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

INFORME DE AUDITORÍA
MANTENIMIENTO 02

Del

Sistema de Gestión de Seguridad de la Información
Norma ISO 27001:2013 / NMX-I-27001-NYCE-2015

De

Auditoría Superior del Estado de Jalisco

Fecha de emisión: 12.07.17 FDAC-05.1 Rev. 11

CLAVE DE AUDITORÍA	CLAVE DE CLIENTE
MA-02	ASJ-1268

DATOS GENERALES DE LA ORGANIZACIÓN	
Domicilio de la organización:	Av. Niños Héroes No. 2409, Col. Moderna, Guadalajara, Jalisco CP. 44190
Nombre del contacto:	Claudia V. Gómez Varela
Correo electrónico del contacto:	cgomez@asej.gob.mx
Teléfono de la organización:	(33) 36794500
Fecha de auditoría:	27 Y 28 DE Noviembre del 2017

GRUPO AUDITOR	
Auditor Líder:	Carlos Guzmán Sigala
Equipo Auditor:	N/A
Experto Técnico	N/A

COONFIRMARCIÓN DE LA INFORMACIÓN PROPORCIONADA POR LA ORGANIZACIÓN		
Solicitud de Certificación (FDCO-02) y Viabilidad Técnica (FDCO-01)	(X) Información correcta	( ) Existen diferencias
Diferencias en la información proporcionada:		
Acciones tomadas derivadas de la diferencia:		

CUMPLIMIENTO DE CRITERIOS, OBJETIVOS Y ALCANCE ESTABLECIDOS EN EL PLAN DE AUDITORÍA	
(X) Sí se cumplió de acuerdo al plan de auditoría	( ) No se cumplió de acuerdo al plan de auditoría
Descripción del incumplimiento:	
Motivo del incumplimiento:	

CUMPLIMIENTO CON LO ESTABLECIDO EN EL REGLAMENTO DE USO DE MARCA / LOGOTIPO (RDCC-02)		
(X) No lo utiliza (no aplica sanción)	( ) Sí cumple	( ) No cumple
Descripción del incumplimiento:		
Acciones tomadas o que realizará la organización:		

DOMICILIO FISCAL	Av. Niños Héroes No. 2409, Col. Moderna, Guadalajara, Jalisco CP. 44190

ALCANCE DE LA CERTIFICACIÓN ISO 27001:2013
Aplica a, Auditorías a entidades auditables, capacitación de servidores públicos, profesionalización de servidores públicos, procesos de transparencia, procesos administrativos, sistemas de gestión, informáticas.

CUESTIONES PERTINENTES PARA EL PROPÓSITO Y DIRECCIÓN ESTRATÉGICA DE LA ORGANIZACIÓN QUE HAN SIDO CONSIDERADOS EN EL SGSI	
CUESTIONES EXTERNAS	**CUESTIONES INTERNAS**
• Entorno político - inestabilidad cada 6 años por cambios en la estructura organizacional	• Gestión adecuada del clima laboral
• Entorno tecnológico - cambio constante de impacto en las operaciones	• Personal competente
• Mantenimiento de las certificaciones de los sistemas de gestión	• Auditorías internas a los sistemas de gestión
• Organismo de fiscalización federal - cumplimiento con el marco legal aplicable	• Cumplimiento con metas y objetivos
• Proveedores cumplimiento de contratos licitados	• Formación constante
• Requerimientos de transparencia de la ciudadanía	•
REQUISITOS DE LAS PARTES INTERESADAS PERTINENTES PARA EL SGSI	
PARTES INTERESADAS	**REQUISITOS PERTINENTES**
• Entidades gubernamentales	• Rendición de cuentas transparencia
• Congreso del estado de Jalisco	• Informe oportuno sobre los resultados de las auditorias ejecutadas
• Organismos de certificación	• Mantenimiento sostenido y mejora de su sistema de gestión
• Sindicatos	• Trato digno a los trabajadores / control del clima laboral
• Sociedad	• Transparencia y rendición de cuentas
• Proveedores	• Cumplimiento oportuno de pagos y contratos
• Entidades auditables	• Capacitación oportuna y orientación sobre los temas legales aplicables
• Servidores/as públicos de la ASEJ -	• Mantener la integridad y secrecía de la información del personal y su no divulgación.
INTERFACES Y DEPENDENCIAS REALIZADAS POR:	
ORGANIZACIÓN (INTERNAS)	**POR OTRAS ORGANIZACIONES (EXTERNAS)**
• Relación interna entre áreas	• Entidades de fiscalización
• Estructura organizacional definida	• Municipios entes auditables
• Establecimiento de roles y responsabilidades	• Sindicatos
• Evaluaciones al personal	• Proveedurías

"APLICABILIDAD –EXCLUSIÓN DE CONTROLES DEL APÉNDICE A "OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA"	
OBJETIVOS DE CONTROL Y CONTROLES EXCLUIDOS	**JUSTIFICACIÓN**
A.11.1.6 AREAS PUBLICAS DE CARGA Y DESCARGA	**La institución no realiza actividades de carga y descarga, ya que no contamos ni con andenes ni con áreas para estos menesteres.**
A.14.2.7. DESARROLLO DE SISTEMAS SUBCONTRATADO	**Dentro de los procesos y actividades del alcance, no se cuenta con servicios de contratación de desarrollo de software, las modificaciones a los procesos se realizan de forma interna.**

LUGARES VISITADOS EN LA AUDITORÍA
Av. Niños Héroes No. 2409, Col. Moderna, Guadalajara, Jalisco CP. 44190

DESCRIPCIÓN DE LA AUDITORÍA REALIZADA		
Evidencia de la Conformidad con los requisitos de las Normas de SGSI y sus controles operacionales, Así como otros Documentos Normativos, Reglamentarios, Legales y Contractuales.		
Descripción del Requisito de Referencia	**Descripción de la muestra y evidencia Presentadas (Proceso, Fecha, Sitio, etc.)**	**Hallazgo**

4. CONTEXTO DE LA ORGANIZACIÓN **4.1 Comprendiendo a la organización y su contexto:** La organización debe determinar asuntos externos e internos que son relevantes para su propósito y que afectan a su capacidad para lograr el(los) resultado(s) esperado(s) de su SGSI. NOTA: La determinación de estas cuestiones se refiere a establecer el contexto externo e interno de la organización, considerado en la cláusula 5.3 de la norma ISO 31000: 2009 [5] **4.2 Comprendiendo las necesidades y expectativas de las partes interesadas:** La organización debe determinar: a) las partes interesadas que son relevantes para el SGSI, y b) los requisitos de estos interesados pertinentes para la seguridad de la información. NOTA: Los requisitos de las partes interesadas pueden incluir los requisitos legales y reglamentarios y las obligaciones contractuales.	La organización cuenta con soporte documental dentro del manual de los sistemas de gestión donde se establece la metodología utilizada para determinar las situaciones relevantes que puedan impactar en la capacidad de lograr los resultados esperados del SGSI. Se considera el análisis del impacto de dichas situaciones en el resultado esperado del SGSI, considerando ligarlas a los métodos de gestión de riesgos operativos por proceso así como aquel establecido para la gestión de la seguridad de la información. Se identifican las partes interesadas, entre las cuales se han identificado: Organismos de certificación, entidades auditables, organismos de fiscalización federales y estatales, proveedores, sociedad, sindicatos, congreso y comisión de vigilancia así como organismos de certificación. Véase sección de encabezado del presente documento. Se identifica el impacto de estas en el SGSI, identificando objetivos, metas, indicadores, frecuencia de medición , Durante la implementación del SGI (los sistemas de gestión) se identifica los requerimientos de las partes interesadas, incluyendo legales y regulatorios, de cada parte interesada en los casos aplicables	C
4.3 Determinando el alcance del SGSI: La organización debe determinar los límites y aplicabilidad del SGSI para establecer el alcance. Al determinar el alcance, la organización debe considerar: a) los problemas externos e internos mencionados en el 4.1; b) los requisitos indicados en el 4.2, y c) las interfaces y las dependencias entre las actividades realizadas por la organización, y los que se llevan a cabo por otras organizaciones. El alcance deberá estar disponible como información documentada. **4.4 Sistema de Gestión de Seguridad de la Información (SGSI)** La organización debe establecer, implementar, mantener y mejorar continuamente un SGSI, de conformidad con los requisitos de este estándar International.	Se ha determinado el alcance del SGSI. Dentro del alcance, se contemplan las situaciones internas y externas que impactan en los resultados esperados del SGSI. Alcance de certificación definido: Aplica a, Auditorias a entidades auditables, capacitación de servidores públicos, profesionalización de servidores públicos, procesos de transparencia, procesos administrativos, sistemas de gestión, informáticas. Alcance y determinación del SGSI Considera el proceso operativo de impacto al cliente COP's, soporte administrativo al SGSI MOP's y procesos soporte de las operaciones SOP's. Se considera procesos de auditorías internas, control documental, acciones correctivas, revisión por la dirección, seguimiento y medición, procesos operativos, gestión de riesgos, acuerdo de aplicabilidad.	C

