ASEJ
AUDITORÍA SUPERIOR DEL ESTADO DE JALISCO
PODER LEGISLATIVO

INFORME FINAL DE AUDITORÍA

Auditoría interna del 27 – 29 de Octubre del 2015
No: 001/2015

Fecha: 30 / Octubre / 2015.

Durante los días del 27 al 29 de Octubre del 2015 se llevó a cabo la Primer auditoría interna del año, al Sistema de Gestión de la Seguridad de la Información de acuerdo a los siguientes puntos:

Objetivo: El objetivo de esta primer auditoria interna al Sistema de Gestión de la Seguridad de la Información. (SGSI) es verificar el nivel de implantación y eficacia del mismo, conforme a los requerimientos de los estándares internacionales ISO/IEC 17021:2011 e ISO 19011:2011, verificando pues Fase I, documental y Fase II eficacia del SG.

Alcance: El alcance de la auditoria son todas las áreas, todos los procesos relacionados al alcance definido para el SGSI.

Criterios aplicados: Los criterios base los cuales se desarrolla este ejercicio de auditoria son:
Los establecidos por la Organización
Los obligados por legislación y normatividad
Los debes y requisitos dentro del estándar ISO/IEC 27001:2013

Auditor/a líder: David Garcia Gonzalez

Equipo auditor: N/V

Auditores/as en entrenamiento:
Minerva Ascencio Ramirez
Roberto Fernández

Desarrollo:

A continuación se presenta un resumen de las actividades realizadas en la auditoría:

FECHA	ACTIVIDAD	OBSERVACIONES
27-10-2015	Auditoria Fase I (verificación Documental) Contexto de la Organización, Expectativas de las partes interesadas Sistema de Gestión	La Organización cuenta con la información documentada que soporta las operaciones del SGSI, dentro del manual de seguridad de la información MSI, ***(MSI-PS-SI-01).*** Se cuenta con análisis de contexto, identificación de las expectativas de las partes interesadas, identificación de alcance y exclusiones aplicables al SGSI, OFI: /área de oportunidad) ***Dentro del análisis de las expectativas de las partes interesadas es necesario identificar los riesgos y vulnerabilidades que puedan afectar la conformidad en el cumplimiento de estas expectativas, si bien la organización cuenta con metodología documentada para la gestión del riesgo, esta metodología está orientada a los activos de la organización dejando de lado la gestión del riesgo orientado como se dijo anteriormente hacia las expectativas de las partes interesadas.*** ***NCm: / No conformidad Menor*** ***A la gestión de las operaciones no se muestra evidencia al cumplimiento de políticas y procedimientos documentados para la gestión de las tecnologías de la información TIC´s. así mismo se detecta que la documentación referida dentro del SoA no se encuentra terminada y autorizada.***

27-10-2015	Registros y procedimientos aplicables al estándar	La Organización cuenta con soporte documental a su SGSI para lo cual toma como modelo base de gestión documental lo declarado en su Sistema de Gestión de la Calidad, SGC. ***NCm: / No conformidad Menor*** ***Si bien la organización cuenta con la documentación soporte al SGSI, no muestra la conformidad con lo establecido en su procedimiento documentado para el control de documentos.*** PG-PS-GC-02 Rev- 09 del 04- sep-2015. ***La documentación soporte al SGSI no ha sido autorizada***

27-10-2015	Alcance del SGSI	La Organización cuenta con alcance y exclusiones al SGSI documentadas dentro de su Manual de la Seguridad de la Información, así mismo las exclusiones están declaradas e identificadas dentro del acuerdo de aplicabilidad SoA.
27-10-2015	Objetivos del SGSI	La Organización cuenta con objetivos documentados ante el SGSI conforme a lo requerido en el apartado 6.2 los cuales se encuentran orientados a la seguridad de la información. ***NCm: / No conformidad Menor*** ***Si bien la organización cuenta con la documentación soporte orientada a los objetivos de seguridad de la información no se muestra evidencia de la medición y monitorea que permita validar la eficacia y alcance en las metas orientadas hacia estos objetivos declarados.***
28-10-2015	Metodología para la gestión del riesgo Inventario de activos SoA	La Organización cuenta con método documentado para la gestión del riesgo el cual se apega a los apartado 6.1, 6.1.2 y 6.1.3,

