



SFP
SECRETARÍA DE
LA FUNCIÓN PÚBLICA

**ÓRGANO INTERNO DE CONTROL EN
TELEVISIÓN METROPOLITANA, S.A. DE C.V.**
CÉDULA DE OBSERVACIONES

ENTE: TELEVISIÓN METROPOLITANA, S.A. DE C.V.

ÁREA AUDITADA: SUBDIRECCIÓN GENERAL DE ADMINISTRACIÓN Y FINANZAS.

CLAVE DE PROGRAMA Y DESCRIPCIÓN DE LA AUDITORÍA: 4.0.0. "SISTEMA DE INFORMACIÓN Y REGISTRO"

SECTOR: EDUCACIÓN
CLAVE DE LA ENTIDAD: 11425

HOJA No. 1 de 2
NÚMERO DE AUDITORIA: 06/2015
NÚMERO DE OBSERVACIÓN: 1
MONTO FISCALIZABLE:
MONTO FISCALIZADO:
MONTO POR ACLARAR: N/A
MONTO POR RECUPERAR: N/A
RIESGO:

OBSERVACIONES

IMPLEMENTACIÓN INCONCLUSA DEL MANUAL ADMINISTRATIVO DE APLICACIÓN GENERAL EN LAS MATERIAS DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES Y EN LA SEGURIDAD DE LA INFORMACIÓN.

Como resultado del análisis efectuado a la implementación del Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y en la Seguridad de la Información (MAAGTICSI), respecto a las actualizaciones al mismo publicadas en el Diario Oficial el 8 de mayo de 2014, mediante el cual las Instituciones tenían como fecha límite para su actualización el 22 de diciembre del 2014 (160 días hábiles siguientes), se determinó que a la fecha de la presente auditoría la Televisora no ha concluido dicha disposición, toda vez que de conformidad a la información proporcionada por la Gerencia de Tecnologías de la Información, respecto de los porcentajes de implementación de los 9 procesos que integran dicho manual, se reporta un avance general del 86.1%, donde únicamente 3 están concluidos al 100%.

Asimismo, como resultado de la revisión efectuada a 6 procesos (equivalente al 67%) de los 9 que integran el MAAGTICSI, se determinó que en 3 de los procesos analizados el porcentaje de cumplimiento es menor al computado por la Gerencia de Tecnologías de la Información, como se muestra a continuación:

Nombre del proceso	Porcentaje según la GTI	Porcentaje determinado por el OIC
Proceso de Planeación Estratégica de TIC	80%	71%
Proceso de Administración de la Seguridad de la Información.	70%	54%
Proceso de Operación de los controles de la seguridad de la Información.	80%	43%

RECOMENDACIONES

CORRECTIVA:

El Subdirector General de Administración y Finanzas gire instrucciones a la Gerencia Tecnologías de la Información, para que a la brevedad lleve a cabo lo siguiente:

Se concluya la implementación del Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y en la Seguridad de la Información MAAGTICSI, respecto de los puntos, formatos y actividades que están pendientes de llevar a cabo de cada uno de los procesos, soportando con evidencia documental los trabajos realizados, a efecto de que no se retrase por más tiempo el cumplimiento a la normatividad en la materia.

PREVENTIVA:

En lo sucesivo, la Gerencia de Tecnologías de la Información deberá reforzar los mecanismos de control y supervisión, que garanticen en forma razonable el cumplimiento oportuno de las disposiciones normativas en materia de Tecnologías de la Información y Seguridad de la Información.

FECHA COMPROMISO

ÁREAS RESPONSABLES:

[Signature]
C.P. Enrique Herrera Carpio.
Subdirector General de Administración y Finanzas.

[Signature]
Lic. Enixe Axtle Suárez
Gerente de Recursos Materiales y Servicios Generales, responsable de los asuntos de la Dirección de Administración

ELABORÓ: BOL
SUPERVISÓ: FLR
INICIO: 18/12/2015
TERMINÓ: 12/12/2015

I.C.E. Ernesto Telésforo Curiel Zárate
Gerente de Tecnologías de la Información.

TITULAR DEL ÁREA DE AUDITORÍA INTERNA

JEFE DE DEPARTAMENTO

LIC. BERENICE ORDAZ LARES

C.P. FELIPE LIMA RODRÍGUEZ

000257

2-4
9

SFP

SECRETARÍA DE LA FUNCIÓN PÚBLICA



ÓRGANO INTERNO DE CONTROL EN TELEVISIÓN METROPOLITANA, S.A. DE C.V.