5. LIDERAZGO **5.1 Liderazgo y Compromiso** La alta dirección debe demostrar su liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información a través de: a) garantizar la política de seguridad de la información y de los objetivos de seguridad de información se establecen y son compatibles con la orientación estratégica de la organización. b) garantizar la integración de los requisitos del SGSI en los procesos de la organización; c) velar por que los recursos necesarios para el SGSI están disponibles; d) comunicar la importancia de una gestión eficaz de seguridad de la información, y de adaptarse a los requisitos del SGSI; e) garantizar que el SGSI alcanza sus objetivos previstos: f) dirección y apoyo de personas para contribuir a la eficacia del SGSI. g) promover la mejora continua y h) el apoyo a otras funciones de gestión para demostrar su liderazgo ya que se aplica a sus áreas de responsabilidad. **5.2 Política** La alta dirección debe establecer una política de seguridad de la información que: a) es apropiada para el propósito de la organización; b) incluye los objetivos de seguridad de la información (ver 6.2) o proporciona el marco para establecer los objetivos de seguridad de la información; c) incluye un compromiso de cumplir con los requisitos aplicables relacionados con la seguridad de la información, y d) incluye un compromiso de mejora continua del SGSI. La política de seguridad de la información deberá: e) estará disponible como información documentada; f) ser comunicada dentro de la organización, y g) estar a disposición de las partes interesadas, según corresponda.	Se muestra compromiso de la dirección a través de: Se cuenta con una política y objetivos documentados: POLITICA: Se cuenta con política integral dentro del manual integrado de los sistemas de gestión, se muestra sección ligada a la seguridad de la información. "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". OBJETIVOS: Se cuenta con 8 objetivos declarados ante el SGSI, véase sección 6.2 objetivos. Se gestiona los recursos necesarios disponibles para la operación del SGSI?	C
5.3 Roles, Responsabilidades y Autoridades de la Organización. La alta dirección debe asegurarse de que las responsabilidades y autoridades para las funciones relacionadas con la seguridad de la información son asignadas y comunicadas. La alta dirección debe asignar la responsabilidad y autoridad para: a) garantizar que el SGSI se ajusta a los requisitos de esta norma internacional y b) informar sobre el desempeño del SGSI a la alta dirección. NOTA: La alta dirección también puede asignar las responsabilidades y autoridades para informar sobre el desempeño del sistema de gestión de seguridad de la información dentro de la organización.	Se han designado los roles y responsabilidades dentro del SGSI. La o el Auditor Superior se asegura que las responsabilidades y autoridades estén bien definidas, comunicadas e interrelacionadas dentro de la organización. Para ello ha descrito sus responsabilidades y atribuciones en cada uno de los puestos y sus procedimientos La Alta dirección ha designado a la o el representante de la dirección para el Sistema de Gestión de Seguridad de la información (RSI) y es la o el titular de la Dirección de Programación, Evaluación y Seguimiento, a quien se le han asignado las siguientes responsabilidades y autoridades.	C

6 PLANEACIÓN **6.1 Acciones para abordar el riesgo y oportunidades ligadas a la seguridad de la información.** **6.1.1 Consideraciones Generales.** Al planificar el SGSI, la organización debe considerar los temas mencionados en el 4.1 y los requisitos mencionados en el 4.2 para determinar los riesgos y oportunidades que deben dirigirse a: a) asegurar que SGSI se puede lograr el resultado(s) previsto (s) b) prevenir o reducir los efectos no deseados, y c) lograr una mejora continua La organización debe planificar: d) las acciones para hacer frente a estos riesgos y oportunidades, y e) cómo. (Como lograrlos y llevar a cabo las actividades inherentes) 1) integrar y poner en práctica las acciones en sus procesos del SGSI, y 2) Evaluar la efectividad de estas acciones. **6.1.2 Evaluación del riesgo ligado a la seguridad de la información.** La organización debe definir y aplicar un proceso de evaluación de riesgos de seguridad de la información que: a) establezca y mantenga los criterios de riesgo de la información de seguridad que incluyen: 1) los criterios de aceptación de riesgo, y 2) los criterios para la realización de las evaluaciones de riesgos de seguridad de la información; b) asegurar que las evaluaciones de riesgos de seguridad de la información sean repetidas y que produzcan resultados consistentes, válidos y comparables; c) identificación de los riesgos de seguridad de la información: 1) aplicar el proceso de evaluación de riesgos de seguridad de información para identificar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información en el ámbito de aplicación del SGSI, y 2) identificar a los propietarios de los riesgos; d) análisis de los riesgos de seguridad de la información: 1) comparar y evaluar las posibles consecuencias que resultarían si los riesgos identificados en 6.1.2 c) cuando (donde) estos se materialicen 2) evaluar la probabilidad realista de la ocurrencia de los riesgos identificados en 6.1.2 c) y 3) determinar los niveles de riesgo; e) evalúa los riesgos de seguridad de la información: 1) comparar los resultados del análisis de riesgos a los criterios de riesgo establecidos en el punto 6.1.2 a), y 2) clasificación de los riesgos analizados para el tratamiento de riesgos. La organización deberá conservará información documentada sobre el proceso de evaluación de riesgos de seguridad de información.	En la ASEJ la planeación del SGSI, ha considerado las necesidades y requisitos de todas las partes interesadas a fin de traducirlas en requisitos a cumplir dentro de dicho sistema y determinar los riesgos y oportunidades que representan para la institución Se identifica los riesgos y oportunidades esto mediante la metodología y matriz de administración de riesgos. Dicha metodología y matriz de gestión de riesgos consideran el control de la planeación operativa ligada a la seguridad de la información, así el cómo lograr el cumplimiento de los mismo y obtener la mejora continua., dentro del SoA, acuerdo de aplicabilidad considera reportes para la validación de la efectividad de los controles así como los indicadores establecidos. La organización cuenta con soporte documental para la gestión de riesgos ligados a la seguridad de la información., Procedimiento para el establecimiento de la matriz de administración de riesgos de la ASEJ. PG-PS-SI-01 Rev. 4 del 16-11-2017 Inventario de activos RC-PS-SI-001 Matriz de administración de riesgos RC-PS-SI-006 Se considera el marco legal aplicable LGPDP, ley general de protección de datos personales, y LTAIPJ ley de transparencia y acceso a la información pública del estado de Jalisco Dicha metodología cuenta con: Criterio de aceptación de riesgo Estableciendo (alto, medio , bajo) Criterios para la evaluación de los riesgos: Establecidos sobre potencialidad y probabilidad de que una amenaza explote las vulnerabilidades así mismo se asegura que la evaluación produce resultados consistentes y que puedan comprarse. Se identifica a los responsables de los riesgos, dentro de la matriz de riesgos establecida. El proceso de evaluación del riesgo se asocia a la perdida de confidencialidad, integridad y disponibilidad de la información determinada dentro del alcance de los sistemas de gestión implementados.	C C

	Así mismo cabe mencionar que la organización mediante esta metodología implementada analiza las consecuencias potenciales de que los riesgos ocurran identificando impacto en degradación sobre al confidencialidad, integridad y disponibilidad. Se incluye un análisis realista de la probabilidad de ocurrencia del riesgo Se muestra información documentada del proceso de tratamiento de riesgos en seguimiento, Matriz de administración de riesgos RC-PS-SI-006 Rev. 2 del 2 de agosto del 2017. Acuerdo de aplicabilidad Rev.RC-PS-SI-007 Rev. 3 del 2 de agosto del 2017.	

6.1.3 Tratamiento del riesgo ligado a la seguridad de la información. La organización debe definir y aplicar un proceso de tratamiento de riesgos de seguridad de la información a: a) seleccionar las opciones de tratamiento de riesgos de seguridad de información adecuados y teniendo en cuenta los resultados de la evaluación de riesgos; b) determinar todos los controles que sean necesarios para poner en práctica la seguridad de la información, así como el tratamiento del riesgo elegido(s). NOTA: la organización puede diseñar controles según sea necesario, considerando aquellos detectados en cualquier búsqueda. c) Comparar los controles determinados en 6.1.3 b) con los del Anexo A y compruebe que no hay controles necesarios que hayan sido omitidos. NOTA 1 Anexo A, Contiene una lista comprensible de objetivos de control y controles, esta Norma se dirigen al Anexo A para asegurarse de que no hay controles necesarios se pasan por alto. NOTA 2 Los objetivos de control se incluyen implícitamente en los controles seleccionados. Se pueden necesitar los objetivos de control y controles que figuran en los objetivos de control, así Como aquellos que no necesariamente pueden estar listados en el anexo A de la norma. d) producir una Declaración de aplicabilidad (SoA) que contiene los controles necesarios (véase 6.1.3 b) y c) e inclusiones y justificaciones, si se aplican o no. y la justificación de la exclusión de los controles del Anexo A; e) formular un plan de tratamiento de riesgos de seguridad de información, y f) Obtener la aprobación del plan de tratamiento de riesgos de seguridad de la información y la aceptación de los riesgos de seguridad de la información residuales del o los propietarios de los riesgos. La organización debe conservar información documentada sobre el proceso de tratamiento de riesgos de seguridad de información. NOTA: El proceso de evaluación y tratamiento de riesgos de seguridad de información en esta norma internacional se alinea con los principios que se proveen dentro de la norma internacional ISO 31000[5]-.	Se cuenta con Acuerdo de aplicabilidad Rev.RC-PS-SI-007 Rev. 3 del 2 de agosto del 2017. (SOA) incluye los controles del anexo A, como resultado del análisis de riesgos así como la adopción de buenas prácticas, requerimiento legal, de cliente Se cuenta con la justificación para la inclusión y exclusión de los controles del anexo A A.11.1.6 áreas públicas de carga y descarga A.14.2.7 desarrollo de software subcontratado Se cuenta documentados planes de tratamiento de riesgo., Actualmente al organización cuenta con 3 PTR abiertos y en proceso., Folio PTR-01 del 3 de nov. Del 2015, Robo de información, infestación de archivos, copias no controladas y autorizadas. Abierto. Folio PTR-02 del 3 de noviembre del 2015 Falta de conciencia, políticas de seguridad, capacitación, manejo inadecuado de la encriptación, degradación en la seguridad de la información. Abierto. Folio PTR-03 del 22 de septiembre del 2015 Falta de conciencia respecto a la seguridad de la inf. Falta de mecanismos de vigilancia., Cerrado: Noviembre del 2016 Dentro de la matriz de riesgos presentada así como dentro de los planea de tratamiento se cuenta con la aprobación de los responsables de los riesgos residuales, roles, responsabilidades y recursos necesario así como la gestión de los planes de acción.	C

