TIPO DE INFORME: GENERAL ☐

PROCESO ☐ NOMBRE: GESTION DE TECNOLOGIA INFORMATICA

1. INFORMACIÓN GENERAL

Fecha auditoría: Agosto 01 de 2017

Responsable de atender auditoría: Bernabé Sanchez Lenis – Auxiliar informática y telecomunicaciones

Hora de Inicio: 2:57 PM

Hora Finalización: 4:26 PM

Nombres del equipo auditor:

- Sandra Milena Moreno Gamboa
- Alvaro David Rodriguez Cardenas

2. OBJETIVO DE LA AUDITORÍA

El objetivo de la auditoria fue evaluar y verificar la eficacia, implementación y mantenimiento del Sistema de Gestión de Calidad, con el fin de identificar oportunidades de mejora frente a los requisitos Norma ISO 9001:2008, NTCGP 1000:2009 el MECI 1000:2014 considerando adicionalmente los procedimientos relacionados a los procesos, riesgos, controles, indicadores y planes de mejora.

3. ALCANCE:

Verificar el cumplimiento de los requisitos de las normas ISO 9001:2008, NTCGP 1000:2009 y MECI, así como la efectividad de las medidas implementadas para la mejora continua en cada uno de los procesos de la Empresa Oficial de Servicios Públicos de Yumbo S.A ESP.

4. CRITERIOS

DOCUMENTACION ANALIZADA Y REQUISITOS DE ENTRADA:

1. Norma NTCGP 1000:2009: Sistema de Gestión de la calidad
2. Registros de cada actividad.
3. Caracterización del proceso

La auditoría a Gestión Gerencial se desarrolló con base en los siguientes criterios, como referentes para la verificación de las evidencias de las auditorías: MECI, NTCGP 1000:2009; NTC ISO 9001:2008; la documentación del Sistema de Gestión; Constitución Nacional y demás normatividad vigente relacionada.

5. DESARROLLO AUDITORIA

Se revisó los requisitos generales del sistema de gestión de calidad, verificando la caracterización del proceso de "GESTION DE TECNOLOGIA INFORMATICA" y se realizaron preguntas que conllevaran a la identificación del cumplimiento de lo planteado en la caracterización del proceso, a continuación se detallan las preguntas, con sus respectivos comentarios y observaciones encontradas.

- ¿Teniendo **en cuenta el plan de acción institucional, evidenciar cual es el plan de acción del área para el fortalecimiento de la infraestructura tecnológica?**

Conforme: SI
Observaciones: existe un plan de acción y el mismo esta elevado a resolución en gerencia

- ¿Teniendo **en cuenta la planificación de los respaldos y/o Backus, favor evidenciar el proveimiento por medio del cual se realiza esta labor?**

Conforme: SI
Observaciones: en el plan de acción del área está establecido el procedimiento.

- ¿teniendo **en cuenta el procedimiento de Backus, favor evidenciar como se realiza la verificación, mediante la cual se evidencie que los respaldos realizados son 100% fiables, mostrar procedimientos y demás soportes?**

Conforme: NO

106

Observaciones: este procedimiento lo hace directamente el proveedor del software (ACTSIS) mas no se tiene el detalle de cómo se realiza el procedimiento, y de igual forma no está el procedimiento.

- **cuál es el procedimiento por medio del cual, cualquiera de las áreas de la empresa, solicita un requerimiento al área Informatica, evidenciar documentos y soportes.**

Conforme: NO
Observaciones: este procedimiento no está documentado, existe un sistema de help desck (mesa de ayuda) que solo es operada por el área de sistemas, en múltiples ocasiones el área de sistemas ha intentado que los usuarios utilicen esta herramienta para solicitar el soporte del área de sistemas, pero no se ha podido implementar, ya que los usuarios no usan la herramienta Informatica.

- **¿evidenciar el procedimiento para el manejo de los requerimientos realizados por los usuarios de la empresa?**

Conforme: NO
Observaciones: en este momento no existe un control, mediante el cual se pueda verificar el cumplimiento o no de lo planteado en el plan de comunicaciones.

- **¿se está aplicando en la actualidad los formatos registrados en los Documentos y registros de la caracterización del proceso?**

Conforme: NO
Observaciones: No existe procedimiento.

- ¿en **la actualidad para el manejo de los requerimientos (Help Desk), se tiene en cuenta alguna de las politicas de ITIL, norma ISO 20000 y/o otros en caso de otros, indicar cuáles?**

Conforme: NO
Observaciones: no existe el procedimiento, el funcionario lo realiza de acuerdo a los conocimientos y consideraciones que se crean pertinentes.

- **¿En la actualidad, la empresa cuenta con alguna de las politicas de gestión de seguridad de la información de acuerdo a la NORMA ISO 27000 y/o ITIL.?**

Conforme: SI
Evidencia Objetiva: El servidor no se encuentra bajo las condiciones mínimas de seguridad que este debería de tener.
Observaciones: ene l plan de acción se tienen contempladas normal legales y otros.

- **¿teniendo en cuenta los requerimientos realizados al área de Informatica, se tiene algún informe en el cual se puede identificar, cuales son los problemas más frecuentes en la empresa, los cuales sirvan de insumo para el mejoramiento continuo de las plataformas informáticas?**

Conforme: NO
Observaciones: al haber 1 sola persona que atienda todo el área Informatica, no todos los requerimientos son documentados o alimentados en la plataforma destinada para tal fin, lo que conlleva a que los informes y/o documentos que se generen, no necesariamente son validados y analizados de acuerdo a los requerimientos que se tiene registrados.