CÉDULA DE OBSERVACIONES



CONACULTA

ENTE: TELEVISIÓN METROPOLITANA, S.A. DE C.V.

ÁREA AUDITADA: SUBDIRECCIÓN GENERAL DE ADMINISTRACIÓN Y FINANZAS.

CLAVE DE PROGRAMA Y DESCRIPCIÓN DE LA AUDITORÍA: 4.0.0. "SISTEMA DE INFORMACIÓN Y REGISTRO"

SECTOR: EDUCACIÓN

CLAVE DE LA ENTIDAD: 11425

HOJA No. 2 de 2
NÚMERO DE AUDITORIA: 06/2015
NÚMERO DE OBSERVACIÓN: 1
MONTO FISCALIZABLE:
MONTO FISCALIZADO:
MONTO POR ACLARAR: N/A
MONTO POR RECUPERAR: N/A
RIESGO:

OBSERVACIONES

RECOMENDACIONES

FECHA COMPROMISO

Al respecto, en los anexos de la presente observación se detallan los aspectos, formatos y actividades que la Gerencia de Tecnologías de la Información no ha llevado a cabo.

Es importante comentar que los 3 procesos restante, que no se revisaron por parte de este Órgano Interno de Control, tampoco estas concluidos y la Gerencia citada señala que tienen entre un 80 y 85% de avance.

FUNDAMENTO LEGAL:

Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como establecer el Manual Administrativo de Aplicación General en dichas materias, Artículo transitorio número 10, último párrafo; y su Anexo Único siguiente:

"Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, apartados: I.A. Proceso de Planeación Estratégica", II. C. Proceso de Administración de la Seguridad de la Información y III.D. Proceso de Operación de los controles de seguridad de la Información y del ERISC.

