se relaciona eficazmente con otros).

El siguiente es el resumen de la metodología propuesta para una empresa proveedora de Internet y en el Anexo adjunto desarrollamos estos puntos de forma específica:

1) Inicio de la auditoría.
2) Preparación y planificación.
3) Reunión de presentación.
4) Ejecución de la auditoría.
5) Finalización de la auditoría.
6) Reunión de clausura y cierre.
7) Elaboración del informe.
8) Presentación y comunicación de los resultados.
9) Comprobación y seguimiento.

Como se aprecia, la metodología sugerida para ejecutar la auditoría interna en empresas proveedoras de Internet no es muy diferente de otras; sin embargo, su valor reside en el énfasis específico en el tipo de empresa y la característica de evaluación orientada al consumidor, lo que hace de esta metodología algo particular, la búsqueda de la verdad, y ésta debe buscarse científicamente como se ha puesto en práctica.

V. Resultados

La evaluación es científica por tanto involucra un proceso de medición y comprobación de los principios y prácticas reconocidas en el cual se utilice una serie de pasos realizados en forma sistemática, ordenada y lógica que permita luego realizar una crítica objetiva del hecho o área examinada.

Del desarrollo de la metodología mostrado en el Anexo adjunto apreciaremos que la auditoría pasa de un enfoque tradicional (punto 2) que se veía como algo negativo por la fiscalización inherente, a la imagen actual como una actividad consultiva (puntos 4.2.8 y 4.2.9) y docente (punto 4) que añade valor a la empresa (puntos 3.2, 7.2, 9.2). Ver anexo.

En efecto, la aplicación de esta metodología de auditoría en una Telco 2.0 de tamaño medio de la ciudad de Lima (Ya chay Telecomunicaciones del Perú S.A., brazo comercializador de la Red Científica Peruana), proporcionó información relevante que condujo a la creación del Área de Valor Agregado en esta empresa, con el objetivo de proveer servicios adicionales y complementarios a los de valor añadido, contemplados por el Ministerio de Transportes y Comunicaciones; y el área de Planeamiento que se encarga de proyectos de inversión. Estas áreas se desarrollaron en 2009 y continúan en operación. El área de Valor Agregado emplea diferentes estándares como ISO9000, ISO20000 e ISO27000 y el área de Planeamiento emplea la metodología del PMI.

VI. Conclusiones

Sin equivocación, una conclusión importante es que la auditoría interna debe ser visualizada como un socio estratégico de la dirección.

Comprobamos que al realizar auditorías internas evaluamos el grado de adecuación entre los objetivos trazados, las disposiciones adoptadas y los resultados obtenidos. Es interesante notar que al realizar auditorías externas evaluamos la aptitud para la prevención y reducción de riesgos; y verificamos la aplicación de disposiciones contractuales.

Podemos resumir entonces que las auditorías internas tienen como finalidad validar el sistema de gestión y por tanto nos ayudan a mejorar. Por otro lado, las auditorías externas tienen como finalidad reconocer la aptitud de la organización para satisfacer los requisitos que han sido especificados. Es nuestra opinión que ambas deban emplearse como base para mantener una vigilancia tecnológica en la empresa, ya que ambas son importantes desde la perspectiva del cliente.

En resumen, la metodología de auditoría presentada brinda orientación a las empresas proveedoras de Internet en el aseguramiento de la confidencialidad, integridad y disponibilidad de los servicios o implementaciones que proveen, con bajo riesgo para los clientes y con un incremento en la confianza que éstos depositan en los servicios que contratan, confianza que representa una ventaja competitiva.

Referencias

[1] Nolle, Tom, "Las cinco primeras tendencias de la industria de las telecomunicaciones para 2010: transformación del mercado", CIMI Corp. Disponible: http://searchtelecom.techtarget.com/tip/0,289483,sid103_gci1375736,00.html?track=NL847&ad=742979&asrc=EM_NLN_10564497&uid=396338. Fecha de acceso: Agosto 2012.

[2] International Organization for Standardization (ISO). ISO/IEC 27011:2008 Information

technology -- Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002.Disponible: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43751. Fecha de acceso: Agosto 2012.