- **¿teniendo en cuenta las directrices nacional sobre Gobierno en línea, evidenciar que el área Informatica de la empresa, este cumpliendo con este lineamiento nacional?**

Conforme: SI
Observaciones: el plan estratégico lo tiene contemplado

¿Evidenciar cuál es el procedimiento por medio del cual, se realizan la verificación y análisis del tráfico de la red, para monitoreo y solución de fallas?

Conforme: NO
Observaciones: no existe el procedimiento, este está en construcción.

¿Cuál es la periodicidad por la cual, se realiza mantenimiento preventivo y/o correctivo a los servidores de la empresa?

Conforme: SI
Observaciones: este mantenimiento preventivo se realiza cada 6 meses.

¿Evidenciar el procedimiento por medio del cual se realiza el mantenimiento preventivo y/o correctivo a los servidores?

Conforme: NO
Observaciones: no existe un procedimiento estipulado para realizar este mantenimiento, se realiza a consideración del responsable del área Informatica.

109

¿Cuál es el procedimiento por medio del cual, se vincula un usuario nuevo a la red privada de la empresa, evidenciar procedimiento?

Conforme: NO
Observaciones: no existe un procedimiento documentado.

Indique cuales son los indicadores del proceso

Conforme: No
Observaciones: La Herramienta Help Desk Provee indicadores de fechas y periodicidad, con gráficas y demás indicadores, pero dado que dicha herramienta no está siendo utilizada por los usuarios, no hay manera de obtenerlos.

Evidenciar Donde se llevan los controles para verificar que las actividades plateadas

Conforme: Si
Observaciones: Se evidencia matriz de seguimiento la cual deberá ser perfeccionada.

Se lleva un control de las acciones de mejora que se realiza o se requieren en la empresa, evidenciar informe o documentos relacionados.

Conforme: No
Observaciones: No existe un informe donde se desglosen las mejoras y requerimientos de la empresa

6. ASPECTOS RELEVANTES:

- Todo lo que enmarca el área de sistemas y telecomunicaciones está a responsabilidad de una (01) persona, lo que en muchas ocasiones puede dar lugar a demoras en la ejecución de los trabajos y actividades planificadas; se aclara que se puede demorar no por el desconocimiento de la persona responsable, si no por las múltiples tareas que pueda llegar tener que le imposibiliten cumplir a cabalidad con sus actividades.

- El sitio donde se encuentra en la actualidad los servidores no cumplen con las condiciones mínimas de seguridad que estos deberían de tener, como las siguientes:

  - El área donde se encuentran los servidores debe ser un espacio que no sea combustible o inflamable.
  - La temperatura no debe de sobrepasar los 18° C y el límite de humedad no debe de superar el 65 % para evitar el deterioro.
  - Debe de estar en un lugar con techo impermeable para evitar el paso del agua

104

- Debe de estar en un lugar totalmente cerrado, sin acceso al personal en general

Como punto final se recomienda tener en cuenta las siguientes normas ISO asociadas a la seguridad Informatica y de telecomunicaciones.

- ISO/IEC 27001: proporciona un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).
- ISO/IEC 27002: proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener un Sistema de Gestión de la Seguridad de la Información (SGSI).
- ISO/IEC 27005: proporciona directrices para la gestión del riesgo de seguridad de la información en una organización. • Directrices de la OCDE (Organization for Economic Co-operation and Development) para la seguridad de sistemas y redes de información: Hacia una cultura de seguridad.

7. ASPECTOS POR MEJORAR:

- Levantar procedimiento que al momento de la auditoria no se encontraron o no existen.

8. NO CONFORMIDADES

- No existe el procedimiento por medio del cual se pueden verificar que los Backus que se generan en la ESPY son 100% confiables.
- No existe el procedimiento por medio del cual se detalle cómo se deben de ingresar los Requerimientos o incidencias al área Informatica.
- No se realizan informes por parte del área Informatica, teniendo en cuenta los requerimientos y/o incidencias reportadas por los usuarios, realizando análisis y conclusiones para una toma de decisiones por parte de la gerencia.
- No existe un procedimiento por medio del cual se hagan las verificaciones, análisis y/o correcciones para el monitoreo de la red y posibles fallas.
- No existe un procedimiento por medio del cual se realicen los mantenimientos a los servidores y equipos de cómputo de la ESPY.
- No existe un procedimiento por medio del cual se detalle cómo se debe de vincular un usuario a la red interna y usuarios del software comercial y financiero de la ESPY.
- No existen los indicadores del proceso.

9. CONCLUSIÓN

La persona auditada conoce todo el procedimiento y las labores propias del proceso, pero no existe la mayoría de los procedimientos del proceso de GESTION DE TECNOLOGÍA INFORMATICA, lo que conlleva a que se realicen labores a consideración del personal de turno.

FIRMA AUDITOR LIDER:

ALVARO DAVID RODRIGUEZ CARDENAS

FIRMA AUDITOR(ES) ACOMPAÑANTE:

SANDRA MILENA MORENO GAMBOA

Pedro Pablo Erazo R
Jefe Oficina Control Interno