Fecha: 16/12/15

Fecha compromiso: 23/02/16

ELABORÓ: BOL
SUPERVISÓ: FLR
INICIO: 18/12/2015
TÉRMINO: 18/12/2015

JEFE DE DEPARTAMENTO

LIC. BERENICE ORDAZ LARES

TITULAR DEL ÁREA DE AUDITORÍA INTERNA

C.P. FELIPE LIMA RODRÍGUEZ

000258

L-3-1
1-3

L-4
10

OBJETIVOS ESPECÍFICOS		ACTIVIDADES DEL PROCESO		FACTORES CRÍTICOS		CUMPLIMIENTO	COMENTARIOS
1.- Establecer, operar y mantener un modelo de gobierno de seguridad de la información.		Establecer un modelo de gobierno de seguridad de la información.	Designar al responsable de la seguridad de la información en la institución, quien deberá tener nivel jerárquico mínimo de director general o equivalente, atendiendo las reglas de este proceso.	Factor crítico	✓	✓	Se proporcionó evidencia que respalda los factores críticos del proceso, así como también el Documento de Integración y Operación del Grupo Estratégico de Seguridad de la Información. Formato ASI F1
			Establecer el grupo estratégico de seguridad de la información (GESI), que estará integrado por servidores públicos que conozcan los procesos institucionales y que cuenten con conocimientos en materia de seguridad de la información, mediante el documento de integración y operación del grupo estratégico de seguridad de la información, y asegures de: a) Que el documento contenga, al menos: los objetivos y responsabilidades del grupo de trabajo; miembros del grupo; roles y responsabilidades de cada miembro, así como el funcionamiento del grupo. b) Que se comuniquen los roles y responsabilidades de los integrantes del grupo estratégico de seguridad de la información. c) Dirigir y coordinar al grupo estratégico de seguridad de la información y dar seguimiento a las acciones establecidas por el mismo.	Factor crítico	✓	✓	
			Coordinar la elaboración y actualización del catálogo de infraestructuras críticas de la institución.	Factor crítico	✓	✓	
			Establecer, conjuntamente con los responsables de los procesos de la UTIC, así como en su caso con los servidores públicos que correspondan, los mecanismos para garantizar la protección de las infraestructuras críticas que estos tengan bajo su responsabilidad.	Factor crítico	✓	✓	
			Operar y mantener el modelo de gobierno de seguridad de la información	Factor crítico	✓	✓	
			Vigilar que los controles de seguridad de la información que se definen e implementan, consideren los mecanismos establecidos en el factor crítico anterior, así como el análisis de riesgos que se indica en la actividad ASI 5.	Factor crítico	✓	✓	
			Constatar que se efectúe la implementación del SSSI en la institución y que se lleven a cabo revisiones al mismo en periodos no mayores a un año, a fin de verificar su cumplimiento.	Factor crítico	✗	✗	No se proporcionó evidencia de la evaluación realizada en 2015 del SSSI, ni de la implementación de acciones de mejora.
			Dar seguimiento a las acciones de mejora continua derivadas de las revisiones al SSSI.	Factor crítico	✗	✗	
			Disenar, en coordinación con las diferentes áreas y unidades administrativas de la institución, la estrategia de seguridad de la información que será implementada al interior de la misma, así como efectuar su revisión al menos una vez al año. Dicha estrategia será la base para establecer el SSSI, cuyo diseño se efectuará atendiendo a lo siguiente: a) Realizar un diagnóstico de los requerimientos de seguridad de la información de la institución, considerando la participación de las unidades administrativas usuarias de la información para establecer adecuadamente el alcance del SSSI. b) Definir el alcance del SSSI, de manera tal que establezca límites de protección desde la perspectiva institucional, para proporcionar la seguridad requerida a los activos de información. c) Generar las estrategias específicas de seguridad de la información, que permitan cumplir con la misión, visión y objetivos de la institución. d) Desarrollar reglas técnicas para verificar que los controles de seguridad de la información que se definen operen según lo esperado. e) Definir métricas para evaluar el grado de cumplimiento de los requerimientos de seguridad identificados para los activos de información. f) Elaborar las reglas técnicas que contemplen las acciones para la adecuada operación del SSSI.	Factor crítico	✗	✗	
			Integrar, con la información del factor crítico anterior, el documento de definición del SSSI e incluir en este el programa de implementación del SSSI que se desarrolló.	Factor crítico	✓	✓	En el reporte realizado en el Sistema de Gestión de la Política, mencionan estos ocho factores se encuentran en revisión para la autorización del grupo de seguridad de la información; asimismo, proporcionó evidencia de 2 de los 8 factores críticos que integran esta actividad del proceso, se proporcionó un documento del Diseño del SSSI. No se proporcionó evidencia de la evaluación realizada en 2015 del SSSI, ni de la implementación de acciones de mejora.
Realizar el conocimiento del titular de la institución el documento de definición del SSSI, que ya incluya el programa de implementación desarrollado.	Factor crítico	✗	✗				
Asegurarse de que se presente a la unidad administrativa responsable de la capacitación en la institución, una propuesta para que se integren al programa de capacitación institucional, los cursos necesarios para difundir los conceptos e importancia de la seguridad de la información, así como la estructura y alcances del SSSI.	Factor crítico	✗	✗				
Dar a conocer el SSSI, y su programa de implementación, a los servidores públicos de la institución involucrados con el mismo.	Factor crítico	✗	✗				
Elaborar un programa de evaluaciones del SSSI, integrado al documento de definición del SSSI y difundirlo en la institución.	Factor crítico	✗	✗				
Elaborar, probar y mantener actualizada una directriz rectora de respuesta a incidentes, en coordinación con el ERISC, la cual deberá contener al menos: a) El rol y el servidor público asignado a este, quien puede iniciar las tareas de respuesta a incidentes. b) El mecanismo de notificación, escalamiento y atención de incidentes en la institución. c) Los mecanismos de interacción con otras instituciones u organizaciones externas. d) Los criterios técnicos de obtención de indicios, preservación de evidencias, e investigación de incidentes, considerando lo establecido en las disposiciones jurídicas aplicables.	Factor crítico	✗	✗				
Hacer del conocimiento del órgano interno de control en la institución y/o, cuando correspondiera, de las autoridades que resulten competentes, el incumplimiento al SSSI a efecto de que se determinen, en su caso, las responsabilidades que procedan en términos de los documentos legales aplicables.	Factor crítico	✗	✗				