6.2. Los objetivos de seguridad de la información y la planificación para alcanzarlos. La organización debe establecer los objetivos de seguridad de la información en las funciones y niveles pertinentes. Los objetivos de seguridad de la información deberán: a) ser coherente con la política de seguridad de la información; b) ser medibles (si es posible); c) tener en cuenta los requisitos de seguridad de la información aplicable, así como los resultados de la evaluación y tratamiento de riesgos; d) ser comunicada; y e) ser actualizada según corresponda. La organización deberá conservará información documentada sobre los objetivos de seguridad de la información. Al planificar cómo alcanzar sus objetivos de seguridad de la información, la organización debe determinar: f) lo qué se hará; g) los recursos que serán necesarios; h) que será responsable; (quien será responsable) i) cuando se completará, y j) cómo se evaluarán los resultados.	La organización cuenta con soporte documental, para la gestión de los objetivos del SGSI., MEDICION DE OBJETIVOS DE PARTES INTERSADAS DE Servidores/as públicos de la ASEJ, Mantener la integridad y secrecía de la información del personal y su no divulgación. Minimizar el número de accesos a la información del personal. I = No. de accesos a la información del personal / No. total de accesos a la información. I = Accesos Total I =25/25 = 1 Proveedores Mantener la información de los diversos proveedores en resguardo y no divulgación. Minimizar el acceso a la información para su divulgación. I = No. de Accesos a la información del proveedor / No. total de accesos a la información. I = Accesos Total I = 0/25 = 0 Sindicatos Mantener la información de las diversas personas en resguardo y no divulgación. Minimizar el acceso a la información para su divulgación. I = No. de accesos a la información del personal / No. total de accesos a la información. I = Accesos Total I = 0/0 = 0 Congreso del Estado/ Organismos de certificación Organismos de fiscalización superior estatales y federales, Se muestra evidencia de la gestión y cumplimiento de los años 2016 y 2017.	C

7. APOYO **7.1 Provisión de los Recursos** La organización debe determinar y proveer de los recursos necesarios para la implementación mantenimiento y mejora continua del sistema de gestión de seguridad de la información.	Se muestra gestión adecuada de: Capacitación, equipo, recursos humanos, infraestructura, ambiente para las operaciones. Se muestra plan operativo anual para la gestión de las operaciones, los sistemas de gestión, y la seguridad de la información. Plan Operativo Anual (POA) Se muestra evidencia y registros de la gestión de los recursos. véase 5.1 del presente documento.	C
7.2 Competencias La organización debe: a) determinar la competencia necesaria de la persona (s) que hace el trabajo bajo su control que afecte a su rendimiento de seguridad de la información; b) asegurar que estas personas son competentes en base a la educación, la formación o la experiencia; c) en su caso, tomar las acciones para adquirir la competencia necesaria, y evaluar la eficacia de las acciones tomadas, y d) retener la información documentada apropiada como evidencia de la competencia. **NOTA:** Acciones aplicables pueden incluir, por ejemplo: la oferta de formación para la tutoría, o la reasignación de los empleados actuales, o la contratación de personas competentes.	Se cuenta con soporte documental para la gestión del reclutamiento, selección y contratación del personal PE-AD.RH-08 Rev. 8 del 16-11-2017. Procedimiento de inducción al personal en coordinación con profesionalizaciones PG-TE-PF-01 Se da seguimiento a la NC-m detectada en ejercicio de auditoria del 2016, Se muestra plan de acciones y seguimiento a esta NC-m. Se trabajó en la re-estructuración de todos y cada uno de los descriptivos de puesto, en especial atención a las descripciones de los auditores de (municipios, OPD, Obra Pública) con los que se encontró observación en el ejercicio anterior de auditoria. Personal Muestreados: LCP. Arturo Álvarez Avalos / Auditor Ing. Jorge Barragán Jalomo / Jefe de Zona	C
7.3 Conciencia. Las personas que hacen el trabajo bajo el control de la organización deben tener en cuenta: a) la política de seguridad de la información; b) su contribución a la eficacia del sistema de gestión de seguridad de la información, incluyendo los beneficios de un mejor desempeño de la seguridad de la información; y c) las implicaciones o (consecuencias) de no ajustarse (sujetarse) a los requisitos del SGSI.	El personal involucrado dentro del alcance del SGSI es consiente del impacto de su contribución en la política, mejora y consecuencias de incumplimientos en el SGSI. Se muestra concimiento del personal y compromiso asi como conocimiento de su participación para el logro de los objetivos y metas institucionales. Se muestra conocimiento de su aportación y participación para con la seguridad de la información.	C
7.4 Comunicación. La organización debe determinar la necesidad de las comunicaciones internas y externas pertinentes para SGSI que incluye: a) en lo que para comunicarse; (sobre que comunicar) b) cuando comunicarse c) con quien comunicarse d) que debe ser comunicado y e) el proceso por el cual debe de efectuar la comunicación.	La Alta Dirección establece los sistemas adecuados y funcionales que garantizan una adecuada comunicación dentro y fuera de nuestra institución, donde se identifiquen los contenidos, la o el comunicador, las y los receptores y la frecuencia. Todo esto ha quedado plasmado en el procedimiento de comunicación PG-AS-AS-01, el cual ha sido difundido y se encuentra en la red interna como elemento de comunicación.	C

7.5 Información documentada **7.5.1 Generalidades** El SGSI deberá incluir. a) la información requerida por esta norma internacional documentado, y b) información documentada, determinada por la organización como necesarios para la efectividad del SGSI. 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: 1) el tamaño de la organización y de su tipo de actividades, procesos, productos y servicios; 2) la complejidad de los procesos y sus interacciones, y 3) competencia de las personas.	La organización establecido y mantenido al día los procedimientos para controlar la información documentada y datos relacionados con el SGSI y otros sistemas, a fin de cumplir con las normas y la eficacia de los diversos sistemas de la ASEJ. Las políticas, procedimientos y todo tipo de documento elaborado para la operación del sistema deben cumplirse por el personal de acuerdo a lo establecido en el manual de los sistemas de gestión. Se considera la documentación obligada tales como: Metodología para la gestión del riesgo Acuerdo de aplicabilidad Matriz para la gestión del riesgo Planes de tratamiento Véase codificación documental en cada uno de los documentos declarados durante el proceso de auditoría.	C
7.5.2 Creación y actualización Al crear y actualizar la información documentada de la organización debe asegurarse apropiadamente: a) la identificación y la descripción (por ejemplo, un título, fecha, autor, o el número de referencia); b) formato (por ejemplo, el idioma, la versión del software, gráficos) y de los medios de comunicación (por ejemplo, papel, electrónico), y c) la revisión y aprobación por la idoneidad y adecuación.	Para la aprobación, emisión y cancelación de documentos, se deberá seguir lo marcado en el procedimiento para desarrollar y clasificar documentos PG-PS-GC-01; y para el control y distribución de los mismos, se deberá seguir el procedimiento para el control de documentos PG-PS-GC-02.	C
7.5.3 Control de la información documentada Información documentada requerida por SGSI y por esta norma internacional se deben controlar para asegurar: a) que está disponible y adecuado para su uso, donde y cuando sea necesario, y b) que esté protegido de forma adecuada (por ejemplo, de pérdida de confidencialidad, uso inadecuado, o la pérdida de la integridad). Para el control de la información documentada, la organización debe responder a las siguientes actividades, según corresponda: c) la distribución, acceso, recuperación y uso; d) almacenamiento y conservación, incluyendo la preservación de la legibilidad; e) el control de cambios (por ejemplo, control de versiones), y f) retención y disposición. Información documentada de origen externo, que la organización determina que son necesarios para la planificación y operación del SGSI, deben ser identificados según el caso, y ser controlados. NOTA: El acceso implica una decisión sobre el permiso para ver la información documentada solamente, o el permiso y la autoridad para ver y cambiar la información documentada, etc.	El control también asegura: a) Que los documentos estén disponibles y actualizados en los lugares donde se está cumpliendo con el SGSI, ya sea de forma electrónica o documental. b) Que todos los documentos son legibles y fácilmente identificables. c) Están protegidos adecuadamente contra accesos que dañen su pérdida de integridad, o confidencialidad, o se les dé un uso inadecuado por personas no autorizadas. d) Que los documentos que han quedado obsoletos se retiran inmediatamente del proceso y son destruidos los originales y las copias, guardando evidencia en el historial de cambios de cada documento. e) Sólo se conservan los originales en archivo.	C

	f) Que las modificaciones en los documentos serán revisadas y aprobadas por las personas que promueven el cambio, y deben ser autorizados por la o el responsable del área que lo emite, según el procedimiento PG-PS-GC-01. g) Que nuestra documentación está siempre actualizada, para lo cual se establece como obligado la revisión bi-anual de todos los documentos del sistema. h) Que se identifican y controlan los documentos de origen externo. El sistema documental de la ASEJ es híbrido, con esto queremos decir que el sistema opera tanto de forma electrónica como de forma documental. En los lugares donde el personal tiene acceso a la intranet, el acceso a la documentación es por vía electrónica; y cuando el personal no cuenta con acceso a la red, el área responsable del control de documentos extiende una copia controlada para su utilización, manteniendo registro de lo anterior, previa solicitud de la misma. Los registros son para nosotros una evidencia de la conformidad con los requisitos de los sistemas por lo que: a) Los registros deben ser mantenidos durante el tiempo requerido para cada caso, quedando determinado su tiempo de retención en el procedimiento de control de registros PG-PS-GC-03. b) Todos los registros deben ser legibles y fácilmente localizables, almacenados en lugares que los protejan del deterioro y el extravío. c) Se han estableciendo controles para la recuperación y disposición de los registros. d) Los registros pueden estar en medio escrito y en algunos casos en medio electrónico NOTA: se cuenta con 95 políticas de seguridad de la información declaradas ante el SGSI.	