[3] Organización de Aviación Civil Internacional (ICAO). Safety Oversight Audit Manual. Disponible: http://legacy.icao.int/osg/isd/afi/Reference%20Material%5CSafety%20Oversight%20Manuals%5CDoc9735.pdf. Fecha de acceso: Agosto 2012.

[4] Morell González, Luisa María, "Manual de Auditoría Interna. Una herramienta indispensable para el auditor". Disponible: http://www.monografias.com/trabajos27/manual-auditoria/manual-auditoria.shtml. Fecha de acceso: Agosto 2012.

[5] Hevia, E., "Concepto moderno de Auditoría Interna". Revista Partida Doble. España: Número 139. 2da quincena Abril, 1999.

[6] Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI). NTP ISO 19011:2003 Directrices para la auditoría de los sistemas de gestión de la calidad y/o ambiental. Disponible: http://www.indecopi.gob.pe/0/modulos/TIE/TIE_DetallarProducto.aspx?PRO=4931. Fecha de acceso: Agosto 2012.

[7] The Institute of Internal Auditors. Disponible: http://www.theiia.org/guidance/standards-and-guidance/ippf/definition-of-internal-auditing/. Fecha de acceso: Agosto 2012.

[8] Audit Telecom. España. Disponible: http://www.audit-telecom.es/auditoria.php. Fecha de acceso: Agosto 2012.

[9] Mora Vanegas, Carlos, "La importancia de la auditoria de la calidad".Disponible: http://www.gestiopolis.com/administracion-estrategia/importancia-de-la-auditoria-de-la-calidad.htm. Fecha de acceso: Agosto 2012.

[10] Di Bello, Marcelo, "La Auditoría Interna como socio estratégico de la Dirección", Instituto Uruguayo de Auditoría Interna. Uruguay. Disponible: http://www.theiia.org/chapters/index.cfm/view.download/fileid/5822/cid/263.Fecha de acceso: Agosto 2012.

[11] Asociación Española de Normalización y Certificación (AENOR). UNE166000:2006, Gestión de la I+D+i: Terminología y definiciones de las actividades de I+D+i. España. Disponible: http://www.aenor.es/aenor/normas/normas/fichanorma.asp?codigo=N0036141&tipo=N.Fecha de acceso: Agosto 2012.

[12] Dey, A.K. & Abowd, G.D. "Towards a better understanding of context and context-awareness". GVU Technical Report GIT-GVU-99-22, College of Computing, Georgia Institute of Technology. Disponible: ftp://ftp.cc.gatech.edu/pub/gvu/tr/1999/99-22.pdf. Fecha de acceso Agosto 2012:

Anexo

Una Metodología Para Auditar Normas De Calidad En Un ISP

1 Inicio de la auditoría.

2 Preparación y planificación:

2.1 Designación del líder del equipo auditor.

2.2 Definición de los objetivos, ámbito, alcance (lo que estará comprendido y lo que no estará comprendido), y los criterios de auditoría.

2.3 Determinación de la viabilidad de la auditoría.

2.4 Determinación de los recursos que puedan ser requeridos y cuándo intervendrán. Se debe tener en cuanta las limitaciones de los recursos, disponibilidad, seguridad, acuerdos, convenios laborales, causas de escasez, otros.

2.5 Análisis crítico de documentos pertinentes al Sistema de Gestión de la Seguridad de la Información (SGSI), incluyendo registros, y determinando su adecuación con respeto al criterio de la auditoría.

2.5.1 Revisión de la documentación referida a la norma ISO 27000 como:

2.5.1.1 Responsabilidad de la Dirección.

2.5.1.2 Auditoría interna del SGSI.

2.5.1.3 Revisión por la Dirección del SGSI.

2.5.1.4 Mejora del SGSI.

2.5.1.5 Objetivos de control y controles.

2.6 Análisis crítico de documentos pertinentes al Sistema de Gestión de la Calidad (SGC), incluyendo registros, y determinando su adecuación con respeto al criterio de la auditoría.

