



American Trust Register, S.C.
Organismo Certificador de Sistemas de Gestión

INFORME DE AUDITORÍA DE CERTIFICACIÓN ETAPA 1

del

Sistema de Gestión de Seguridad en la
Información

de

AUDITORIA SUPERIOR DEL ESTADO DE
JALISCO

Dirección: Av. Niños Héroes no. 2409 Col.
Moderna Guadalajara, Jalisco.

Teléfono: (33) 3679-4500 Ext. 1823 ó 1845

Fecha: 1 de Diciembre de 2015

EQUIPO AUDITOR

Auditor Líder:	Lic. Alexandro Fernández Rodríguez
Grupo Auditor:	Lic. Cristian Luna
Experto Técnico:	No aplica
Auditor en Entrenamiento:	No aplica
Auditor Evaluador:	No aplica
Observador:	No aplica



INFORME DE AUDITORÍA ETAPA 1

CLAVE DE AUDITORÍA
MA-01

NÚMERO DE CLIENTE
ASJ-1268

NORMAS DE REFERENCIA	
<input type="checkbox"/> NMX-CC-9001-IMNC-2008 (ISO 9001:2008)	<input type="checkbox"/> NMX-SAA-14001-IMNC-2004 (ISO 14001:2004)
<input type="checkbox"/> NMX-SAST-001-IMNC-2008 (BSI OHSAS 18001:2007)	<input type="checkbox"/> NMX-F-CC-22000-NORMEX-IMNC-2007 (ISO 22000:2005)
<input checked="" type="checkbox"/> NMX-I-27001-NYCE-2009 (ISO/IEC 27001:2013)	

LUGAR DE AUDITORÍA ETAPA 1	
<input type="checkbox"/> En sitio	<input checked="" type="checkbox"/> En gabinete

FECHA PROPUESTA PARA LLEVAR A CABO LA AUDITORÍA DE ETAPA 2
La fecha propuesta es: 2 al 8 de Diciembre 2015
NOTA: La fecha propuesta no debe pasar de 90 días naturales

CONFIRMACIÓN RELACIONADA CON LA INFORMACIÓN PROPORCIONADA POR EL CLIENTE
Información Correcta: Si (X) No ()
Diferencias en la información proporcionada: Haga clic aquí para escribir texto.
Acciones tomadas derivadas de la diferencia: Haga clic aquí para escribir texto.

ALCANCE DE LA CERTIFICACIÓN ACORDADO CON EL CLIENTE	
ALCANCE DEL SISTEMA DE GESTIÓN	El alcance del SGSI aplica a Auditorías a entidades auditables, capacitación de servidores públicos, profesionalización de servidores públicos, procesos de transparencia, procesos administrativos, sistemas de gestión, informáticas.
LISTADO DE PROCESOS QUE INTEGRAN EL SG	Planeación estratégica, Auditoría a entidades auditables, Responsabilidades, Auditor Especial de cumplimiento financiero, Administración, Dirección técnica, Unidad de Transparencia, Asuntos jurídicos, Sistemas de gestión.
LISTADO DE PRODUCTOS Y/O SERVICIOS QUE SE INCLUYEN EN EL SG	Pliegos de Recomendaciones, Auditorías a la entidades, Capacitaciones a externos, capacitaciones a internos, documentos de transparencia.
INSTALACIONES DENTRO DEL ALCANCE	
INSTALACIÓN	PROCESO(S), ACTIVIDAD(ES), ELEMENTO(S)
Se cuenta con una instalación ubicada en Av. Niños Héroes no. 2409 Col. Moderna Guadalajara, Jalisco.	Planeación estratégica, Auditoría a entidades auditables, Responsabilidades, Auditor Especial de cumplimiento financiero, Administración, Dirección técnica, Unidad de Transparencia, Asuntos jurídicos, Sistemas de gestión.