8. FUNCIONAMIENTO **8.1 Planificación y control operacional.** La organización debe planificar, ejecutar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información, y para poner en práctica las acciones determinadas en el punto 6.1. La organización debe aplicar también planes para lograr los objetivos de seguridad de información determinadas en 6.2 La organización debe mantener la información documentada en la medida necesaria para tener confianza en que los procesos se han llevado a cabo según lo previsto. La organización debe controlar los cambios previstos, y revisar las consecuencias de los cambios no deseados, la adopción de medidas para mitigar los posibles efectos adversos, según sea necesario. La organización debe asegurarse de que los procesos externalizados se determinan y controlan.	La organización somete a revisión y gestión del riesgo sobre la matriz implementada de manera anual con apego a lo establecido dentro del procedimiento documento para la gestión de riesgos. Se muestra minuta de acuerdos y planeación para la gestión del riesgo por parte de los miembros del comité. Se muestra minuta de reunión del comité del 19 de mayo del 2016, donde se muestra en el orden del día Con temas a tratar: Reporte de altas y bajas de activos de las unidades administrativas, Actualización de la matriz de riesgos, Se muestra notificación de cambios sobre activos de información y riesgos a la matriz establecida., 8 de agosto del 2017,	C
8.2 Evaluación del riesgo de la seguridad de la información. La organización debe llevar a cabo las evaluaciones de riesgos de seguridad de la información a intervalos planificados o cuando se propongan o se lleven a cabo modificaciones importantes, teniendo en cuenta los criterios establecidos en el punto 6.1.2 a). La organización debe retener (detener) información documentada de los resultados de las evaluaciones de riesgos de seguridad de información.	La organización cuenta con resultados delas evaluaciones anuales., 2015 inicial, 2016 primer revisión y 2017 segunda revisión a la seguridad de la información y evaluación de riesgos.	C
8.3 Información del tratamiento del riesgo La organización debe implementar el plan de tratamiento de riesgos de seguridad de la información. La organización debe conservará la información documentada de los resultados del tratamiento de los riesgos de seguridad de información.	La organización cuenta con resultados y soporte documental de la gestión de los planes de tratamiento de riesgos, anuales., 2015 inicial, 2016 primera revisión y 2017 segunda revisión a la seguridad de la información y evaluación de riesgos.	C

9. EVALUACIÓN DEL DESEMPEÑO **9.1 Seguimiento, medición, análisis y evaluación.** La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del SGSI. La organización debe determinar: a) lo que necesita ser monitoreado y medido, incluyendo los procesos de seguridad de la información y los controles; b) las modalidades de seguimiento, medición, análisis y evaluación, en su caso, para garantizar resultados válidos; NOTA: Los métodos seleccionados deben producir resultados comparables y reproducibles para ser considerado válido. c) cuando deberá de llevarse a cabo el seguimiento y medición d) que deberá estar en un seguimiento y medición; e) cuando los resultados de seguimiento y medición deberán ser analizados y evaluados, y f) cuando se deberán analizar y evaluar los resultados. La organización deberá de conservará información documentada apropiada como prueba de los resultados del monitoreo y medición.	Lo organización cuenta con soporte documental para la gestión de las mediciones ligadas a la seguridad de la información mismas que se encuentran plasmadas dentro del Acuerdo de Aplicabilidad. SoA. Se cuenta con programa de revisión de controles del anexo A de la norma del 8 de marzo del 2017. RC-PS-SI-008 R/0 TW: RE Formato de gestión del nivel de madurez de controles del SGSI. Del 23 al 27 de octubre del 2017. Protocolo re auditoria forense Pt- te-ei-03 Rev. 0 del 28 de junio del 2017	C
9.2 Auditoría interna. La organización debe llevar a cabo auditorías internas a intervalos planificados para proporcionar información sobre si el SGSI: a) cumple con 1) las propias necesidades de la organización para su SGSI, 2) los requisitos de esta norma internacional; b) se ha implementado y mantiene de manera eficaz. La organización debe: c) planificar, establecer, implementar y mantener un programa(s) de auditoría, incluida la periodicidad los métodos, responsabilidades, requisitos de planificación y presentación de informes. Las auditorías programadas) deberán tomar en consideración la importancia de los procesos en cuestión y los resultados de auditorías anteriores; d) definir los criterios de auditoría y el alcance de cada auditoría; e) selección de los auditores y realizar auditorías que garanticen la objetividad e imparcialidad del proceso de auditoría; f) asegurarse de que los resultados de las auditorías se reportan a la gerencia pertinente, y g) conservar la información documentada como evidencia de la auditoría programada) y los resultados de la auditoría.	La organización cuenta con soporte documental para el ejercicio y gestión de la auditorías internas al a sus Sistemas de gestión implementados. Procedimiento de auditoria interna PG.PS-GC.04 Rev. PG.II del 16 de noviembre del 2017. Calendario de auditoria RC-PS-GC-004 .4 /tde re se muestra la programación de auditorías a los sistemas de gestión , calidad, seguridad de la información, RS, así mismo se muestra la programación de auditorias de carácter externo ATR, Se muestra plan de auditoria RC-PS-GC-005 a los sistemas de gestión con fecha del 18 de septiembre del2017. Reunión de apertura 23-10-2017 Auditoria del 23 al 27 de octubre del 2017 Cierre 27 de octubre del 2017 Criterios establecidos de auditoria, lo que la norma, lo que la organización y consideración del marco legal aplicable. Se muestra listas de verificación RC-PS-GC-006 R-3 TD reporte de auditoria RC-PS-GC-007 Informe de auditoría R-2 TD-:RE Auditora (Minerva Ascencio Ramirez) Total de auditores participantes 19 Se muestra registro de evaluación de desempeño de auditores 2017.	C

	Muestreo de auditores evaluados (puntaje máximo 4) Criterios a evaluar (teoría, resultado de evaluación anterior y desempeño de auditoria) Carmen lucia Vargas Curiel = 3.82 / 4 Claudia Verónica Gómez Varela = 3.82 / 4 Grisel Gabriela casillas García = 3.63 / 4 Minerva Ascencio Ramírez = 3.59 / 4 Roberto Alejandro Fernández Hernandez = 3.7 / 4 Maria Guadalupe Cabral Cazares = 3.76 / 4 Se cuenta con soporte documental para la selección, inducción y evaluación de las y los auditores internos. PG-PS-GC-08 REV. 11 del 16-11-2017 Resultado integral de auditoria. NC-M = 12 NC-m = 82 Observaciones = 182 Se da seguimiento al resultado de las NC-M detectadas en el ejercicio de auditoria dela año pasado Con fechas de ejecución del 7 al 9 de noviembre del 2017 por ATR., Se muestran cerradas véase sección correspondiente.	

9.3 Revisión por la dirección La alta dirección debe revisar el SGSI de la organización a intervalos planificados para asegurarse de su conveniencia, adecuación y eficacia. La gestión revisión por la dirección debe incluir la consideración de: a) el estado de las acciones de las revisiones por la dirección previas; b) los cambios en los problemas externos e internos que son relevantes para SGSI; c) la retroalimentación sobre el desempeño de la seguridad de la información, incluyendo las tendencias en: 1) las no conformidades y acciones correctivas; 2) seguimiento y medición a los resultados; 3) los resultados de auditoría, y 4) el cumplimiento de los objetivos de seguridad de la información; d) la retroalimentación de las partes interesadas; e) los resultados de la evaluación del riesgo y el estado del plan de tratamiento de riesgos, y f) oportunidades para la mejora continúa. Las salidas de la revisión por la dirección deben incluir las decisiones relacionadas con las oportunidades de mejora continua y de cualquier necesidad de cambios en el SGSI. La organización deberá de conservar la información documentada como evidencia de los resultados de las revisiones por la dirección.	La organización cuenta con soporte documental para la gestión del ejercicio de las revisiones por la dirección a los sistemas de gestión implementados. Dentro del manual de los sistemas de gestión se establecen las directrices para el ejercicio de revisiones por la dirección. La Alta Dirección revisa el avance del SGSI 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. En esta evaluación se incluyen las oportunidades de mejora y la necesidad de efectuar cambios en el sistema incluyendo la política integral y los objetivos de seguridad de la información, así como la evaluación y tratamiento de los riesgos. En el procedimiento de revisión de direcciones PG-AS-AS-02 se establecen los lineamientos que se deberán seguir al respecto. Se conservan los documentos asociados a las revisiones de la dirección (ver procedimiento PG-PS-GC-03). Revisiones trimestrales (de avances de POA), Última revisión por la dirección., completa anual en el 4to trimestre del 2016. Se muestra cumplimiento: a los requisitos de entrada conforme a lo establecido en la norma ISO 9001:2015, e ISO 27001:2013 Se muestra las 4 minutas trimestrales del año 2016, Así mismo se muestra 3 minutas de revisiones por la dirección correspondiente a las revisiones	C

