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

INFORME DE AUDITORÍA DE CERTIFICACIÓN ETAPA 2

del

Sistema de Gestión de Seguridad de 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: **18 de Noviembre del 2016**

EQUIPO AUDITOR

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

INFORME DE AUDITORÍA

CLAVE DE AUDITORÍA
MA-01

NÚMERO DE CLIENTE
ASJ-1268

NORMAS DE REFERENCIA	
☐NMX-CC-9001-IMNC-2008 (ISO 9001:2008)	☐NMX-SAA-14001-IMNC-2004 (ISO 14001:2004)
☐NMX-SAST-001-IMNC-2008 (BSI OHSAS 18001:2007)	☐NMX-F-CC-22000-NORMEX-IMNC-2007 (ISO 22000:2005)
☒ NMX-I-27001-NYCE-2009 (ISO 27001:2013)	

CUMPLIMIENTO DEL OBJETIVO DE AUDITORÍA
☒Se cumplió de acuerdo a lo establecido en el plan de Auditoría.
☐No se cumplió debido a:

CUMPLIMIENTO DEL ALCANCE DE AUDITORÍA
☒Se cumplió de acuerdo a lo establecido en el plan de Auditoría.
☐No se cumple debido a:
☐Áreas/Procesos/Sitios o Instalaciones no auditados:

CUMPLIMIENTO DE MARCA Y LOGOTIPO (No Aplica para las Auditorías Iniciales)
☒Se cumple con lo establecido en la guía de uso de marca y logotipo GDCC-01 del Organismo.
☐No lo utiliza (No aplica sanción)
☐No se cumple debido a:
Sanciones Aplicables por Incumplimiento:

American Trust Register, S. C.
Paseo de la Hacienda de Echegaray No. 40, Col. Bosque de Echegaray, Naucalpan de Juárez, Estado de México, CP 53310 Tel: (0155)5236-7383 y 84 www.americantrust.com.mx

CONFIRMACIÓN RELACIONADA CON LA INFORMACIÓN PROPORCIONADA POR EL CLIENTE (Sólo Aplica para las Auditorías Iniciales, Recertificaciones o de Cambio de Alcance)
Información Correcta: Si (X) No ( ) No Aplica
Diferencias en la información proporcionada: No Aplica
Acciones tomadas derivadas de la diferencia: No Aplica

SE CONFIRMA EL ALCANCE DE LA CERTIFICACIÓN	
☒Si	☐No (ver descripción en la parte inferior).

ALCANCE DE LA CERTIFICACIÓN ACORDADO CON EL CLIENTE (Sólo Aplica para las Auditorías Iniciales, Recertificaciones o de Cambio de Alcance)	
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 Sistema de Gestión	Planeación estratégica, Auditoría a entidades auditables, Responsabilidades, Auditor Especial de cumplimiento financiero, Administración, Dirección técnica, Unidad de Transparencia, Asuntos jurídicos, Sistema de gestión.
Listado de productos y/o servicios que se incluyen en el SG	Pliegos de Recomendaciones, Auditorias a la entidades, Capacitaciones a externos, capacitaciones a internos, documentos de transparencia

INSTALACIONES DENTRO DEL ALCANCE	
Instalación	**Proceso(s), Actividad(es), Elemento(s)**
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, Sistema 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

EXCLUSIONES DEL SGSI		CUMPLE		HALLAZGO
		Si	No	
Exclusión	**Justificación**			
A.11.1.6 Áreas de entrega y carga	La organización no cuenta con procesos en que se involucren actividades de carga y descarga. Ninguna persona tiene acceso por entradas fuera del área de ingreso.	X		
A.14.2.7 Desarrollo de sistemas subcontratado (outsourcing)	Se excluye pues dentro de los procesos y las actividades dentro del alcance no existe algún servicio contratado de desarrollo de Software, todo proceso y	X		

American Trust Register, S. C.
Paseo de la Hacienda de Echegaray No. 40, Col. Bosque de Echegaray, Naucalpan de Juárez, Estado de México, CP 53310 Tel: (0155)5236-7383 y 84 www.americantrust.com.mx

	actividad se ejecuta dentro de las instalaciones de la ASEJ como se establece en el alcance documentado del SGSI.			