SITIOS MUESTREABLES DENTRO DEL ALCANCE:	
SITIO MUESTREABLE	PROCESO(S), ACTIVIDAD(ES), ELEMENTO(S)
No hay sitios muestreables dentro del alcance del SGSI	N/A

EVALUACIÓN DE LA DOCUMENTACIÓN BÁSICA DEL SISTEMA DE GESTIÓN

DOCUMENTO	ASPECTO A EVALUAR	CUMPLE		HALLAZGO
		Si	No	
POLITICA DE GESTIÓN	<p>La alta dirección debe establecer una política de seguridad que:</p> <p>a) es apropiada al propósito de la organización;</p> <p>b) incluye objetivos de seguridad de la información (ver 6.2) o provee el marco de trabajo para establecer los objetivos de seguridad de la información;</p> <p>c) incluye el compromiso para satisfacer requerimientos aplicables y relacionados con seguridad de la información; e</p> <p>d) incluye el compromiso para la mejora continua del sistema de gestión de seguridad de la información.</p> <p>La política de seguridad de la información debe:</p> <p>e) estar disponible como información documentada;</p> <p>f) estar comunicada dentro de la organización; y</p> <p>g) estar disponible a las partes interesadas.</p>	X		
CONTROL DE LA INFORMACIÓN DOCUMENTADA	<p>7.5.1 General</p> <p>El sistema de gestión de seguridad de la información de una organización debe incluir:</p> <p>a) información documentada requerida por el estándar internacional ISO 27001; e</p> <p>b) información documentada que haya determinado la organización como necesaria para la efectividad del sistema de gestión de seguridad de la información.</p> <p>NOTA El alcance de la información documentada para un sistema de gestión de seguridad de la información puede diferir de una organización a otra debido a:</p> <p>1) el tamaño de la organización y su tipo de actividades, procesos, productos y servicios;</p> <p>2) la complejidad del proceso y sus interacciones; y</p> <p>3) la competencia de las personas</p>	X		
PROCEDIMIENTO DE AUDITORÍA INTERNA	<p>La organización debe realizar auditorías internas a intervalos planeados para proveer información en su sistema de gestión de seguridad de la información:</p> <p>a) está conforme a:</p> <p>1) Los requerimientos de la organización para su sistema de gestión de seguridad de la información; y</p> <p>2) los requerimientos del estándar Internacional ISO 27001;</p> <p>b) es efectivamente implementado y mantenido.</p> <p>La organización debe:</p> <p>c) planear, establecer, implementar y mantener un programa de auditoría(s), incluyendo la frecuencia, método, responsabilidades, requerimientos de planeación y reportes. El programa de auditoría debe considerar la importancia de los procesos relacionados y los resultados de las auditorías previas;</p> <p>d) definir los criterios de auditoría y el alcance para cada auditoría;</p> <p>e) elegir auditores y realizar auditorías que aseguren objetividad e imparcialidad del proceso de auditoría;</p> <p>f) asegurar que los resultados de las auditorías son reportados a la alta dirección; y</p> <p>g) retener información documentada como evidencia del programa de auditoría(s) y</p>	X		



	los resultados de la auditoría.			
PROCEDIMIENTO DE ACCIONES CORRECTIVAS Y PREVENTIVAS	<p>Cuando una no conformidad ocurre, la organización debe:</p> <p>a) reaccionar a la no conformidad, según corresponda</p> <p>1) tomar acción(es) para controlar y corregir; y</p> <p>2) tratar las consecuencias;</p> <p>b) evaluar la necesidad de acción para eliminar las causas de las no conformidades, con el fin de que no vuelva a ocurrir o se produzca en otro lugar, por:</p> <p>1) revisar la no conformidad;</p> <p>2) determinar las causas de la no conformidad; y</p> <p>3) determinar si existen no conformidades similares, o si potencialmente puedan ocurrir;</p> <p>c) implementar cualquier acción necesaria;</p> <p>d) revisar la efectividad de las acciones correctivas llevadas a cabo; y</p> <p>e) realizar cambios al sistema de gestión de seguridad de la información, si es necesario.</p> <p>Las acciones correctivas deben ser apropiadas para los efectos de las no conformidades encontradas.</p> <p>La organización debe retener información documentada como evidencia de:</p> <p>f) la naturaleza de la no conformidad y cualquier acción subsecuente, y</p> <p>g) los resultados de cualquier acción preventiva.</p>	X		