10. MEJORA DEL SGSI **10.1 No conformidad y acciones correctivas** Cuando se produce una no conformidad, la organización deberá: a) reaccionar a la no conformidad, y según sea el caso: 1) tomar medidas para controlar y corregirlo, y 2) hacer frente a las consecuencias; b) evaluar la necesidad de acciones para eliminar las causas de no conformidad, con el fin de que no vuelva a ocurrir o se producen en otros lugares, a través de: 1) la revisión de la no conformidad; 2) determinar las causas de la no conformidad 3) determinar si existen incumplimientos similares o podrían producirse; c) poner en práctica las medidas oportunas; d) revisar la eficacia de las medidas correctivas tomadas, y e) realizar cambios en el sistema de gestión de seguridad de información, si es necesario. Las acciones correctivas deben ser apropiadas a los efectos de las no conformidades encontradas. La organización debe conservar información documentada como evidencia de: f) la naturaleza de la no conformidades y de cualquier acción tomada, posteriormente, y g) el resultado de cualquier acción correctiva.	Se cuenta documentado un plan de tratamiento de riesgo., actualmente al organización cuenta con 3 PTR abiertos y en proceso. Folio PTR-01 del 3 de nov. Del 2015, Robo de información, infestación de archivos, copias no controladas y autorizadas. Abierto. Folio PTR-02 del 3 de noviembre del 2015 Falta de conciencia, políticas de seguridad, capacitación, manejo inadecuado de la encriptación, degradación en la seguridad de la información. Abierto. Folio PTR-03 del 22 de septiembre del 2015 Falta de conciencia respecto a la seguridad de la inf. Falta de mecanismos de vigilancia., Cerrado: Noviembre del 2016. Se muestra registros de acción correctiva de auditoria interna en proceso de seguimiento: No. 05AC, No. 04AC, No. 10AC = DEL 2017 Se muestra soporte documental y registros para la atención de las no conformidades antes mencionadas., Oficios.,0882 / 2017, 859/ 2017 del 14-11-2017 Asiendo a lesión a las políticas 38, 75 de cambio de perfiles y personal., Así mismo se muestra los oficios de acciones correctivas en seguimiento. 847/2017 10-11-2017 855/ 2017 10-11-2017 8290/2017 16-11-2017 419/2017 16-11-2017	**NC**

10.2 mejora continua La organización debe mejorar continuamente la conveniencia, adecuación y eficacia del sistema de gestión de seguridad de la información.	En la ASEJ nos hemos propuesto mejorar continuamente la idoneidad, adecuación y eficiencia del SGSI, mediante la difusión y el cumplimiento de la Política Integral, los objetivos de seguridad de la información, el análisis y evaluación de riesgos, los resultados de las auditorías y el análisis de datos, las acciones correctivas y la revisión por la o el Auditor Superior.	C
Quejas recibidas por parte de las partes interesadas.	Véase seguimiento a la gestión de incidentes de seguridad Dominio A.16.	C

ANEXO A **ACUERDO DE APLICABILIDAD SOA., VERSIÓN:_____**		
CONTROLES	**DESCRIPCIÓN DE LA MUESTRA Y EVIDENCIA PRESENTADAS (PROCESO, FECHA, SITIO, ETC.)**	**Hallazgo**
A.5 Políticas de seguridad de la información. **A.5.1 Dirección de gestión de seguridad de la información.** **Objetivo: Proporcionar orientación y apoyo a la gestión de seguridad de la información de acuerdo con los requerimientos** del negocio y las leyes reglamentos pertinentes. A 5.1.1 Política para la seguridad de la información. A.5.1.2 Revisión de las políticas para el control de la seguridad de la información.	La organización cuenta con 95 políticas generales orientadas a la seguridad de la información, estas declaradas ante su SGSI. Se ejecutan revisiones anuales a los soportes documentales, revisión de la evidencia de los controles, y procesos de auditorias internas al SGSI.	c
A.6 Organización de la seguridad de la información. **6.1 Organización Interna** **Objetivo: Establecer una gestión y estructura de trabajos para iniciar y controlar implementación y el funcionamiento de la organización de la seguridad de la información**. A 6.1.1 Roles y responsabilidades de la seguridad de la información. A 6.1.2 Seguridad de la funciones. A 6.1.3 Contacto y comunicación y contactos con autoridades. A 6.1.4 Contacto y comunicación con grupos especiales de interés. A 6.1.5 Control de proyectos para la seguridad de la información.	La organización cuenta ha determinado la implementación de un comité de seguridad de la información, donde todas las áreas operativas dentro del alcance de los sistemas de gestión cuenta con presencia y participación. Se establece por oficio los roles y responsabilidades de cada uno de los miembros del comité. Responsabilidades asignadas orientadas a la seguridad de la información tales como: Enlace entre las áreas del alcance Gestión y validación del inventario de activos Identificación y clasificación documental Análisis y evaluación de riesgos Gestión de amenazas y vulnerabilidades Gestión de impactó en las vulnerabilidades Apoyo en el establecimiento de controles Gestión y difusión del SoA Apoyo en la aplicación de políticas y procedimientos Gestión y tratamiento de PTR´s . Contactos con autoridades: Congreso del estado, Policías locales, CISEN,	C

	Contacto con grupos de interés, La jefatura del departamento de evaluación estadística y sistemas, se muestra registros de notificación foro Kaspersky, boletines de firewall Fortinet así mismo suu muestra registros en foro de Cisco Sistemas, inteco, Microsoft., Cada una de las notificaciones obtenidas es analizada por la jefatura y segregada en comunicación con el personal del área de soporte técnico y desarrollo.,	
A.7. Seguridad en el recurso Humano. **A.7.1 Previo al empleo.** **Objetivo: Para asegurarse de que los empleados y contratistas conozcan y cumplan con sus responsabilidades de seguridad de la información.** A 7.1.1 Proyección (monitoreo) en las contrataciones análisis de antecedentes. A 7.1.2 Términos y condiciones para la contratación. **A7.2 Durante el empleo.** **Objetivo: Para asegurarse de que los empleados y contratistas conozcan y cumplan con sus responsabilidades de seguridad de la información.** A 7.2.1 Gestión de la responsabilidades. A 7.2.2 "Educación , concientización y capacitación en la seguridad de la información " A 7.2.3 (procesos) Controles Disciplinarios. **A 7.3 Terminación y cambio de empleo.** **Objetivo: Proteger los intereses de la organización durante (como parte) (d) el cambio o término del empleo.** A 7.2.3 Términos o cambios de las responsabilidades del empleado.	La organización cuenta con políticas para la gestión de la seguridad de la información ligadas al personal en tres tiempos: Durante la selección, Dúrate el empleo / relación laboral Y posterior al empleo. POLÍTICAS DE RECURSOS HUMANOS P33.- "Es responsabilidad de la o el Director General de Administración asegurarse de que las personas contratadas tengan la competencia necesaria para realizar trabajos que afecten el desempeño de seguridad de la información". P34.- "La información de todas y todos los candidatos debe ser validada antes de ser contratado/a". P35.- "Todo personal de reciente ingreso deberá ser orientado/a sobre sus funciones y responsabilidades en relación a la seguridad de la información referente a las actividades de su puesto". P36.- "Dependiendo del tipo y características de su trabajo, al personal de nuevo ingreso se le asignará el perfil sobre acceso a programas, identificaciones, uniformes, etc." P37.- "Todo el personal de nuevo ingreso deberá ser capacitado/a en aspectos de seguridad de la información y ser evaluado/a en cuanto a su aprendizaje". P38.-"La o el titular de la unidad administrativa correspondiente deberá, en un plazo máximo de un día, enviar comunicado oficial para la remoción de perfil del personal que ha sido dado de baja de su puesto de trabajo". P39.- "La o el Jefe del Departamento de EIES, es responsable de respaldar la información generada por el personal que sea separado de su trabajo y cuyo aviso ha sido dado por la o el titular de la unidad administrativa correspondiente". P40.- "El personal que sea separado de su puesto deberá realizar un proceso de entrega-recepción de	C

	los activos asignados y de la información generada por él/ella en su puesto".	

A.8. Gestión (administración) de los activos. **A.8.1 Propiedad de los activos.** **Objetivo: La organización e identificación de los activos así como definir las responsabilidades apropiadas para su protección.** A.8.1.1 Inventario de activos A.8.1.2 propiedad de los activos A.8.1.3 Uso aceptable e los activos A.8.1.4 Retorno de los activos	La organización cuenta con 2 inventarios de activos uno de ellos declarado ante la matriz de gestión de riesgos donde se controla los activos de información por categoría analizando las amenazas y vulnerabilidades para daca tipo de activo declarado y un control sobre la cantidad de activos en la organización , declarando DVR, equipo de escritorio, portátiles, sistemas de comunicación. La política 64 habla del uso aceptable de los equipos. POLÍTICAS PARA LA OPERACIÓN DE LOS ACTIVOS. P14.- "Se deberá elaborar y mantener un inventario de activos, el cual estará a cargo de la o el Representante de Sistema de Seguridad de la Información (RSI) y cualquier cambio o modificación de algún activo deberá ser reportado por la o el dueño del activo al RSI". P15.- "La clasificación de los activos deberá realizarse de acuerdo al procedimiento para el establecimiento de la matriz de administración de riesgos de la ASEJ". P16.- "La o el RSI debe revisar el inventario de activos al menos una vez por año a fin de corroborar su vigencia y actualización". P17.- "Todos los activos deben contar con un responsable o dueño/a, quien deberá verificar que el activo esté funcionando correctamente". P18.-"Queda estrictamente prohibida la extracción de cualquier activo perteneciente a la institución sin que exista una previa autorización de la o el titular de la unidad administrativa correspondiente, o bien, de la o el titular de la institución". P19.- "Los activos deben ser utilizados con fines estrictamente laborales y no para uso privado o doloso".	C