2.6.1 Verificar que se ha establecido en la empresa las recomendaciones de la norma ISO 9000 tal que permita:

2.6.1.1 Identificar los procesos necesarios y la aplicación de estos procesos en toda la empresa.

2.6.1.2 Determinar la secuencia e interacción de los procesos.

2.6.1.3 Determinar los criterios y métodos de operación y control de los procesos.

2.6.1.4 Asegurar la disponibilidad de los recursos y la información que respalda los procesos, y el seguimiento de estos procesos.

2.6.1.5 Examinar, medir y analizar estos procesos.

2.6.1.6 Establecer acciones para lograr los resultados planeados y el mejoramiento continuo.

2.6.1.7 Establecer medidas correctivas y gestionar el conocimiento de las mismas en la forma de lecciones aprendidas que alimentan la documentación existente.

2.6.1.8 Si los procesos son subcontratados, ¿se encuentran estos procesos controlados e identificados?

2.6.2 ¿Posee la empresa un manual de calidad? Dicho manual deberá incluir:

2.6.2.1 El alcance del SGC y justificaciones y detalles de cualquier exclusión.

2.6.2.2 Los procedimientos documentados del SGC o una referencia a ellos.

2.6.2.3 Una descripción de las interacciones entre los procesos y el SGC.

2.6.2.4 Una clasificación de la estructura de responsabilidades, con autoridades.

2.6.2.5 ¿Se verifica que la alta dirección está comprometida con el SGC y su mejora continua? La alta dirección está conformada por una persona o grupo de personas que dirigen y controlan al más alto nivel una organización (3.2.7 ISO 9000:2005).Este compromiso se puede verificar si la alta dirección ha, de manera comprobada y visible:

2.6.2.6 Establecido su enfoque en la importancia de los clientes.

2.6.2.7 Establecido su Política de Calidad.

2.6.2.8 Definido sus objetivos de calidad.

2.6.2.9 Revisado el sistema de calidad.

2.6.2.10 Proporcionado los recursos adecuados.

2.6.2.11 Demostrado su el grado en que se involucra con el SGC y su mejora continua y consistente.

2.6.2.12 Comunicado a la organización la importancia del cumplimiento de los requisitos.

2.6.3 ¿Posee la empresa un procedimiento formal con respecto al control de los documentos? Este procedimiento deberá incluir:

2.6.3.1 La aprobación de los documentos antes de su publicación.

2.6.3.2 La revisión, actualización y nueva aprobación de los documentos cuando sea necesario.

2.6.3.3 La identificación de los cambios y el estado de revisión de cada documento.

2.6.3.4 La distribución adecuada de la versión vigente de los documentos relevantes en el lugar en que se usan.

2.6.3.5 Los criterios de legibilidad y los procesos de identificación de los documentos.

2.6.3.6 La forma de identificación de documentos de origen externo y el control de su distribución.

2.6.3.7 Un mecanismo que evite el uso involuntario de documentos obsoletos.

2.6.4 ¿Posee la empresa un procedimiento formal para el control de los registros de calidad? Estos registros de calidad deberán ser:

2.6.4.1 Legibles.

2.6.4.2 Fácilmente identificables.

2.6.4.3 Fácilmente recuperables.

2.6.5 El procedimiento para los registros de calidad, debe incluir instrucciones sobre su:

2.6.5.1 Identificación.

2.6.5.2 Registro.

2.6.5.3 Almacenamiento.

2.6.5.4 Protección, física y lógica.

2.6.5.5 Permiso de acceso.

2.6.5.6 Nivel de acceso.

2.11 acuerdo con las recomendaciones planteadas en la norma ISO 17021. Por cada integrante, mediante entrevista, observación y examen, se deberá:

2.11.1 Evaluar su independencia en relación con el motivo de la auditoría.

2.11.2 Identificar la experiencia necesaria (evaluación cuantitativa): años experiencia, número de auditorias realizadas, horas de formación en auditoria.

2.11.3 Considerar competencias (evaluación cualitativa): demostradas cualidades personales, conocimientos o desempeño de las habilidades en formación o en el lugar de trabajo. Debe poder ser capaz de, entre otras competencias:

2.11.3.1 Elaborar y utilizar instrumentos de diagnóstico para identificar áreas críticas y de riesgo institucional, en el marco de la normativa, las definiciones estratégicas, las características de la organización y los procedimientos internos.