ELABORÓ: AAT/MAEL
 SUPERVISÓ: BOL
 INICIO: 08/10/2015
 TÉRMINO: 22/10/2015

000259
 11
 2-4

6-9
 9-10

Objetivos Específicos	Actividades del Proceso	Factores Críticos	Cumplimiento	Comentarios
3.- Establecer los mecanismos de administración de riesgos que permitan identificar, analizar, evaluar, atender y monitorear los riesgos.	Elaborar el análisis de riesgos.	<p>Establecer la directriz de administración de riesgos, efectuando las siguientes acciones: a) La definición de estrategias, metodologías y herramientas que se usaran para administrar los riesgos. b) La integración del marco normativo que resulte aplicable a los riesgos identificados. c) El establecimiento de las reglas para medir la efectividad de los controles en la gestión de los riesgos. d) La definición de la forma y periodicidad con las que se informará a los grupos de trabajo, a las áreas y unidades administrativas de la institución y externos involucrados, sobre los riesgos a los que se encuentran expuestos los procesos y servicios que utilizan. e) La definición de consideraciones sobre riesgos de TIC y seguridad a la información que coadyuven en la toma de decisiones estratégicas de la institución. f) Someter a consideración y aprobación del RSI, las definiciones efectuadas en los incisos anteriores.</p>	✓	
		<p>Integrar el equipo de trabajo de análisis de riesgos y asegurar, al menos, lo siguiente: a) La definición de los objetivos y responsabilidades del equipo, roles y responsabilidades de cada miembro, y el funcionamiento del mismo (tipos de sesiones, levantamiento de minutos y seguimiento de acciones y acuerdos). b) La conformación del equipo se hará con servidores públicos que, preferentemente, deberán tener conocimientos en TIC, seguridad de la información y seguridad física; así como por aquellos que se considere puedan aportar mayor capacidad de análisis y alcance de objetivos. c) Que los integrantes del equipo cuenten con al menos un año de experiencia y conocimientos en el área en la cual se desempeñan. d) Se delimita el objetivo y alcance del análisis de riesgos que se efectuará por el equipo de trabajo. e) Se selecciona al líder del equipo y se haga de su conocimiento que su rol será el de interpretar y difundir instrucciones, coordinar tareas y materializar resultados. f) Integrar, en caso de ser necesario, más de un equipo de trabajo de análisis de riesgos, para efectuar el adecuado acople de información e integración que deriva del análisis de riesgos que se efectúa en esta actividad.</p>	✓	
		<p>Identificar los procesos críticos, recopilando la información siguiente: a) La de aquellos procesos de los que la institución dependa para alcanzar sus objetivos y niveles de servicio comprometidos, derivada de la identificación realizada conforme al factor crítico 2 de la actividad ASI 4, en los casos en que la institución no hubiera identificado procesos críticos vinculados con la Seguridad Nacional. b) La obtenida como resultado del desarrollo de la actividad ASI 4, por haberse identificado procesos críticos vinculados con la Seguridad Nacional.</p>	✓	
		<p>Identificar los activos de información y consultar a los responsables de estos, para identificar los elementos que se pretenden proteger ante la posible materialización de amenazas y elaborar una relación detallada con la información obtenida.</p>	✓	
		<p>Identificar las vulnerabilidades, mediante las acciones siguientes: a) Integrar, a la relación de activos de información, las características de los mismos que pudieran ser aprovechadas para poner en riesgo la confiabilidad, integridad y disponibilidad de estos, considerando, asimismo, las características del ambiente y de la institución en que se ubican. b) Considerar como vulnerabilidad la ausencia y/o falta de controles. c) Integrar a los responsables de la administración, operación y, en su caso, resguardo de los activos de información en el proceso de identificación de vulnerabilidades.</p>	✓	
		<p>Identificar las amenazas mediante las acciones siguientes: a) Registrar las posibles amenazas que, en caso de materializarse, tendrían efectos negativos sobre la seguridad en uno o varios de los activos de información que ya se tiene enlistados b) Identificar y registrar los agentes que podrían materializar una amenaza, utilizando la lista de amenazas y agentes que se provee en el formato del producto "Documento de resultados del análisis de riesgos".</p>	✓	<p>Se proporciona evidencia de que la elaboración del análisis de riesgos, así como también de que se identificó mediante el Documento Directriz Rectora para la Administración de Riesgos, el análisis de procesos críticos y activos de información. Sin embargo, no presentan evidencia del "Documento de resultados del análisis de riesgos", Formato ASI F3, en el cual deben de reportar en el sistema de Gestión de la Política, los resultados obtenidos del análisis de riesgos efectuado, amenazas, situación de la Directriz Rectora de Administración de Riesgos, análisis del costo-beneficio de controles de seguridad, etc.</p>