Aspecto a Evaluar	Evidencias Presentadas	Resultado de la Evaluación	Cumple		Hallazgo
			Si	No	
Revisión por la Dirección	Manual del Sistema de Gestión de Seguridad de la Información Procedimiento de Revisión de Direcciones PG-AS-AS-02 Informe de Revisión por la Dirección 9.3	<p>En el punto MGS1 9.3 Revisión por la Dirección, la ASJ establece que La Alta Dirección revisa el avance del Sistema de Gestión de la Seguridad de la información conforme a su planeación, siendo preferentemente después de obtener los resultados de una auditoría interna o externa, con el fin de contar con información reciente del funcionamiento del sistema.</p> <p>De igual forma, cuentan con el procedimiento "Revisión de Direcciones PG-AS-AS-02" donde se establecen los lineamientos que se deberán seguir al respecto.</p> <p>Algunos de los requisitos de la norma ISO 27001, en sus incisos b), c) 2) y 4) y el d) no es clara la evidencia y los resultados presentados, por lo que se invita a complementar la evidencia para verificarla en sitio.</p>	X		
Auditoría Interna	Procedimiento de Auditoría Interna PG-PS-GC-04	Procedimiento alineado a los Sistemas de Gestión de la Organización, incluye las fases de planeación, desarrollo, reporte y seguimiento de desviaciones,	X		



		además de referencia a competencia del equipo auditor y seguimiento a acciones.			
No Conformidades y Acciones Correctivas	Procedimiento para Implantar Acciones Correctivas PG-PS-GC-06	Se cuenta con un procedimiento que establece el método de gestión de las acciones correctivas de acuerdo a los requerimientos de ISO 27001	x		

OBJETIVOS, METAS Y PROGRAMAS CLAVE PARA EL SISTEMA DE GESTIÓN					
No.	DESCRIPCIÓN DEL(OS) OBJETIVO(S), META(S) O PROGRAMA(S)	RESULTADOS OBTENIDOS Y PERIODO ANALIZADO	CUMPLE		HALLAZGO
			Si	No	
1	Garantizar que la información recibida de las diversas entidades no se dañe, se modifique y esté accesible para cuando se requiera.	Describen la meta como "Minimizar el tiempo de estancia de la información desde su recepción hasta su resguardo final" y un indicador bajo la siguiente fórmula "I = Promedio del tiempo total transcurrido desde la recepción hasta su resguardo final, menor o igual a 90%".	X		
2	Permitir que la información esté disponible para el personal que la requiera de acuerdo con sus atribuciones de acceso	Describen la meta como "Establecer los diversos permisos al personal para evitar retrasos " y un indicador bajo la siguiente fórmula "I = Persona con atribuciones definidas para el acceso a la información / No. total de personal de la institución con atribuciones".	X		
3	Mantener la integridad y la secrecía de la información del personal y su no divulgación.	Describen la meta como "Minimizar el numero de personas que tienen acceso a la información del personal, a fin de garantizar su resguardo" I = No de personas autorizadas/ no. Total de personas en el área".	X		
4	Mantener la información de los diversos proveedores en resguardo y no divulgación.	Describen la meta como "Minimizar el numero de personas que tienen acceso a la información de los proveedores, a fin de garantizar su resguardo" y un indicador bajo la siguiente fórmula "I = No de personas autorizadas/ no. Total de personas en el área".	X		
5	Garantizar que la información solicitada por transparencia sea veraz y oportuna.	Describen la meta como "Minimizar el número de observaciones del organismo verificador" y un indicador bajo la siguiente fórmula "Número de observaciones del organismo/ número total de solicitudes por transparencia."	X		