2.11.3.2 Diseñar matrices de riesgo, para detectar y priorizar áreas institucionales críticas.

2.11.3.3 Incorporar al diagnóstico de la organización metas y exigencias de gestión institucionales.

2.11.3.4 Diseñar un plan de auditoría considerando, al menos, el diagnóstico y requerimientos gubernamentales, regulatorios e institucionales.

2.11.3.5 Verificar y promover la existencia y generación de sistemas de información confiables y oportunos.

2.11.3.6 Entregar periódicamente informes de recomendaciones y seguimiento a los responsables de los controles internos del Servicio, recomendando medidas para su mejoramiento.

2.11.3.7 Organizar a los usuarios internos en torno a reuniones y/o presentaciones programadas periódicamente como además, solicitar reuniones extraordinarias en el caso que sea necesario.

2.12 Asignación de responsabilidades y autoridad.

2.6.5.7 Competencia de uso.

2.6.5.8 Recuperación.

2.6.5.9 Tiempo de retención.

2.6.5.10 Destrucción.

2.7 Preparación de las actividades de auditoría en el sitio para lo cual, a partir de la información anterior, se debe identificar los sistemas o procesos que se van a auditar.

2.8 Preparación del plan de auditoría, el cual:

2.8.1 Debe ser previamente aprobado por la empresa.

2.8.2 Debe ser comunicado a el(los) auditor(es) asignado(s) y al auditado.

2.9 Elaboración del calendario de las auditorias.

2.10 Selección del equipo auditor de

2.13 Asignación de las tareas al equipo auditor.

2.14 Preparación de los documentos de trabajo.

2.15 Papel y responsabilidades de los guías y observadores.

2.16 Establecer los requisitos necesarios de confidencialidad.

3 Reunión de presentación:

3.1 La premisa fundamental es desarrollar una atmósfera de confianza.

3.2 Aclarar desde el comienzo, si es necesario, los conceptos básicos de auditoría, donde se independiza el resultado de las actividades de la habilidad

3.2.1 Lo que es la auditoría: evaluar un sistema.

3.2.2 Lo que no es la auditoría: evaluar los actores del sistema.

3.3 Presentar a los participantes.

3.4 Confirmar objeto y alcance de la auditoría.

3.5 Confirmar el plan que se va a iniciar.

3.6 Presentar la metodología de la auditoría.

3.7 Validar los medios logísticos que serán requeridos antes, durante y después de la auditoría, aclarando concreta y correctamente oportunidad de uso, forma, cantidad, asignación, responsabilidad, entrega.

3.8 Acordar la reunión de cierre.

4 Ejecución de la auditoría:

4.1 Realización de las actividades de auditoría en el sitio.

4.2 En las entrevistas, el auditor debe:

4.2.1 Presentarse, buscar inspirar confianza y calma, mostrar respeto.

4.2.2 Explicar el objetivo.

4.2.3 Explicar el método.

4.2.4 Ayudar a hablar al auditado.

4.2.5 Permitir hablar al auditado.

4.2.6 Ayuda a explicar al auditado.

4.2.7 Ayudar a resumir al auditado.

4.2.8 Escuchar, comprender, no juzgar, consagrar el tiempo necesario, permitir hablar al auditado de sí mismo, de su trabajo.

4.2.9 Formular nuevamente, discutir, no polemizar, no ser agresivo.

4.2.10 Escribir.

4.2.11 Ponerse a disposición.

4.2.12 Agradecer.

4.3 En las entrevistas el auditor puede emplear diferentes técnicas para formular preguntas, entre las que se pueden citar las siguientes:

4.3.1 Preguntas abiertas.

4.3.2 Preguntas cerradas.

4.3.3 Preguntas emocionales.

4.3.4 Preguntas engañosas.

4.3.5 Preguntas capciosas.

4.3.6 Preguntas hipotéticas.

4.3.7 Preguntas sistemáticas.

4.3.8 Preguntas múltiples.

4.3.9 Peticiones.

4.4 Comunicación durante la auditoría:

4.4.1 Las decisiones deben quedar por escrito y ser comunicadas.

4.4.2 Se debe proveer información sobre el progreso.

4.4.3 Se ha de definir cual es la información que se comunicará formalmente, periodicidad de la comunicación, establecer la prioridad de la comunicación, los medios y formatos utilizados, así como la frecuencia de la comunicación.