REVISIÓN Y CIERRE DE LOS HALLAZGOS DETECTADOS EN LA AUDITORÍA ANTERIOR						
Tipo	Criterio	Sistema	Descripción del Hallazgo anterior	Descripción de las Acciones Tomadas por la Organización	Status	
					Cerrada	Abierta
O1	7.2 b)	SGSI	A través de entrevistas y revisión de competencias de los servidores públicos, **no se encontraron elementos suficientes** para determinar la existencia de alguien dentro del organismo, que cuente con la experiencia técnica necesaria para la implementación, gestión y monitoreo de los controles declarados en el documento de aplicabilidad.	Se ha capacitado al personal en general en temas relacionados con seguridad de la información, así como en el uso de herramientas tecnológicas y la norma ISO 27001.	X	
O2	9.1	SGSI	En el manual del Sistema de gestión de Seguridad de la Información están definidos **8 indicadores** (con frecuencia anual) y en el Documento de aplicabilidad tienen definidos indicadores (no indican frecuencia) para cada control, sin embargo durante la auditoría no se mostró evidencia de que esta medición se esté llevando a cabo.	Se pudo comprobar la existencia del programa de revisiones para la efectividad de los controles, así como la evidencia del nivel de madurez de 51 controles. De igual forma en el documento de aplicabilidad se encuentran definidos indicadores para cada uno de los controles definidos como incluyentes.	X	
O3	A.9.2.3	SGSI	Se solicitó documentación sobre el manejo de **cuentas administrativas** para Base de datos y Sistemas Operativos, sin embargo el departamento de Informática no cuenta con los mecanismos necesarios para proteger estas cuentas privilegiadas. De igual forma, se pudo comprobar que **no existe un área / responsable que se encargue de vigilar y monitorear** las actividades que realiza el departamento de Informática.	Cuentan con un procedimiento de ensobretado seguro para la contraseña de administrador de la red, la cual es cambiada con una periodicidad de 15 días. Para la cuenta de administrador de base de datos, no se sigue el mismo procedimiento debido a que la información contenida en las bases de datos no está clasificada como confidencial, aunque para el Sistema Informático Estatal de Auditoria (SIEA) si será necesario adoptar este procedimiento.	X	
O4	A.8.3.2 A.11.2.7	SGSI	Se solicitó el procedimiento de borrado seguro, el cual no fue mostrado, solo se entregó una hoja con la descripción de algunas herramientas gratuititas que se pueden usar para el borrado seguro de información.	Adquirieron 2 licencias de la herramienta KillDisk Ultimate v.10 (de paga) para el borrado seguro de información.	X	
O5	A.16.1.1 a) 4	SGSI	Se solicitaron procedimientos, matriz de roles y responsabilidades, herramientas y metodologías formales para la **atención de incidentes de seguridad de la información** que requieran	No cuentan con un procedimiento ni están capacitados para realizar un análisis sobre cómputo forense.		X

Paseo de la Hacienda de Echegaray No. 40, Col. Bosque de Echegaray, Naucalpan de Juárez, Estado de México, CP 53310 Tel: (0155)5236-7383 y 84 www.americantrust.com.mx

	A.16.1.5 b)		efectuar un **análisis de cómputo forense**, sin embargo no cuentan con esta documentación.			
O6	**A.18.1.2**	**SGSI**	Deficiencia en la administración de las licencias de Kaspersky, ya que en la consola se pudo observar un mensaje de "Clave Bloqueada" refiriéndose a las licencias del Kaspersky. El encargado del departamento de informática aseguró que esto se presentaba debido a que al momento de formatear los equipos de la ASEJ no desactivaron las claves y por esa razón mostraba este mensaje junto con otro de lista negra.	Efectuaron revisiones por parte de un tercero (Gama Sistemas) para corregir el tema de las llaves (licencias) del Kaspersky.	**X**	