28-10-2015 Y 29-10-2015	Acuerdo de Aplicabilidad SoA	La Organización cuenta con soporte documentado con referencia a la gestión de controles del anexo A de la norma ISO/IEC 27001:2013 donde se establezca motivo de la selección de controles, documentación soporte de referencia, método de medición y monitores. ***NCm: / No conformidad Menor*** ***Si bien la organización cuenta con la documentación soporte a su SGSI y esta se encuentra relacionada dentro del SoA, control, documento, política, procedimiento. No se cuenta con evidencia de la medición a los indicadores establecidos a cada control y dominio de control dentro del SoA. Por lo tanto no se cuenta con evidencia a la eficacia del SGSI y sus controles implementados***
28-10-2015 y 29-10-2015	Competencias	La organización cuenta con procedimientos documentados orientados a la selección, contratación de personal y/o capital humano, para lo cual se toma como modelo base los requerimientos legislativos y lo declarado dentro de su SGC, así mismo se cuenta con procedimientos documentados para la gestión de los roles y responsabilidades ante los sistemas de gestión. ***NCm: / No conformidad Menor*** ***Si bien la organización cuenta con la documentación soporte orientada a los roles, responsabilidades gestión del personal y las competencias.*** ***No se muestra conformidad en la conciencia ligada al personal de la organización para con el SGSI.***

ASEJ: Primer Auditoria Interna al SGSI efectuada del 27 al 29 de Octubre del 2015 :

Durante el ejercicio de la auditoria efectuada a todas las áreas operativas del ASEJ conforme al alcance documentado para su SGSI, entre las principales áreas auditadas se encuentran:

Área encargada de los SG: a la cual se audito los apartados:

4. contexto de la organización
4.1 comprendiendo a la organización y su contexto
4.2 comprendiendo a las necesidades y expectativas de las partes interesadas
Donde se detecta una OPORTUNIDAD de MEJORA OFI: con referencia a fortalecer la identificación y riesgo asociado a la conformidad de las expectativas de las partes interesadas.

4.3 determinación del alcance del SGSI
4.4 SGSI y soporte documental al mismo
NC m (durante el proceso de auditoría de detecta que la documentación soporte del SGSI no se encuentra autorizada conforme a lo establecido en procedimiento de control de documentos).

5. (5.1) liderazgo y compromiso

Todas las Áreas de la ASEJ
5.2 política del SGSI NC m (Durante el ejercicio de auditoria se detectó la necesidad de fortalecer el conocimiento del SGSI entre el personal dentro del alcance así como la concientización entre los roles y responsabilidades del personal para con las políticas y procedimientos documentados al SGSI).

6 planeación del SGSI
6.1.1 generalidades del SGSI y la gestión del riesgo orientado a partes interesadas y expectativas de estos.
6.1.2 método para la evaluación del riesgo
6.1.3 método para el tratamiento del riesgo
6.1.3 d) Acuerdo de Aplicabilidad SoA NC m (Durante el proceso de auditoría al SGSI en la verificación de controles aplicados, vs políticas y procedimientos documentados en referencia no se mostró evidencia de la eficacia del SGSI mediante sus políticas y procedimientos documentados esto conforme a las métricas e indicadores establecidos dentro del documento SoA).

6.2 Objetivos del SGSI NC m (Durante el proceso de auditoria no se mostró evidencia de la conformidad a los indicadores establecidos y ligados a los objetivos del SGSI.

Área encargada de los SG: a la cual se audito los apartados:

7.1 provisión de recursos
7.2 gestión de las competencias véase NC m del Apartado 5.2
7.3 gestión de la concientización
7.4 comunicación
7.5 Información documentada véase NC m del apartado 4.4

Arreas auditadas: Área encargada de los SG y área de tecnologías de la información:

8.1 Funcionamiento
8.1 planificación y control operacional NC m (Durante el proceso de auditoria se detecta que la documentación ligada a la gestión de tecnologías de la información no se encuentra terminada, autorizada y liberada por lo que no fue posible evidenciar el cumplimiento a la gestión, operación y funcionalidad del SGSI.

8.2 evaluación del riesgo (soporte documental de los resultados de la evaluación)

8.3 información documentada (del resultante de los planes de tratamiento del riesgo).

Área encargada de los SG:

9.1 seguimiento, medición, análisis y evaluación véase NC m del 6.1.3 d) SoA
9.2 Auditorías Internas
9.3 Revisión por la dirección
10 mejora continua del SGSI

Arreas auditadas: Área encargada de los SG y área de tecnologías de la información:

Anexo A ligado al Acuerdo de Aplicabilidad SoA,

Véase NC m del apartado 8.1 y 6.1.3 d)

Hallazgos generales:
5 No Conformidades de Carácter Menor (m)
1 área de oportunidad (OFI) / observación (O)

Observaciones adicionales:
La organización cuenta con el soporte documental al SGSI y su alcance declarado, sin embargo es necesario fortalecer la concientización con el personal de la ASEJ en cuanto a sus roles y responsabilidades para con el SGSI, políticas y procedimientos declarados, de igual manera es importante realizar la autorización y liberación oficial de esta documentación conforme a los establecido en sus procedimientos y políticas declaradas para este fin.,

Es de suma importancia dar seguimiento a la revisión de controles aplicados mediante sus métricas establecidas y con esto verificar la eficacia del SGSI, y por ende el apego y cumplimiento a los Objetivos de Seguridad declarados ante el SGSI.

David García Gonzalez.
A.L. (Auditor Líder)

Distribución:

C.c.p. (Unidades administrativas a las que se les entrega el informe).