EVALUACIÓN DE ASPECTOS RELEVANTES DE LOS SISTEMAS DE GESTIÓN

Aspectos relacionados al SGSI (ISO 27001)

ELEMENTO EVALUADO	EVIDENCIAS ANALIZADAS	DESCRIPCIÓN DE LA OPINIÓN DEL EQUIPO AUDITOR SOBRE LA EVIDENCIA	RES
Contexto de la Organización 4.1 Entendiendo a la organización y su contexto	Manual del Sistema de Gestión de Seguridad de la Información	Existe la definición del contexto del SGSI, ante el requisito de la norma 4.1 Entendiendo a la Organización y su Contexto, dentro del manual se hacen referencia a los siguientes, Procedimientos, procedimiento de comunicación PG-AS-AS-01 Formato RC-PS-SI-006 Matriz de administración de riesgos , sin embargo hace falta claridad sobre el contexto externo de la ASEJ.	TP1
Contexto de la Organización 4.2 Entendiendo las necesidades y expectativas de las partes interesadas	Manual del Sistema de Gestión de Seguridad de la Información Anexo 1: Diagrama de Interacción de Procesos	En el inciso 4.4 del Manual de Seguridad (MGSJ) se establece la siguiente declaración : "Las principales expectativas de nuestras partes interesadas están plasmadas en las leyes y reglamentos" Al revisar el documento "NORMATIVIDAD APLICABLE A LA OPERACIÓN, PRODUCTO/SERVICIO", este hace referencia al Sistema de Gestión de Calidad pero no al Sistema de Seguridad de la Información. Hay que asegurarse que para ambos sistemas sean los mismos requerimientos normativos y legales.	TP2
Contexto de la Organización 4.3 Alcance del SGSI	Manual del Sistema de Gestión de Seguridad de la Información	Definido: "Los procesos de revisión, examen y auditoría de cuentas públicas, asesoría técnica y capacitación a sujetos de entidades auditables, profesionalización de las y los servidores públicos internos y la transparencia en la información".	C
Liderazgo 5.1 Liderazgo y Compromiso	Manual del Sistema de Gestión de Seguridad de la Información	Se definen en base a los requisitos de la norma ISO 27001.	C



Liderazgo 5.2 Política	Manual del Sistema de Gestión de Seguridad de la Información	Se presenta como información documentada "Resguardar todo tipo de información mediante los más altos niveles de confidencialidad, integridad y disponibilidad, basados en una estrategia de administración de riesgos, direccionados siempre a la mejora continua" y se presentan los Objetivos de seguridad de la Información	C
Liderazgo 5.3 Roles, responsabilidades y autoridad	Manual del Sistema de Gestión de Seguridad de la Información	Hace referencia a Procedimiento de inducción al personal de la ASEJ, PG-TE-PF-01.	C
6.1.3. d) Evaluación del documento de aplicabilidad y versión de este documento	Documento de aplicabilidad Apéndice A CONTROLES	El SoA este no permite visualizar la justificación de la exclusiones y las inclusiones de los controles del Anexo A de ISO/IEC 27001:2013 El SOA menciona que de un total de 114 controles , se excluyó 3 controles (A.6.2.2, A.11.1.6 y A.14.2.7) El documento de aplicabilidad contiene los siguientes campos: <ul style="list-style-type: none"> • Control • Objetivo • Descripción • Método de implementación 	TP3
Planeación 6.2 Objetivos de Seguridad de la Seguridad de la Información y planeación para alcanzarlos	Manual del Sistema de Gestión de Seguridad de la Información	Los objetivos de seguridad de la información están descritos en el MGS 6.2. - OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y PLANIFICACIÓN PARA SU CONSECUCCIÓN.	C
Soporte 7.4 Comunicación	Manual del Sistema de Gestión de Seguridad de la Información Procedimiento de Comunicación PG-AS-AS-01	Se cuenta con procedimiento institucional de formalización de comunicación y sus diversos mecanismos.	C
Soporte 7.5 Información Documentada	Manual del Sistema de Gestión de Seguridad de la Información Procedimiento para Desarrollar y Clasificar Documentos PG-PS-GC-01 RC-PS-GC-015 Listado de procedimientos	En la documentación recibida y evaluada no se pudo verificar el control de la documentación externa que hace el SGSI de la Organización, de acuerdo a los requisitos de ISO/IEC 27001.	TP4