		<p>Efectuar la identificación y evaluación de escenarios de riesgo, evaluando aquellos que se identifiquen y registrando los resultados obtenidos, considerando los datos recopilados en los factores críticos anteriores y efectuando las acciones siguientes: a) Definir los escenarios de riesgo, para lo cual es necesario efectuar los cálculos para establecer el valor del riesgo para cada escenario, utilizando la fórmula: R=P, en la que "P" es la probabilidad de ocurrencia de la amenaza, e "T" es el impacto ocasionado por la materialización de la misma. b) Establecer las variables complementarias que se indican en el formato del producto "Documento de resultados del análisis de riesgos", ya que éstas determinan el valor final del riesgo, utilizando la tabla denominada "Probabilidad de ocurrencia contra impacto", que se encuentra en el formato de este mismo producto. c) Integrar en este resultado de la identificación y evaluación de los escenarios de riesgo. c) Definir la estrategia de seguridad para cada riesgo, seleccionando alguna de las establecidas en el citado formato, evitar, mitigar o reducir, financiar o asumir y transferir o compensar, debiendo evaluarse en este mismo orden. d) Obtener la relación de riesgos que requieren atención, su prioridad y estrategia de seguridad.</p>	✓	
		<p>Elaborar el análisis del costo-beneficio de controles de seguridad, mediante las acciones siguientes: a) Elaborar la lista de escenarios de riesgo, cuya acción de seguridad implica el uso de controles o la modificación de un proceso para evitar, mitigar o reducir, financiar o asumir y transferir los riesgos. b) Comparar el costo del control que se propone contra el impacto que se podría ocasionar por la materialización del riesgo. c) Verificar el costo-beneficio de controles de seguridad, debiendo definir los valores indicados en este, para cada escenario de riesgo, e integrar los datos en el "Documento de resultados del análisis de riesgos".</p>	✗	
		<p>Elaborar el "Documento de resultados del análisis de riesgos", mediante las acciones siguientes: a) Integrar la lista de controles recomendados, para un adecuado tratamiento de los riesgos detectados en el orden de prioridad establecido, indicando además los requerimientos para su implementación. b) Incluir, de ser el caso, el nivel de riesgo residual de cada escenario. c) Elaborar e integrar las declaraciones de aplicabilidad con los controles necesarios, de acuerdo a los resultados obtenidos de los factores críticos anteriores. d) Elaborar e incluir las propuestas para los programas de mitigación de riesgos, considerando los controles establecidos en las declaraciones de aplicabilidad. e) Elaborar e incluir en el "Documento de resultados del análisis de riesgos", un programa de contingencia a los riesgos, considerando, de ser el caso, la intervención del ERSC.</p>	✗	
		<p>Obtener del grupo estratégico de seguridad de la información, la aprobación del "Documento de resultados del análisis de riesgos" y enviarlo a los responsables de los procesos en las diversas áreas y unidades administrativas de la institución para su revisión.</p>	✗	
		<p>Seleccionar de entre los controles recomendados por el grupo estratégico de seguridad de la información, contenidos en el "Documento de resultados del análisis de riesgos", aquellos a implementar de acuerdo a las capacidades y recursos de las áreas y unidades administrativas involucradas.</p>	✗	
		<p>Justificar ante el grupo estratégico de seguridad de la información las razones por las cuales existan controles recomendados no seleccionados.</p>	✗	
		<p>Elaborar e integrar en el "Documento de resultados del análisis de riesgos", el programa de implementación para el manejo de riesgos, de acuerdo a los resultados de la selección efectuada conforme al factor crítico 11 de esta actividad. Dicho programa deberá incluir la asignación de responsables de la implementación de cada control, integrando estas al "Documento de resultados del análisis de riesgos" y los datos necesarios para su implementación, así como documentarlas conjuntamente con la implementación de las acciones y controles del SGSI.</p>	✗	
		<p>En el programa de implementación para el manejo de riesgos se deberá establecer un responsable de la implementación de cada uno de los riesgos a manejar.</p>	✗	
		<p>Obtener del grupo estratégico de seguridad de la información la aprobación del programa de implementación elaborado y verificar su adecuada integración con las demás actividades de implementación o mejora de los controles de seguridad y las acciones del SGSI.</p>	✗	
		<p>Cuidar que el análisis de riesgos se realice o actualice conforme a los factores críticos de esta actividad, al menos una vez al año, o bien, en caso de un cambio en los procesos, activos de información o cuando se detecte una nueva amenaza o vulnerabilidad a la seguridad de la información y/o los activos de TIC que la soportan.</p>	✗	
		<p>Asegurar que se ejecuten los factores críticos integralmente y se obtengan los productos de esta actividad debidamente actualizados. Asimismo, se documente la mejora continua que resulte necesaria, derivada del factor crítico anterior.</p>	✗	