4.5 Recopilación y verificación de la información que permita verificar que se cumple con lo siguiente:

4.5.1 Lo establecido en los procedimientos documentados y las instrucciones de trabajo contenidos en ellos.

4.5.2 Se realizan mejoras a los procesos, de manera consistente.

4.5.3 Se conducen auditorías internas de manera periódica, de modo que se pueda verificar el ciclo completo PHVA.

4.5.4 Se realizan revisiones frecuentes por parte de la gerencia, lo que demuestra su grado de compromiso.

4.5.5 Se monitorea la consecución de los objetivos mediante, por ejemplo, resultados de encuestas; desempeño de los procesos y conformidad del producto; situación de las acciones correctivas y preventivas; seguimiento de las acciones derivadas de las revisiones anteriores de la dirección.

4.5.6 Se mantienen registros que se generan en los procesos, como evidencia.

4.6 Practicar el examen por muestreo de evidencias objetivas referidas a lo siguiente:

4.6.1 Los equipos de comunicaciones como las PBX, sistemas de correo de voz, y los IVR, y otros servicios de valor añadido que se provean, para determinar si se satisfacen las actuales exigencias del negocio y si se debería considerar posibles soluciones alternativas.

4.6.2 El proceso de compras de modo que satisfacen los requerimientos formulados, de la formulación de necesidades, precio, conveniencia, oportunidad, puntualidad en las entregas, conformidad de la entrega con las especificaciones requeridas, cantidad, capacidad, calidad del producto/servicio, suficiencia, garantía y trámite de garantías, apoyo técnico y de reclamaciones.

4.6.3 Las contrataciones de personal, subcontratación de servicios y proveedores de modo que satisfacen los acuerdos de nivel de servicio acordados, evaluación y selección, experiencia, seguridad, disponibilidad, responsabilidad, y otros atributos como dedicación, concienciación y confidencialidad (durante y después de haber terminado la relación contractual).

4.6.4 Los servicios de comunicaciones como líneas telefónicas, líneas arrendadas, servicios CENTREX y servicios contestadores, establecimiento de rutas para llamadas a teléfonos fijos y móviles, y de larga distancia, tanto nacional como internacional, y otros servicios de consultoría o gestión, para determinar si los niveles de servicio y los precios satisfacen los objetivos de la organización, y si se deben evaluar servicios alternativos o mejorados.

4.6.5 El apoyo técnico, físico, lógico y administrativo para los servicios prestados, con la finalidad de comprobar el grado de satisfacción del cliente, acuerdos de nivel de servicio, definición de ámbito, alcances, inclusiones y exclusiones del servicio, métricas de servicio, cumplimiento de las condiciones de uso, indicadores, otros.

4.6.6 La gestión de la seguridad de la red, monitoreo y control, gestión de los requerimientos del negocio para el control de acceso, tanto físico como lógico, a las aplicaciones y sistemas, y control criptográfico.

4.6.7 Definición, preparación, mantenimiento de áreas seguras y protegidas, y seguridad de los equipos, así como la gestión de su seguridad, personalizada por usuario.

4.6.8 La fiabilidad de la interconexión con otros operadores, señalización y conmutación, escalamiento de problemas.

4.6.9 Respaldo de datos y protección del medio, tecnología o método empleado.

4.6.10 Planeamiento del crecimiento en infraestructura en relación con incremento en el número de clientes y los nuevos requerimientos de éstos.

4.6.11 Cambios en la tecnología subyacente, y su apropiado registro y actualización de la documentación pertinente. Estos cambios pueden referirse a modificaciones en las configuraciones, actualizaciones de software por funcionalidad o seguridad. También pueden darse como resultado de una vigilancia tecnológicaen la empresa. Una vigilancia tecnológica es una forma organizada, selectiva y permanente de captar información del exterior sobre tecnología, analizarla y convertirla en conocimiento para tomar decisiones con menor riesgo y poder anticiparse a los cambios.