<p>Evaluación del desempeño 9.2 Auditoría Interna</p>	<p>Procedimiento de auditoría interna PG-PS-GC-04 Calendario de auditoría 2015 RC-PS-GC-004</p>	<p>En la sección de "ACTIVIDADES" declaran realizar auditorías semestrales a proveedores y en el calendario de auditoría 2015 (RC-PS-GC-004) no contiene ninguna referencia a auditorías semestrales a proveedores.</p>	<p>TP5</p>
<p>Identificación de los Principales Documentos Normativos, Requisitos Legales y Otros Aplicables</p>	<p>NORMATIVIDAD APLICABLE A LA OPERACIÓN, PRODUCTO/SERVICIO</p>	<p>Las referencias normativas establecidas e identificadas para el sistema de gestión de seguridad de la información son:</p> <ul style="list-style-type: none"> • Ley Orgánica del Poder Legislativo del Estado de Jalisco. • Ley de ingresos del Gobierno del Estado de Jalisco del ejercicio fiscal de que se trate. • Presupuesto de egresos del Gobierno del Estado de Jalisco del ejercicio fiscal del que se trate. • Ley de Hacienda del Estado de Jalisco. • Ley de Obra Publica del Estado de Jalisco. • Ley de Responsabilidades de los Servidores Públicos del Estado de Jalisco. • Ley de Fiscalización Superior y Auditoría Pública del Estado de Jalisco y sus municipios. • Reglamento Interno de la Auditoría Superior del Estado de Jalisco. • Ley de transparencia y acceso a la información pública del Estado de Jalisco y sus municipios. 	<p>C</p>
<p>Descripción de la Metodología para identificar activos y del proceso de evaluación de riesgos</p>	<p>Metodología y evaluación de riesgos</p>	<p>La metodología de riesgos se encuentra documentada en el "Procedimiento para el establecimiento de la matriz de administración de riesgos de la ASEJ" con fecha 15 de Junio del 2015, contiene el control de</p>	<p>C</p>



		<p>cambios, objetivo, alcance, referencias, definiciones, Abreviaturas, responsabilidades, actividades, documentos asociados y anexos.</p> <p>De igual forma cuentan con la "Matriz de Administración de riesgos RC-PS-SI-006", en la cual se indica el activo, el impacto a la seguridad, el análisis de riesgos y el tratamiento de los mismos.</p>	
Plan(es) de Tratamiento de Riesgos	Plan de Tratamiento del Riesgo	<p>La ASJ cuenta con un formato para la documentación de los planes de tratamiento de riesgos, el cual contiene la siguiente información: Fecha programada de inicio, Fecha real de inicio, responsable de implementación, responsable de supervisión, vulnerabilidad, activos, objetivos del plan, recursos involucrados, actividades, posibles riesgos (Riesgo y Mitigación), acciones preventivas y firmas de Elaboró, Revisó, Autorización .</p>	C