HALLAZGOS DE INCUMPLIMIENTO O MEJORA DETECTADOS EN LA AUDITORÍA					
Tipo	**Criterio**	**Sistema**	**Descripción del Hallazgo**	**Descripción del requisito incumplido**	**Nivel de Criticidad del Hallazgo**
O1	**A.16.1.5 b)**	**SGSI**	Se solicitaron procedimientos, matriz de roles y responsabilidades, herramientas y metodologías formales para la **atención de incidentes de seguridad de la información** que requieran efectuar un **análisis de cómputo forense**, sin embargo no cuentan con esta documentación.	**Competencia**: Realizar análisis forense de seguridad, como se requiera.	Se considera **Observación** debido a que en el procedimiento para el tratamiento de incidentes de seguridad no consideran mecanismos para realizar actividades relacionadas con cómputo forense.
02	**A.12.6.1 k)**	**SGSI**	Se solicitaron los procedimientos de gestión de **vulnerabilidades técnicas** y el procedimiento de **gestión de parches** y evidencia para validar que se llevaron a cabo estas actividades, sin embargo no se cuenta con dichos procedimientos.	**Competencia**: un proceso de gestión de vulnerabilidades técnicas debe estar alineado con las actividades de gestión de incidentes para comunicar datos de vulnerabilidades a la función de respuesta a incidentes y proveer de procedimientos a seguir en caso de que se presente un incidente.	Se considera **Observación** debido a que no cuentan con procedimientos para la gestión de vulnerabilidades técnicas ni parches. Anteriormente esto se había establecido como oportunidad de Mejora (OM iii)

American Trust Register, S. C.
Paseo de la Hacienda de Echegaray No. 40, Col. Bosque de Echegaray, Naucalpan de Juárez, Estado de México, CP 53310 Tel: (0155)5236-7383 y 84 www.americantrust.com.mx

O3	**9.1 b)**	**SGSI**	Se revisó el documento de aplicabilidad, en la parte de indicadores y se pudo constatar que las métricas ahí definidas no coinciden con las realizadas para los controles.	**Competencia**: Los métodos para monitorear medir, analizar y evaluar son aplicables para validar resultados.	Se considera **Observación** debido a que las métricas que usan para medir no están alineadas con los indicadores definidos en el Documento de Aplicabilidad.
O4	**OM** A.12.1.4 A 14.1.1	**SGSI**	Se realizaron análisis de vulnerabilidades pero no pruebas de intrusión debido a una falta de entendimiento entre una actividad y otra.	**Competencia**: Llevar a cabo pruebas de intrusión a la infraestructura tecnológica y ataques de ingeniería social para tener una evaluación realizada por un tercero (que sea efectuada por un tercero que sea totalmente ajeno al organismo)	Se considera **Observación** debido a que se había documentado como Oportunidad de mejora (OM ix) y se tomaron medidas incorrectas.
OM	i. Documentar los procedimientos operativos relacionados con la gestión de seguridad de la información, tales como borrado seguro, gestión de seguridad en el Directorio Activo, uso de herramientas entre otros. ii. Alinear los indicadores definidos en el documento de aplicabilidad con la operación, iii. Llevar a cabo pruebas de intrusión a la infraestructura tecnológica y ataques de ingeniería social para tener una evaluación realizada por un tercero (que sea efectuada por un tercero que sea totalmente ajeno al organismo) iv. Detallar el procedimiento de formateo a bajo nivel v. Contratar los servicios de un externo para ser usado en caso de requerir servicios de cómputo forense. vi. Contratación de una persona que pueda realizar actividades de oficial de seguridad.				