4.6.12 Con respecto a la seguridad de la información (ISO 27001:2005), se debe evaluar que en los sistemas de información y servicios implantados, en general, se satisface la:

4.6.12.1 Confidencialidad, propiedad por la cual la información no esté disponible ni sea divulgada a individuos, organismos o procesos no autorizados. El énfasis de la norma ISO 27011 en empresas de telecomunicaciones es: "*La Información relacionada con organizaciones de telecomunicaciones debería ser protegida de una revelación no autorizada. Esto implica el secreto de las comunicaciones en términos de existencias, contenido, fuente, destino, así como en la fecha y hora de la información comunicada. Es crítico que las empresas de telecomunicaciones aseguren que su implementación del secreto de las comunicaciones no sea violada. Las personas encargadas por la empresa de telecomunicaciones deberían mantener la confidencialidad de cualquier información que añade a terceros y que haya sido de su conocimiento durante el desempeño de sus labores*".

4.6.12.2 Integridad, propiedad de proteger la precisión y la totalidad de los activos. El énfasis de la norma ISO 27011 en empresas de telecomunicaciones es: "*La instalación y uso de las instalaciones de telecomunicaciones deberían ser controladas, para asegurar su autenticidad, exactitud y entereza de la información transmitida, reenviada o recibida, y a sea por medios alámbricos, inalámbricos u otros métodos*".

4.6.12.3 Disponibilidad, propiedad de estar accesible y ser utilizable a demanda por parte de un organismo autorizado. El énfasis de la norma ISO 27011 en empresas de telecomunicaciones es: "*Solo se debería proporcionar acceso autorizado cuando sea necesario a la información de telecomunicaciones, instalaciones y el medio utilizado para la provisión de los servicios de telecomunicaciones ya sea que éstos se provean por medio alámbrico, radio, o cualquier otro método. Como una extensión a la disponibilidad, las empresas de telecomunicaciones deberían brindar prioridad a las comunicaciones esenciales en caso de emergencia y satisfacer los requerimientos del organismo regulador*".

4.6.12.4 Autenticidad, imposibilidad de rechazo, consistencia, aislamiento, auditoría de los datos.

4.6.12.5 Autenticación, provisión de seguridad de que es correcta la supuesta característica de una entidad.

4.6.12.6 Rendición de cuentas (accountability).

4.6.12.7 No repudio, habilidad de probar la ocurrencia de un supuesto evento o acción, y sus entidades originales, con la finalidad de resolver disputas sobre la ocurrencia o no ocurrencia de un evento o acción y la partición de entidades en el evento.

4.6.12.8 Fiabilidad, propiedad de obtener un comportamiento y resultados predeterminados de manera consistente.

4.6.13 Medidas y contra medidas, físicas, lógicas, administrativas o legales, adoptadas para identificar y reducir vulnerabilidades y/o amenazas de manera efectiva. Estas vulnerabilidades y/o amenazas pueden ser tanto técnicas, humanas o de código malicioso.

4.6.14 Gestión de incidentes o debilidades, efectividad del sistema de reclamaciones.

4.6.15 Gestión de la continuidad del negocio, con la participación general y comprometida de todos los colaboradores, colaboración y confianza mutua, capacidad y valores de todas las personas. Establecimiento de políticas y medidas de seguridad y continuidad del negocio en caso de desastres naturales.

4.7 Las evidencias pueden existir en cualquier tipo de soporte o medio, ya sea físico, electrónico o digital, audible o visual. Ejemplos de evidencias son:

4.7.1 Políticas: orientación directiva de la empresa - Real Academia Española (RAE).

4.7.2 Normas: reglas de cumplimiento obligado -RAE.

4.7.3 Manuales: libro que recoge lo esencial o básico de una materia -RAE- (operación).

4.7.4 Procedimientos: método o sistema estructurado para ejecutar algunas cosas -RAE- (instalación, configuración, mantenimiento, verificación).

4.7.5 Registros: libro, a manera de índice, donde se apuntan noticias o datos -RAE- (controles, alarmas, implementaciones, modificaciones, actualizaciones, órdenes de compra o servicio, listados de proveedores y productos).

4.7.6 Contratos: pacto o convenio, oral o escrito, entre partes que se obligan sobre una materia o cosa determinada (acuerdos de nivel de servicio además).