TEMA DE PREOCUPACIÓN				
No	Criterio	Sistema	Descripción del Hallazgo	Descripción del Requisito en Riesgo de incumplimiento
TP1	4.1	SGSI	Falta de claridad respecto a la identificación de los elementos externos relevantes para el Sistema de Gestión de Seguridad de la Información ya que la documentación presentada no especifica de manera clara dichos elementos.	La organización debe determinar los elementos externos e internos que son relevantes para el SGSI el propósito y que puedan afectar la capacidad para lograr el resultado deseado.
TP2	4.2	SGSI	En el inciso 4.4 del Manual de Seguridad (MGS) se establece la siguiente declaración : <i>Las principales expectativas de nuestras partes interesadas están plasmadas en las leyes y reglamentos a los cuales nosotros damos puntual respuesta</i> Al revisar el documento "NORMATIVIDAD APLICABLE A LA OPERACIÓN, PRODUCTO/SERVICIO", este hace referencia al Sistema de Gestión de Calidad pero no al Sistema de Seguridad de la Información. Hay que asegurarse que para ambos sistemas sean los mismos requerimientos normativos y legales.	La organización debe determinar : a) las partes interesadas que son relevantes para SGSI ; y b) los requisitos de estas partes interesadas relacionados a la seguridad de la información. NOTA Los requisitos de las partes interesadas pueden incluir requisitos legales y reglamentarios y obligaciones contractuales.
TP3	6.1.3 d)	SGSI	El SoA este no permite visualizar la justificación de la exclusiones y las inclusiones de los controles del	Producir una Declaración de aplicabilidad que contiene los



			Anexo A de ISO/IEC 27001:2013	controles necesarios (véase 6.1.3 b) y c)) y la justificación de inclusiones, aún si están implementadas o no, y la justificación de las exclusiones de los controles del Anexo A;
TP4	7.5	SGSI	En la documentación recibida y evaluada no se pudo verificar el control de la documentación externa que hace el SGSI de la Organización, de acuerdo a los requisitos de ISO/IEC 27001.	La Información documentada de origen externo, que la organización determine que es necesaria para la planificación y operación del SGSI, debe ser identificada como la necesaria y controlada.
TP5	9.2	SGSI	Al validar el <i>Procedimiento de auditoría interna PG-PS-GC-04</i> , en el primer párrafo de la sección <i>Actividades</i> , define que "el calendario de auditoría (RC-PS-GC-004) debe contemplar que se realicen al menos una auditoría a cada uno de los Sistemas de Gestión durante el año, además de auditorías semestrales a proveedores , así como las auditorías externas que se programen". La evidencia presentada del <i>calendario de auditoría 2015 (RC-PS-GC-004)</i> no contiene ninguna referencia a auditorías semestrales a proveedores como los establecidos en el procedimiento.	La Organización debe: c) planear, establecer, implantar y mantener un programa de auditoría, que incluya la frecuencia, métodos, responsabilidades, requisitos planeados y reporte.

■ Se realizará la evaluación de las acciones tomadas para la atención de los temas de preocupación durante la Auditoría de Certificación de Etapa 2.

NOTA 2: La falta de atención de los temas de preocupación detectados, podrán derivar en Observaciones o No Conformidades durante la realización de la Auditoría de Certificación de Etapa 2.

REVISIÓN DE LA ASIGNACIÓN DE RECURSOS NECESARIO PARA EFECTUAR LA ETAPA 2

Los recursos necesarios para la etapa 2 consisten en la asignación de un guía para acompañar al auditor líder durante la auditoría a los procesos o elementos determinados en el plan de auditoría. Además será necesario contar con un espacio disponible para la elaboración del informe de etapa 2, el acceso a un impresora y a Internet.

CONCLUSIÓN

Preparada

La organización se encuentra lista para la auditoría Etapa 2 en la fecha propuesta, ya que su nivel de implementación es aceptable o los Temas de Preocupación declarados no impiden su realización.



No preparada

La organización tendrá que resolver los Temas de preocupación identificados para realizar la auditoría de Etapa 2. Por lo que se recomienda programar esta Auditoría hasta que la organización considere que los Temas de Preocupación han sido atendidos, lo cual debería ser en un plazo no menor a 15 días y no mayor a 90 días naturales.



Clasificación del resultado

C	Conforme
TP	Tema de Preocupación

Nombre y Firma del Auditor Líder	Nombre y Firma del representante del cliente
 Lic. Alejandro Fernández Rodríguez Auditor Líder	 Dra. Claudia Verónica Gómez Varela Directora de Programación, Evaluación y Seguimiento
Firma de revisión de DAC	

Nota: si es en gabinete solo aparecen nombres y firmas del Auditor Líder y DAC