A.8.2 Clasificación de la Información. **Objetivo Asegurar que la Información reciba un nivel de seguridad apropiado y en concordancia con la importancia de la organización.** A8.2.1 Clasificación de la información A8.2.2 Etiqueta de la información A8.2.3 Manejo de los activos A8.3.1 Gestión de los medios removibles A8.3.2 Eliminación de los medios A8.3.3 Medios físicos en transito	La organización cuenta con soporte documental para la clasificación de documentos. Guía para la clasificación de la información GI-PS-SI-01 Rev. 3 del 21 de julio del 2017. Tipo de clasificación (Fundamental, libre acceso, restringida y confidencialidad). Con apego al marco legal aplicable se gestiona. Manejo de activos. P64.- "Es responsabilidad de la o el empleado que el uso del equipo sea exclusivamente para fines laborales; en la PC se habilitarán únicamente los puertos, servicios y aplicaciones necesarios para el desempeño de las actividades laborales de las y los empleados. En caso de que por alguna necesidad laboral se requiera habilitar algún puerto o servicio, se debe contar con la autorización de la o el titular de la unidad administrativa correspondiente. Se muestra soporte documental para la gestión del borrado seguro, PT-TE-EI- 02 rev. 0 del 6 del – nov. Del 17. La organización cuenta con aplicación para la gestión del borrado seguro y eliminación e medios., KillDisk V.10 Eraser Hard Drive. Se muestra registro de notificación de borrado seguro oficio 929/2017, del 24 de noviembre del 2017. Equipo borrado del lic. Lorenzo estrada La aplicación emite certificado de borrado seguro, Fecha del borrado. 22-11-2017 HDD Western de 37.3 GB. S/N. 337A0C Se cierra observación levantada en el 2016 por proceso de auditoria externa. Se cuenta con políticas y controla para la gestión delos medios físicos en tránsito. La organización cuenta con soporte documental para la gestión delos medios físicos en tránsito. Dentro del as Políticas generales no. 62 establece que los medios físicos deberán de ser	C

A.9 Control de Acceso **A.9.1. Requerimientos de la organización para el control del acceso.** **Objetivo: limitar el acceso a la información y las instalaciones de procesamiento de la información y servicios.** A9.1.1 Políticas de control de acceso A9.1.2 Acceso a la red Y servicios de la red.	POLÍTICAS PARA EL ACCESO Y PERMANENCIA EN EL EDIFICIO P6.- "El personal interno debe registrar su entrada y salida en los puntos de control establecidos, y deberá portar su identificación de manera visible en todo momento dentro de las instalaciones de la institución". P7.- "El personal que no tenga su gafete no podrá ingresar al edificio, salvo que obtenga autorización de la o el titular de la unidad administrativa correspondiente". P8.- "Las salidas de emergencia deben permanecer cerradas, y solo deberán utilizarse en caso de contingencia". P9.- "Todo visitante o proveedor que ingrese a las instalaciones deberá registrarse e informar al personal de ingreso el nombre de la persona con la que desea entrevistarse, presentar una identificación oficial vigente y portar el gafete correspondiente". P10.- "Personal interno deberá acompañar a las y los visitantes y proveedores desde el momento de ingreso hasta su salida". P11.- "El personal del área de recepción realizará un informe mensual de las y los visitantes y proveedores que tuvieron acceso al edificio". P12. -"El personal que no porte el corbatín de acceso al estacionamiento no podrá ingresar al mismo. El corbatín deberá permanecer en el automóvil de manera visible" Aun y cuando la organización cuenta con soporte documental para la gestión del control de acceso, privilegios, servicios, RED, se cuenta con PTR Abierto.	**NC**
A9.2 Gestión de accesos de usuario. **Objetivo: Asegurar el acceso a los usuarios autorizados y evitar el acceso no autorizados a los sistemas de información y servicios.** A9.2.1 Registro de usuarios (login and logout Entrada y salida de los usuarios. A9.2.2 Gestión delas claves de usuarios asignadas. A9.2.3 Gestión de los Privilegios. A9.2.4 Gestión de la autenticación secreta de los usuarios de información. A9.2.5 Revisión de los derechos de acceso de los usuarios. A9.2.6 Remoción o ajustes (modificación) de los derechos de acceso.		
A9.3 Responsabilidades de los usuarios. **Objetivo Para responsabilizar a los usuarios de las cuentas de autenticación.** A9.3.1 Uso de las cuentas de autenticación (uso de la autenticación secreta.		
A9.4 Control de Acceso a los sistemas o aplicaciones. **Objetivo Prevenir el acceso no autorizados a las aplicaciones del sistema de la información.** A9.4.1 Restricción de acceso a la información. A9.4.2 Procedimiento de loggeo (entrada) segura. A9.4.3 Sistema de gestión de contraseñas. A9.4.4 Uso de Privilegios y utilidades del sistema. A9.4.5 Control de acceso al código fuente.		
A.10 Criptografía. **A.10.1 Controles criptográficos.** **A.10.1.1 Políticas sobre el uso de controles criptográficos.** A.10.1.2 Administración (Gestión) de claves.	Dentro del as Políticas generales no. 62 establece que los medios físicos deberán de ser encriptados y autorizado por las partes interesadas pertinentes. Se muestra oficio de gestión de medios No. 366/2017 del 8 de noviembre del 2017. Herramienta de encripción End-Point Security, de GFI.	**C**

A11.Seguridad Física y ambiental. **A.11.1 Áreas Seguras.** **Objetivo: Evitar el acceso físico no autorizado, daño o interferencia a la información de la organización o a los medios procesamientos de la información.** A11.1.1 Seguridad física y perimetral. A11.1.2 Control de entradas físicas. A11.1.3 "Seguridad de oficinas, habitaciones y medios". A11.1.4 Protección contra amenazas externas y ambientales. A11.1.5 Trabajo en áreas seguras. A11.1.6 Áreas de carga y descargas. Excluido	Se cuenta con Medios para garantizar que el acceso a los activos está restringido y autorizado, en base a los requerimientos de la institución y de la seguridad. Se cuenta con personal asignado a la seguridad de las áreas físicas y control de accesos tanto del personal de la organización como de terceros y partes interesadas.,	C
A11.2 Seguridad del equipo. **Objetivo Evita la perdida, daño robo o compromiso de los archivos y la interrupción de las actividades de la organización.** A11.2.1 Ubicación y protección de equipo. A11.2.2 Servicios Públicos. A11.2.3 Seguridad en el cableado. A11.2.4 Mantenimiento del equipo. A11.2.5 Traslado o movimiento de activos. A11.2.6 Seguridad del equipo Fuera del local (organización). A11.2.7 Eliminación segura o re-uso de activos. A11.2.8 Equipo de usuario desatendido. A11.2.9 Políticas de pantalla y escritorio limpio.	La organización cuenta con soporte documental y políticas institucionales para la gestión las tecnologías de la información, control de medios en tránsito, tales como: POLÍTICAS DE SISTEMAS DE INFORMACIÓN P29.- "Los requerimientos para el desarrollo de sistemas de información nuevos o cambios en los sistemas existentes, se apegarán a las políticas y procedimientos de desarrollo de sistemas de información". P30.- "En el proceso de desarrollo se debe verificar que el procesamiento de las aplicaciones sea adecuado, considerando los siguientes puntos: ▯ Entrada de datos. ▯ Procesamiento interno. ▯ Integridad de mensajes. ▯ Salida de datos. P31.- "La instalación de software operacional debe seguir un procedimiento para su adecuado control a fin de minimizar el riesgo de corrupción". P32.- "El área de desarrollo de sistemas de información debe evitar el uso de bases de datos operacionales que contengan información personal o confidencial para propósitos de pruebas de los sistemas de información y aplicaciones". POLÍTICAS DE OPERACIÓN P55.- "Todo/a usuario/a que requiera acceso a los sistemas o servicios de la institución deberá contar con la autorización de la o el titular de la unidad administrativa correspondiente y deberá utilizar una cuenta de usuario/a y contraseña, la cual es confidencial, por lo que queda totalmente prohibida su divulgación o préstamo".	C

A.12 Seguridad en las operaciones. **A12.1 Procedimientos y responsabilidades operacionales.** **Objetivo: Asegurar la operación correcta y segura de los medios de procesamiento de información.** A12.1.1 Procedimientos de operaciones documentados. A12.1.2 Gestión de cambios. A12.1.3 Gestión de capacidad. A12.1.4 Separación de los medios de desarrollo y operacionales. **A12.2 Protección del código malicioso.** **Objetivo: asegurar que la información y los medios de manejo de la información son protegidos contra el código malicioso.** A.12.2.1 Controles contra Software maliciosos.	P56.- "Después de tres intentos consecutivos fallidos para introducir la contraseña en el mismo día, el equipo de la o el empleado será bloqueado. La o el usuario es responsable de solicitar el desbloqueo al Departamento de EIES". P57.- "Después de un periodo de inactividad de 5 minutos en una sesión de usuario/a, se debe habilitar de manera automática el bloqueo con contraseña del equipo de trabajo, lo cual será configurado previamente por el personal del Departamento de EIES, o bien, la o el empleado deberá habilitar el bloqueo de contraseña manualmente, si se retira de su sitio de trabajo". P58.- "Todos los equipos de cómputo utilizados dentro de los procesos considerados dentro del alcance, deberán contar con un sistema antivirus autorizado para su uso. Su instalación es responsabilidad del Departamento de EIES". P59.- "Queda estrictamente prohibida la instalación de todo tipo de software que no cuente con las licencias correspondientes para su uso. En caso de que, por necesidades laborales, se requiera la instalación de software, debe contarse con la autorización de la o el titular de la unidad administrativa correspondiente y solicitar la instalación a la o el Director Técnico y/o Jefe/a del Departamento de EIES".	
A.12.3 Respaldos. **Objetivo: Mantener la disponibilidad e integridad de los servicios de procesamientos de la información. (Protección contra la pérdida de información).** A12.3.1 Respaldos de la información.	POLÍTICAS DE RESPALDOS P49.- "Se deben realizar respaldos totales de los sistemas y bases de datos, los cuales deberán ser resguardados de acuerdo al procedimiento para el respaldo de información". P50.- "Deberá asegurarse la integridad de los respaldos realizados. A su vez, se ejecutarán pruebas de recuperación a las bases de datos al menos una vez cada 3 meses, y este evento deberá registrarse en la bitácora de recuperación de respaldos". P51.- "Se deberá realizar un respaldo completo mensual de la base de datos en un medio extraíble (cintas magnéticas, medios ópticos, discos externos, USB o el que se designe) el cual será entregado de acuerdo a lo estipulado en el procedimiento para el respaldo de información" P52.- "Se deberán realizar respaldos incrementales semanales de sistemas, archivos y la base de datos, los cuales se almacenarán en cinta magnética". P53.- "Los medios que sean utilizados para los respaldos deberán estar plenamente identificados con etiquetas y su respectivo código".	C