APELACIONES DE LOS HALLAZGOS DE AUDITORIA POR PARTE DEL AUDITADO		
¿Existen apelaciones sobre la clasificación de hallazgos de incumplimiento?	☐Si	Se aplicará el Procedimiento de Apelaciones vigente del Organismo de Certificación
	☐No	
Descripción de la Información que soporta la apelación (puede ser proporcionada al término o fecha posterior de la Auditoría):		

ESTADO DE IMPLEMENTACIÓN, MANTENIMIENTO Y MEJORA DEL SISTEMA DE GESTIÓN	
Aspecto	**Nivel**
Estado de Implementación del Sistema de Gestión	1
Evidencia de Auditoría analizada que describe el cumplimiento de los Controles Operacionales Aplicados para el SG	1
Resultado de la Evaluación de las Competencias del Personal necesarias para lograr la conformidad del SG	1
Resultado de la Evaluación de las mejoras aplicadas al SG	1

Paseo de la Hacienda de Echegaray No. 40, Col. Bosque de Echegaray, Naucalpan de Juárez, Estado de México, CP 53310 Tel: (0155)5236-7383 y 84 www.americantrust.com.mx

DESCRIPCIÓN BREVE DE LA AUDITORÍA REALIZADA
Lugares visitados durante la presente auditoría
Únicas instalaciones: Av. Niños Héroes no. 2409 Col. Moderna Guadalajara, Jalisco.
Identificación de los principales documentos Normativos, Requisitos Legales y Otros Aplicables
• 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 Pública del Estado de Jalisco. • Ley de Responsabilidades de los Servidores Públicos del Estado de Jalisco. • Ley de Fiscalización Superior y Auditoria Publica del Estado de Jalisco y sus municipios. • Reglamento Interno de la Auditoria Superior del Estado de Jalisco. • Ley de transparencia y acceso a la información pública del Estado de Jalisco y sus municipios
Información Resumida de la Muestra Tomada
Documento de aplicabilidad Revisión de **7 controles** contenidos en el documento de aplicabilidad (Eliminación de medios, Gestión de derechos de acceso privilegiado, Eliminación segura o re-uso de activos de información, Responsabilidades y procedimientos en Gestión de incidentes, Responsabilidades en los eventos de seguridad Derechos de propiedad industrial) contra lo que tienen establecido en las políticas y procedimientos del sistema de gestión de seguridad de la información. ***Auditorías a entidades auditables, capacitación de servidores públicos, profesionalización de servidores públicos, procesos de transparencia, procesos administrativos, sistemas de gestión, informáticas.*** Entrevistas con los responsables del sistema de gestión de seguridad de la información, así como con las personas del área de tecnologías de información.

Aspecto a Evaluar	Evidencias Presentadas	Resultado de la Evaluación	Cumple		Hallazgo
			Si	No	
Revisión por la Dirección	Minutas de las sesiones llevadas a cabo con la dirección donde trataron puntos diversos relacionados con los resultados de la auditoria externa de mantenimiento del SGSI.	El informe de revisión por la dirección contiene los hallazgos de auditoria interna, resumen de las no conformidades y acciones correctivas. Generaron 3 planes de tratamiento de riesgos para la mitigación de los riesgos detectados.	X		
Metodología de Evaluación de Riesgos, Criterios de aceptación de riesgos	Manual de Metodología de Evaluación y Tratamiento de Riesgos.	La metodología de evaluación de riesgos, no sufrió cambios significativos	**X**		

American Trust Register, S. C.
Paseo de la Hacienda de Echegaray No. 40, Col. Bosque de Echegaray, Naucalpan de Juárez, Estado de México, CP 53310 Tel: (0155)5236-7383 y 84 www.americantrust.com.mx

e identificación de niveles aceptables de riesgo					

OBJETIVOS, METAS Y PROGRAMAS CLAVE PARA EL SISTEMA DE GESTION					
No.	**Descripción del(os) Objetivo(s), Meta(s) O Programa(s)**	**Resultado de la Evaluación**	**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 número de personas que tienen acceso a la información del personal, a fin de garantizar su resguardo = 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 número 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		

Elementos Relevantes derivados de la presente Auditoría a considerar durante la siguiente auditoría:	REQUISITOS DEL SISTEMA DE GESTIÓN:				
	C	**A**	**ST**	**IA**	**SI**
1. Cierre a las Observaciones emitidas en este informe.	--	--	--	--	X
2. Considerar la revisión de las oportunidades de mejora (OM) descritas en este informe.	--	--	--	--	X