2-4
9-10

000262

Objetivos Específicos	Actividades del Proceso	Factores Críticos	Cumplimiento	Comentarios
4. Establecer un SCS que proteja los activos de información de la institución con la finalidad de preservar su confidencialidad, integridad y disponibilidad.	Mejorar el SCS (los controles mínimos de seguridad de la información).	Definir los controles de seguridad necesarios para salvaguardar a los activos de TIC, los activos de información y las infraestructuras críticas de la institución, siendo como mínimo los necesarios para: a) La definición, en términos de seguridad, de la visibilidad del software que se ejecuta en los equipos de cómputo, dispositivos electrónicos o sistemas de información de personal en las áreas relacionadas con el manejo, administración y gestión de los activos de información de la institución, con apego a las disposiciones jurídicas aplicables y considerando los procedimientos que, en su caso, se tengan implementados en el área o unidad administrativa de que se trate. b) La instalación y configuración del software, así como para la administración de la seguridad de los servicios de TIC que se utilicen en la institución. c) El ingreso y salida de activos de información. d) El control seguro de dispositivos de almacenamiento que por algún motivo necesiten ser reparados, reemplazados o asignados a otro usuario y mantener evidencia auditable del proceso. e) El backup, copia y restauración de los datos de información. f) El control de acceso a la información. g) La configuración de los dispositivos de acceso a la información. h) El control de acceso a la información de los proveedores de servicios u otros usuarios, al inicio o término de su empleo, cargo o comisión, relación contractual o de cualquier otro naturaleza, o bien, cuando por algún motivo el nivel de privilegios de acceso asignado cambie. i) Los niveles de asignación de usuarios y contraseñas permitidas para los diversos componentes de los diversos tecnológicos. j) La configuración de los mecanismos de protección implementados en las redes institucionales. Las conexiones a redes públicas y privadas, así como para los dispositivos electrónicos que contengan información considerada como reservada o sensible para la institución. k) La seguridad física y lógica que permita mantener, para los recursos de información, su confidencialidad, integridad y disponibilidad. l) El uso del servicio de Internet en la institución, el cual debe contar con herramientas de seguridad y de filtrado de contenido. m) El intercambio seguro de la información, ya sea de manera interna o hacia el exterior. n) Que la información clasificada o aquella que tiene valor para la institución, sea respaldada y restaurada en el momento en que se requiera. o) Contar con registros de auditoría y bitácoras de seguridad en los sistemas identificados como críticos, así como con las condiciones de seguridad que impidan borrar o alterar dichos registros.	✓	Se proporción evidencia de que el área trabaja en la implementación del SCS, así como también de que se elaboró el análisis de infraestructuras críticas y activos clave. Sin embargo, no presentan evidencia del Documento de definición del SCS, Formato ASI-F4, en el cual deben de reportar en el Sistema de Gestión de la Política, los avances de la implementación, acciones preventivas, correctivas y de mejora del SCS.
5. Establecer mecanismos para la respuesta inmediata e integrales a la seguridad de la información.		Documentar los procesos determinantes conforme al factor crítico anterior, incluyendo su definición detallada e integrarlos al documento de definición del SCS y alinear conjuntamente con los responsables de los procesos institucionales involucrados, el programa de implementación del SCS e integrarlo al mismo documento. El programa de implementación deberá incluir el nombre del responsable de la implementación de cada uno de los controles de seguridad del SCS que se hayan establecido.	X	
6. Vigilar los mecanismos establecidos y el desempeño del SCS, a fin de prevenir desviaciones y mantener una mejora continua.	Mejorar el SCS.	Constar, en coordinación con las áreas y unidades administrativas involucradas, que las actualizaciones de seguridad en todos los componentes de la infraestructura tecnológica de la institución se apliquen, a fin de hacer del conocimiento al titular de la misma el cumplimiento de los controles de seguridad establecidos.	X	No se proporcionó evidencia de la evaluación realizada en 2015 del SCS, ni de la implementación de acciones de mejora.
		Obligado, de la evaluación del SCS, los datos sobre su desempeño, a fin de diseñar y documentar las acciones correctivas y preventivas al documento de definición del SCS.	X	
		Elaborar el documento de implementación de la mejora al SCS e integrarlo al documento de definición del SCS. El documento de implementación deberá utilizarse para la planeación y el seguimiento de las acciones de mejora, ya sean preventivas o correctivas.	X	
		Comunicar las mejoras que deberán aplicarse al SCS al responsable del grupo de trabajo para la implementación de la seguridad de la información, previsto en la actividad D-SEC-1, por medio del documento de definición del SCS.	X	
		Validar y registrar las observaciones respecto a la implementación de las mejoras mediante un sistema de seguimiento a los procesos de seguimiento a los documentos de definición del SCS.	X	