A12.4.1 Registro y seguimiento. **Objetivo: Detectar y generar evidencia de los eventos en los sistemas de la información.** A12.4.1 Registro de eventos. A12.4.2 Protección de la información de los registros. A12.4.3 Registro del administrador y operador. A12.4.4 Sincronización de relojes.	La organización ha implementado un sistema NTP para la gestión de la sincronización de relojes. Con la finalidad de mantener en integridad y trazabilidad las bitácoras y registros electrónicos.	C
A12.5 Control de Accesos a los sistemas de operaciones. **Objetivo: Asegurar la integridad de los sistemas operacionales (sistemas operativo).** A12.5.1 Instalación de software en sistemas operacionales (Sistemas Operativos)	Queda estrictamente prohibida la instalación de todo tipo de software que no cuente con las licencias correspondientes para su uso. En caso de que, por necesidades laborales, se requiera la instalación de software, debe contarse con la autorización de la o el titular de la unidad administrativa correspondiente y solicitar la instalación a la o el Director Técnico y/o Jefe/a del Departamento de EIES".	C
A12.6 Explotación de vulnerabilidades Técnica. **Objetivo: Reducir el Riesgo de la explotación de vulnerabilidades técnicas públicas.** A12.6.1 Gestión de la vulnerabilidad técnica. A12.6.2 Restricción de instalación de software.	Se encuentra en proceso de ejecución de análisis de vulnerabilidad técnica y ejercicio de PENTEST, Trabajos ejecutados por el proveedor TELENET DE MEXICO SA DE CV del 6 de Noviembre al 01 de diciembre del 2017 Análisis de Vulnerabilidad del 27 de Noviembre al 8 de diciembre del 2017. Esto en seguimiento a las observaciones derivadas de las observaciones de auditoria externa en el 2016. Oficio con descripción del seguimiento No. 060-2017 Del 26 de enero del 2017. Documentos implementados PE-TE-EI-02, PE-TE-EI-09 y PE-TE-EI-10,	C
A12.7 Consideración de auditorías de los sistemas de información. **Objetivo: Minimizar el impacto de la actividades de auditoria a los sistemas de operación.** A12.7.1 Control de auditoria para los sistemas de información.		
A.13. Seguridad en la comunicación. **A13.1. Gestión de seguridad en RED.** **Objetivo: Asegurar las protecciones de la información en la red y la protección de la infraestructura de soporte.** A13.1.1 Control de RED. A13.1.2 Seguridad en los servicios de Red. A13.1.3 Segregación de las REDES	Se cuenta con segmentación de redes de Voz y Datos, así como gestión de direccionamiento IP fijo.	C

A.13.2 Intercambio de información. **Objetivo: Mantener la seguridad de la información y software de la organización en las transferencias con organizaciones u entidades extremas.** A13.2.1 Políticas y procedimientos documentados para la transferencia de información. A13.2.2 Acuerdos de (intercambio) Transferencia de información. A13.2.3 Mensajes electrónicos A13.2.4 Acuerdos de confidencialidad.	Se muestra registro de segmentación e RED y sistema de Firewall. Para la gestión de la trasferencia de información por las redes internas y externas. Se cuenta con las políticas y acuerdos de aplicabilidad, tanto del personal interno como de terceros y partes interesadas.	C
A.14 Adquisición de desarrollo y mantenimiento de los sistemas de información. **A14.1 Requerimiento de seguridad en los sistemas.** **Objetivo: Asegurar que la seguridad sea una parte integral de los sistemas de información a través del ciclo de vida de, Este deberá de incluir los requerimientos de los servicios de los sistemas de información sobre la presentación de servicios en las redes públicas.** A.14.1.1 Análisis y especificación para los requerimiento de seguridad A.14.1.2 Servicios de aplicación de la seguridad en redes publicas A.14.1.3 Protección en la transacción de servicios y aplicaciones	La organización cuenta con soporte documental para la gestión del desarrollo de software. PE-TE-EI-07 Procedimiento de desarrollo y aplicación de la intranet P29.- "Los requerimientos para el desarrollo de sistemas de información nuevos o cambios en los sistemas existentes, se apegarán a las políticas y procedimientos de desarrollo de sistemas de información". P30.- "En el proceso de desarrollo se debe verificar que el procesamiento de las aplicaciones sea adecuado, considerando los siguientes puntos: ▯ Entrada de datos. ▯ Procesamiento interno. ▯ Integridad de mensajes. ▯ Salida de datos. P32.- "El área de desarrollo de sistemas de información debe evitar el uso de bases de datos operacionales que contengan información personal o confidencial para propósitos de pruebas de los sistemas de información y aplicaciones".	C
A.14.2 Seguridad en los procesos de desarrollo y soporte. **Objetivo: Mantener la seguridad del software e información de los sistemas de aplicación. Considerado en ciclo de vida.** A.14.2.1 Políticas de seguridad para el desarrollo. A.14.2.2 Procedimiento para el control de cambios. A.14.2.3 Revisión técnica de las aplicaciones después de cambios en los sistemas de software. A.14.2.4 Restricción en cambios sobre los paquetes de software. A.14.2.5 Principios de ingeniería de sistemas de seguridad. A.14.2.6 Seguridad en el entorno de desarrollo. A.14.2.7 Contratación y desarrollo de software outsourced. Excluido		
A.14.3 Pruebas a la información. **Objetivo: Garantizar la información de los datos utilizadas en pruebas.** A.14.3.1 Protección de los datos de pruebas.		

A.15 Relaciones con proveedores. **A.15.1. Seguridad de la información y activos de la organización que son accedidos por proveedores.** **Objetivo: Asegurar la protección de la información y activos de la organización que son accedidos por proveedores.** A.15.1.1 Políticas de seguridad para proveedores. A.15.1.2 Abordar la seguridad dentro de los acuerdos con proveedores. A.15.1.3 Abordar la información y la tecnología dela información en la cadena de proveedores.	La organización cuenta con soporte documental para la gestión dela proveeduría., Se muestra en transparencia dela página oficial de la ASEJ, Telenet cuenta con plataforma para levantamiento de tickets, Help Desk. Se muestrea contratos de proveeduría: Gama Sistemas : Telenet: Se muestra convenio de confidencialidad. En términos de la seguridad de la información y tecnologías de la información será el departamento de TIC´s quien evalúe la calidad del servicio proporcionado. POLÍTICAS DE PROVEEDORES P41.-"Todo servicio proporcionado por terceros debe ser solicitado de acuerdo a lo estipulado en las políticas de adquisiciones de la institución, considerando la seguridad de la información independientemente del tipo de proyecto". P42.- "Todo servicio proporcionado por terceros en su contrato de trabajo debe contener las cláusulas de confidencialidad necesarias para cumplir con la legislación aplicable en materia de acceso a la información y protección de datos personales". P43.- "Los servicios entregados por terceros se deben supervisar y monitorear a fin de evitar accesos a información no autorizados o fallas en la entrega de los servicios contratados". P44.- "En caso de requerirse cambios en los servicios proporcionados por terceros, se analizará el impacto en los procesos operativos, a fin de que éstos puedan ser administrados adecuadamente". P45.- "Se debe llevar a cabo un análisis de riesgos de acceso de terceros para identificar los controles necesarios a implementar, a fin de garantizar la seguridad de la información en la institución y deberán documentarse los mismos". P46.- "Antes de dar acceso a proveedores a la información o a las instalaciones de la institución, se deben haber tratado los riesgos resultantes del análisis previo". P47.- "Los acuerdos de seguridad con terceros deben considerar: 1. El apego a las políticas de seguridad vigentes. 2. Especificar el monitoreo del acceso a la información o instalaciones de procesamiento de información de la ASEJ. 3. Auditorías al servicio contratado. 4. Niveles de servicio especificado y responsabilidad por incumplimientos del contrato".	C
A.15.2 Gestión de la presentación de servicios de proveedores (gestión de la entrega de servicios por terceros). **Objetivo: Implementar y mantener el nivel apropiado de seguridad de la información y entrega de servicios en línea con los contratos de servicio.** A.15.2.1 Monitoreo y revisión de los servicios de proveedores (terceros). A.15.2.2 Gestión de los cambios en los servicios de proveedores (terceros).		