CONFIDENCIALIDAD EN EL MANEJO DE LA INFORMACIÓN A LA QUE SE TUVO ACCESO
Se ha realizado la auditoría con base en un muestreo y en consecuencia, pueden existir otras desviaciones que no fueron identificadas en este ejercicio. Cabe recordar que toda la información a la que tuvo acceso el equipo auditor se maneja con carácter confidencial.
AGRADECIMIENTO

American Trust Register, S. C.
Paseo de la Hacienda de Echegaray No. 40, Col. Bosque de Echegaray, Naucalpan de Juárez, Estado de México, CP 53310 Tel: (0155)5236-7383 y 84 www.americantrust.com.mx

En nombre de American Trust Register S.C. agradecemos a la Organización y al personal auditado las facilidades otorgadas, información proporcionada y atenciones recibidas durante la presente Auditoría.

ACCIONES DE SEGUIMIENTO CUANDO EXISTEN OBSERVACIONES Y/O NO CONFORMIDADES

OBSERVACIONES: Se verificará la implementación de las acciones tomadas para la atención de los hallazgos por la Organización, en la siguiente auditoría.

NOTA: En caso de no evidenciar la eficacia de las acciones tomadas de la(s) Observación(es) en la próxima auditoría, ésta(s) será(n) declarada(s) como No Conformidad(es).

NO CONFORMIDADES: La Organización **deberá enviar al Organismo Certificador**, las evidencias documentadas de las correcciones específicas y acciones correctivas planificadas o realizadas para eliminar la(s) causa(s) de la(s) No Conformidad(es) en un plazo **no mayor a 90 días naturales** a partir de la fecha de este informe.

NOTA: En caso de no enviar al Organismo Certificador la información requerida en el período establecido:

Será necesario re-iniciar el proceso de su Certificación. (Aplica en Certificación o Recertificación)

Se iniciará el proceso de suspensión de su Certificación. (Aplica en Mantenimiento o/y Cambio de Alcance)

LUGAR DE CIERRE DE NO CONFORMIDADES

☐ Las No Conformidades encontradas requieren que el Cierre de las mismas se realice en las Instalaciones de la organización, por lo que la Dirección Comercial de American Trust Register S.C. se pondrá en contacto con el cliente para cotizar dicha Auditoría.

☐ La organización debe enviar a American Trust Register S.C. las evidencias documentadas del análisis, plan de acción, implementación y cierre de las No Conformidades detectadas durante esta auditoría con el objetivo de determinar si son aceptables. En caso que las evidencias enviadas dentro del plazo establecido, no aseguren eliminar la(s) causa(s) de la(s) No Conformidad(es), será necesario programar una auditoría In Situ, lo cual será comunicado a la Organización.

La eficacia de las acciones tomadas será confirmada en la próxima auditoría programada.

CONCLUSIÓN

☒ **Aceptable**	☐ **No Aceptable**
Se concluye que el Sistema de Gestión de la Organización cumple con lo establecido en la Norma(s) de Referencia, por lo que el(los) auditor(es) líder(es) recomienda(n):	La organización requiere enviar la documentación que evidencie la eliminación de la(s) causa(s) de la(s) No Conformidad(es) en el plazo establecido para su revisión y determinar si son aceptables.
☒Otorgar ☐Mantener ☐Modificar	
La Certificación del (los) Sistema(s) de Gestión.	

Clasificación del resultado

C	Cumple
O	Observación
NC	No Conformidad
OM	Oportunidad de Mejora

American Trust Register, S. C.
Paseo de la Hacienda de Echegaray No. 40, Col. Bosque de Echegaray, Naucalpan de Juárez, Estado de México, CP 53310 Tel: (0155)5236-7383 y 84 www.americantrust.com.mx

NA	No Aplica

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

American Trust Register, S. C.
Paseo de la Hacienda de Echegaray No. 40, Col. Bosque de Echegaray, Naucalpan de Juárez, Estado de México, CP 53310 Tel: (0155)5236-7383 y 84 www.americantrust.com.mx