TOTAL DE FACTORES CRÍTICOS = 54 (100%)
 FACTORES CRÍTICOS CUMPLIDOS = 29 (54%)
 FACTORES CRÍTICOS NO CUMPLIDOS = 25 (46%)

6-9
 9-16

PROCESO DE OPERACIÓN DE LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN Y DEL ERISC (OPEC).

Objetivos Específicos	Actividades del Proceso	Factores Críticos	Cumplimiento	Comentarios
	Designar un responsable de la supervisión de la implementación de los controles de la seguridad definidos en el SGSI y en el análisis de riesgos.	Asignar a un servidor público que será responsable de supervisar que los responsables de implementar controles de seguridad del SGSI y controles para el manejo de riesgos, lleven a cabo su labor en tiempo y forma, con apego a la definición del control de seguridad correspondiente. Comunicar la asignación a todos los involucrados	✓	No se proporcionó el Documento de Resultados del análisis de riesgos
		Mantener actualizada la información del Documento de resultados del análisis de riesgos y el programa de implementación del SGSI, incluyendo su avance.	X	
		Establecer las reglas de operación del ERISC, en las que se prevén los mecanismos de coordinación del ERISC al interior de la institución o con otros ERISC u organizaciones externas, en concordancia con la directriz rectora de respuesta a incidentes, incluyendo al menos, los relativos a: a) Los canales de comunicación, que deberán ser seguros. b) Los relativos a la disseminación de datos de los incidentes.	X	El área auditada, menciona que trabajó en los factores críticos que integran esta actividad del proceso, sin embargo no proporciono evidencia que sustente dicho trabajo. No se proporciono la Directriz Rectora de Respuesta a Incidentes
1.- Implementar y operar los controles de seguridad de la información.	Establecer los elementos de información.	Elaborar, de acuerdo a lo establecido en la directriz rectora de respuesta a incidentes, la guía técnica de atención a incidentes, de acuerdo a la criticidad de los activos de TIC afectados, considerando en su elaboración al menos los siguientes apartados: a) Detección y registro de los incidentes. b) Priorización de los incidentes. c) Investigación técnica de los incidentes. d) Criterios técnicos de contención de los incidentes, de acuerdo a la criticidad de los activos de TIC. e) Obtención, preservación y destino de los indicios de los incidentes. f) Erradicación de los incidentes. g) Recuperación de la operación. h) Documentación de las lecciones aprendidas	X	
		Establecer el mecanismo de registro de los incidentes de seguridad de la información, que incluya un repositorio para contener los datos de éstos y crear una base de conocimiento.	X	
		Reportar al responsable de la seguridad de la información, los incidentes de seguridad de la información que se presenten.	X	
		Definir las acciones de atención a los incidentes con apoyo de la guía técnica de atención de incidentes, respecto del incidente que se haya presentado.	X	El área auditada, menciona que trabajó en los factores críticos que integran esta actividad del proceso, sin embargo no proporciono evidencia que sustente dicho trabajo
	Operación del ERISC en la atención de incidentes.	Asegurarse que los responsables de la implementación de los controles de seguridad de la información y de manejo de riesgos, ejecuten las acciones siguientes: a) Apliquen la solución necesaria. b) Registren los datos del incidente y su solución. c) Comuniquen el incidente y su solución al grupo estratégico de seguridad de la información y a los responsables de los dominios tecnológicos involucrados, así como a los usuarios afectados.	X	
		Integre los datos del incidente y su solución a los repositorios con los que cuente la UTIC y en su caso, a los repositorios de la institución que determine el grupo estratégico de seguridad de la información.	X	
		Ejecutar los programas de implementación para el manejo de riesgos y de implementación del SGSI, de acuerdo a lo que se establece en el documento de definición del SGSI, y con apoyo de los titulares de las unidades administrativas en las cuales se implementarán los controles	X	
		Dar seguimiento a la ejecución del programa de implementación del SGSI y actualizar el avance del mismo.	X	
		Elaborar un informe de resultados de la implementación del SGSI e integrarlo al documento de definición del SGSI.	X	
2.- Definir y aplicar la planeación para la mitigación de riesgos por incidentes.		Asegurar que los controles de seguridad se hayan implementado de acuerdo a lo previsto en el documento de definición del SGSI y su programa de implementación del SGSI.	X	No se proporcionó evidencia de la evaluación realizada en 2015 del SGSI, ni de la implementación de acciones de mejora.
		Elaborar los informes correspondientes a las desviaciones en la implementación y/o en la operación de los controles de seguridad.	X	
		Integrar los resultados de los factores críticos 3, 4 y 5 autorrevisores e incorporarlos, para efectos de su actualización, en el documento de definición del SGSI y enviarlos al grupo estratégico de seguridad de la información.	X	