A.16 Gestión de incidentes de seguridad de la información. **A.16.1Gestion de incidentes a la seguridad de la información y mejoras.** **Objetivo: asegurar un efecto y consistente a la gestión de los incidentes a la seguridad de la información, incluyendo la comunicación de los eventos de seguridad y las debilidades.** A.16.1.2 Reporte de eventos en la seguridad de la información. A.16.1.3 Reporte de debilidades a la seguridad de la información. A.16.1.4 Evaluación y decisión en los eventos de seguridad. A.16.1.5 Responsabilidades en los incidentes de seguridad. A.16.1.6 Aprendizaje de los incidentes de seguridad dela información A.16.1.7 Recolección de evidencias	Seguimiento a incidente severo del 21 de noviembre del 2017, se muestra Oficio de notificación 928/2017, Se muestra gestión de las actividades en seguimiento para servicio de implementación de servidor Bizit4U. Estatus incidente de seguridad = en proceso Se detona revisión y mantenimiento a los sistemas de información y centros de datos programados junto con proveedores para el próximo 2 de diciembre el 2017	C
A.17 Seguridad de la información para la continuidad de las operaciones (negocio) **A.17.1 Continuidad de la seguridad dela información.** **Objetivo: asegurar que la continuidad de las operaciones (del negocio) se encuentra incluido en el sistema de gestión para la continuidad de las operaciones (negocio).** A17.1.1 Información para la continuidad de las operaciones incluyendo la seguridad de la información. A17.1.2 Implementación de plan y procedimientos para la continuidad de las operaciones y seguridad de la información. A17.1.3 "Verificar, revisar y evaluar la continuidad de las operaciones y seguridad de la información".	La organización cuenta con soporte documental para la gestión de la continuidad de la operaciones., Procedimiento para la ejecución del plan de continuidad de las operaciones. PG-PS-SI-06. Rev.3 del 21 de julio del 2017. Considera criterios para la activación ligando a los incidentes e incidentes severos, considera las áreas, TIC´S , COORDINACIÓN GENERALD E MERGENCIAS, dirección general de administración, coordinación general de la unidad interna de protección civil, personal de Bases de datos y telecomunicaciones Se muestra registros y evidencias del 12 de noviembre del 2016 de la gestión de la continuidad de las operaciones. Se muestra correo para soporte y pruebas a l plan de continuidad de las operaciones., Fecha del correo 27-11-2017, proveedor asignado Gama sistemas. TELENET de México, mantenimiento y pruebas a la continuidad en los equipos de telecomunicaciones., Programadas para el sábado 2 de diciembre del 2017. Así como registros de avances de pruebas y mantenimientos del 2017 proveedor Gama Sistemas Se muestra reportes por parte de proveedor de los servicios y equipos probados. Del 2016	C

A.17.2 Redundancia. **Objetivo: asegurar la disponibilidad de instalaciones de procesamiento de la información.** A17.2.1 Disponibilidad de las instalaciones de procesamiento de información.	La organización cuenta con infraestructura tipo BLADE, servidores virtual izados, cada uno delos balde cuenta con UPS de respaldo. Se cuenta con planta de suministro eléctrico, así mismo se cuenta con UPS, 30 y 15 KVA., Se muestra registros de bases de datos., incrementales diarios. Herramienta de respaldo por tarea programada de Microsoft. Así mismo se respalda en cinta / Ultrium 6. IBM, Robot de respaldo de 1 brazo. Modelo 3573	C
A.18 Cumplimiento. **A.18.1 Cumplimiento con requerimientos legales y contractuales.** **Objetivo: Evitar la violación de cualquier ley u obligación contractual relacionada con la seguridad de la información y cualquier requerimiento en la seguridad de la información.** A18.1.1 Identificación de la legislación aplicable y requerimientos contractuales. A18.1.2 Derechos de propiedad intelectual. A18.1.3 Protección de los registros. A18.1.4 Privacidad y protección de información de personas identificables. A18.1.5 Regulación de los controles criptográficos.	La organización muestra cumplimiento con la propiedad intelectual y el derecho de marca, se muestra registro de licencias de aplicaciones utilizadas en la organización VLM, de Microsoft., Así mismo la organización cuenta con soporte documental para la gestión de la protección de datos personales en posesión de los particulares. Con apego al marco legal aplicable., La aplicación implementada de End-Point, de GFI. cuenta con registro y autorización de las regulaciones nacionales e internacionales de controles y llaves de criptografía.	C
A.18.2 Revisiones a la seguridad de la información. **Objetivo: Implementar políticas y procedimientos para asegurar la seguridad de la información en concordancia con las organización.** A18.2.1 Revisiones independientes a la seguridad de la información. A18.2.2 Cumplimiento con el estándar y las políticas de seguridad. A18.2.3 Revisión del cumplimiento técnico.	Se encuentra en proceso de ejecución de análisis de vulnerabilidad técnica y ejercicio de PENTEST, Trabajos ejecutados por el proveedor TELENET DE MEXICO SA DE CV del 6 de Noviembre al 01 de diciembre del 2017 Análisis de Vulnerabilidad del 27 de Noviembre al 8 de diciembre del 2017. Esto en seguimiento a las observaciones derivadas de las observaciones de auditoria externa en el 2016. Oficio con descripción del seguimiento No. 060-2017 Del 26 de enero del 2017. Documentos implementados PE-TE-EI-02, PE-TE-EI-09 y PE-TE-EI-10,	C

CAMBIOS SIGNIFICATIVOS QUE DEBE CONSIDERAR EL EQUIPO AUDITOR PARA LA SIGUIENTE AUDITORÍA PROCESOS, ÁREAS, ELEMENTOS Y ACTIVIDADES
N/A

ASPECTOS RELEVANTES DETECTADOS QUE SE DEBEN CONSIDERAR PARA LA SIGUIENTE AUDITORÍA
Seguimiento a planes de tratamiento del 2015 y acciones correctivas en proceso derivadas de ultima auditoria interna

RESULTADO DE LA AUDITORÍA		
TIPO	SISTEMA DE GESTIÓN	NO CONFORMIDADES MAYORES Y/O MENORES
NC-m-01	SGSI	Requisito: 10 Mejoramiento 10.1 No conformidad y acciones correctivas Cuando se produce una no conformidad, la organización deberá: a) reaccionar a la no conformidad, y según sea el caso: 1) tomar medidas para controlar y corregirlo, y 2) hacer frente a las consecuencias; b) evaluar la necesidad de acciones para eliminar las causas de no conformidad, con el fin de que no vuelva a ocurrir o se producen en otros lugares, a través de: 1) la revisión de la no conformidad; 2) determinar las causas de la no conformidad 3) determinar si existen incumplimientos similares o podrían producirse; c) poner en práctica las medidas oportunas; d) revisar la eficacia de las medidas correctivas tomadas, y e) realizar cambios en el sistema de gestión de seguridad de información, si es necesario.
		Descripción: Durante el proceso de auditoria se detectó que la organización no ha determinado las medidas para controlar y determinar las causas de las no conformidades presentadas, así como el determinar y analizar situaciones similares considerando acciones y cambios en caso de requerirse. Véase sección 10.1 acciones correctivas y planes de tratamiento abiertos desde el año 2015, PTR01. PTR02

SEGUIMIENTO DE NO CONFORMIDADES MENORES (NC-m)			
( )	Se verificó durante la auditoría que el Plan de Acción de la Organización para la atención de las no conformidades menores, es viable ya que contiene una referencia de la misma, responsable, acciones propuestas y fechas compromiso de finalización, para corregir lo detectado.	(X)	La organización debe enviar a American Trust Register S.C. el Plan de Acción para la atención de las no conformidades menores, que incluya: una referencia de la misma, responsable, acciones propuestas y fechas compromiso de finalización, en un plazo no mayor a 90 días naturales. ATR determinará si es aceptable.

En auditorías de certificación, recertificación y cambios de alcance no se podrá recomendar para su dictaminación por parte del Consejo de Certificación de ATR hasta que sea aprobado el Plan de Acción.

La eficacia de las acciones tomadas será revisada en la próxima auditoría, en caso de no evidenciar dicha eficacia, podrán ser declarada(s) como No Conformidad(es) Mayores.

Para auditorías de Mantenimiento y Recertificación: En caso de no enviar a ATR el Plan de Acción para la atención de la(s) no conformidad(es) menor(es) que incluya: una referencia de la misma, responsable, acciones propuestas y fechas compromiso de finalización en los siguientes 90 días naturales, el estatus del Certificado a partir del día 91 será "suspendido", por un periodo máximo de 180 días naturales, pasando dicho plazo y de no haber presentado el Plan de Acción el estatus cambiará a "Cancelado" en auditorías de Mantenimiento o de vencido en auditorías de recertificación.

Pasando los 90 días naturales en auditorías de:

- Cambio de alcance se mantendrá el alcance anterior, hasta la realización de la siguiente auditoría.
- Certificación se podrá realizar nuevamente la auditoría de Etapa 2 en los siguientes 180 días naturales.

APELACIONES DE LOS HALLAZGOS DE AUDITORÍA POR PARTE DE LA ORGANIZACIÓN	
¿Existen diferencias de opinión o puntos no resueltos sobre las No Conformidades declaradas y/o su clasificación?	( ) Sí, se aplicará el procedimiento de apelaciones vigente de ATR
	Descripción de la información que soporta la apelación:
	(X) No, se aplicará el Procedimiento de Apelaciones vigente de ATR

CONFIDENCIALIDAD EN EL MANEJO DE LA INFORMACIÓN
Se ha realizado la auditoría con base en un muestreo y en consecuencia, pueden existir otros hallazgos que no fueron identificados en este ejercicio. Cabe recordar que toda la información a la que tuvo acceso el equipo auditor se maneja con carácter confidencial.

AGRADECIMIENTO
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.

CONCLUSIÓN DE LA AUDITORIA		
( ) **Aceptable**	(X) **Condicionado:**	
Se concluye que el SG de la organización cumple con lo establecido en la norma: **ISO 27001:2013 / NMX-I-27001-NYCE-2015.**	( ) **NO CONFORMIDAD MAYOR** La organización debe atender las no conformidades mayores para su seguimiento y cierre en un plazo no mayor a 90 días naturales a partir de la fecha de este informe.	(X) **NO CONFORMIDAD MENOR** La organización debe presentar un plan de acción para atender las no conformidades menores detectadas en el SG en los 90 días naturales siguientes, para su revisión y aceptación
Por lo que el auditor líder recomienda: ( ) **Otorgar / Certificar** ( ) **Renovar / Recertificar** ( ) **Modificar / Cambio de alcance** (X) **Mantener**		

CLASIFICACIÓN DEL HALLAZGO	
C	Conforme / cumple
NC-M	No conformidad mayor
NC-m	No conformidad menor

NOMBRE Y FIRMA DEL AUDITOR LÍDER	NOMBRE Y FIRMA DEL REPRESENTANTE DE LA ORGANIZACIÓN
 Carlos Guzmán Sigala