4.7.7 Indicadores: datos o conjunto de datos que ayudan a medir objetivamente la evolución de un proceso o de una actividad. Se sugiere emplear la herramienta 5W-1H para definir un indicador.

4.7.8 Mediciones. Medición es la acción y efecto de medir, de comparar una cantidad con su respectiva unidad, con el fin de averiguar cuántas veces la segunda está contenida en la primera.

4.7.9 Aprobaciones (visto bueno).

4.8 Tres ejes de observación sobre la información:

4.8.1 La forma:

4.8.1.1 Conformidad con el procedimiento de la empresa.

4.8.1.2 Identificación clara y correcta del material, documentación, otros.

4.8.2 El fondo:

4.8.2.1 Cubrimiento del tema con suficiencia, propiedad, corrección, exactitud, oportunidad, claridad.

4.8.2.2 Conciencia del contexto de modo tal que se obtenga información relevante de la tarea y/o servicios.Según Dey &Abowd [12], contexto es cualquier información que puede ser usada para caracterizar la situación de una entidad, donde una entidad puede ser una persona, el lugar, o el objeto físico o computacional.

4.8.2.3 Exactitud de las referencias a otros documentos.

4.8.2.4 Secuencia adecuada.

4.8.2.5 Coherencia.

4.8.2.6 Actualizada.

4.8.2.7 Aprobaciones.

4.8.3 La aplicación:

4.8.3.1 Difusión correcta, completa, pertinente, oportuna, autorizada.

4.8.3.2 Implementación efectiva.

4.9 Tres criterios de evaluación:

4.9.1 La existencia (de los registros y material de comprobación necesarios).

4.9.2 La práctica (la ejecución de tareas siguiendo los procedimientos escritos correspondientes).

4.9.3 La apropiación (grado en que la empresa ha hecho suya el proceso en su totalidad).

5 Finalización de la auditoría.

6 Reunión de clausura y cierre.

7 Elaboración del informe:

7.1 Generación de hallazgos del auditor.

7.2 Preparación del informe de la auditoría. Este informe traduce fielmente las conclusiones de la reunión de cierre y contiene:

7.2.1 El alcance y el objetivo de la auditoría.

7.2.2 La fecha de la auditoría.

7.2.3 La conformación del equipo auditor.

7.2.4 Los documentos de referencia.

7.2.5 Las observaciones realizadas (no implica desviación ni incumplimiento de requisitosy constituye una oportunidad de mejora).

7.2.6 Las no conformidades detectadas (según la ISO 9000:2005, es el incumplimiento de un requisito y no se presupone que el producto o servicio tenga defectos).

7.2.7 Los defectos encontrados (según la ISO 9000:2005, es el incumplimiento de un requisito asociado a un uso previsto o especificado).

7.2.8 Los puntos fuertes de la actividad.

7.2.9 Una solicitud de acción correctiva.

7.3 Aprobación y distribución del informe de la auditoría.

8 Presentación y comunicación de los resultados.

8.1 Preparación de las conclusiones de la auditoría:

8.1.1 Resumen de los puntos fuertes y débiles del sistema auditado.

8.1.2 Formula una opinión sobre las acciones prioritarias que hay que iniciar.

8.1.3 Es la única parte subjetiva del informe.

8.2 Preparación, aprobación y distribución del informe de la auditoría. Las comunicaciones deben ser precisas, objetivas, claras, concisas, constructivas, completas y oportunas.

9 Comprobación y seguimiento:

9.1 El auditor:

9.1.1 Acuerda la fecha de la auditoría de seguimiento.

9.1.2 Desarrolla la auditoría de seguimiento de acuerdo con las acciones correctivas y preventivas propuestas.

9.1.3 Presenta el informe de auditoría.

9.2 El auditado:

9.2.1 Propone y desarrolla las acciones correctivas y preventivas, de acuerdo con las no conformidades detectadas durante la auditoría.

9.2.2 Establece la fecha de implantación de acciones.

9.2.3 Desarrolla las acciones correctivas correspondientes.

9.3 Evaluación posterior del desempeño del auditor. Por ejemplo, utilizando encuestas.