ELABORÓ: AAT/MAEL
 SUPERVISÓ: BOL
 FECHA: 08/10/2015
 22/10/2015
 000263
 HOJA 1 DE 3

6-4
 2-10

Objetivos Específicos	Actividades del Proceso	Factores Críticos	Cumplimiento	Comentarios
3.- Implementar las mejoras recibidas del Proceso de Administración de la Seguridad de la Información (ASGI), para el fortalecimiento del SGSI, tanto de sus guías técnicas como de los controles de seguridad de la información en operación.	Aplicar al SGSI las mejoras que define el grupo estratégico de seguridad de la información.	<p>Aplicar las acciones correctivas y preventivas a los controles de seguridad de la información, indicados por el grupo estratégico de seguridad de la información.</p> <p>Documentar el resultado de la aplicación de la mejora, para cada uno de los controles de seguridad de la información que resultaron impactados, incluyendo las mejoras del SGSI aplicadas.</p> <p>Actualizar el informe de seguimiento a las acciones de mejora al SGSI e integrarlo en el documento de definición del SGSI.</p> <p>Verificar el contenido del informe de seguimiento a las acciones de mejora al SGSI; actualizar el programa de evaluaciones del SGSI; integrarlo en el documento de definición del SGSI y enviar éste al grupo estratégico de seguridad de la información para su revisión.</p>	<p>X</p> <p>X</p> <p>X</p> <p>X</p>	<p>No se proporcionó evidencia de la evaluación realizada en 2015 del SGSI, ni de la implementación de acciones de mejora.</p>

TOTAL DE FACTORES CRÍTICOS = 40 (100%)

FACTORES CRÍTICOS CUMPLIDOS = 17 (42.5 %)

FACTORES CRÍTICOS NO CUMPLIDOS = 23 (57.5 %)

2-4
9-10

ELABORÓ: AAT/MAEL
SUPERVISÓ: BOL
INICIO: 08/10/2015
TÉRMINO: 22/10/2015

000265

HOJA 3 DE 3

<p>ENTE: TELEVISIÓN METROPOLITANA, S.A. DE C.V. ÁREA AUDITADA: SUBDIRECCIÓN GENERAL DE ADMINISTRACIÓN Y FINANZAS. CLAVE DE PROGRAMA Y DESCRIPCIÓN DE LA AUDITORÍA: 4.0.0. "SISTEMA DE INFORMACIÓN Y REGISTRO"</p>	<p>SECTOR: EDUCACIÓN CLAVE DE LA ENTIDAD: 11425</p>	<p>HOJA No. 1 de 2 NÚMERO DE AUDITORÍA: 06/2015 NÚMERO DE OBSERVACIÓN: 2 MONTO FISCALIZABLE: MONTO FISCALIZADO: MONTO POR ACLARAR: N/A MONTO POR RECUPERAR: N/A RIESGO:</p>
<p>OBSERVACIONES</p> <p>DEBILIDADES EN EL PROCESO DE PLANEACIÓN ESTRATÉGICA EN MATERIA DE TECNOLOGÍAS DE LA INFORMACIÓN</p> <p>1.- Como resultado de la revisión a la implementación y cumplimiento del proceso de Planeación Estratégica efectuado en el año 2014, se determinó lo siguiente:</p> <p>a).- La Gerencia de Tecnologías de la Información no presentó al Grupo de Trabajo integrado para la dirección de TIC, el Plan Estratégico de Tecnologías de la Información y Comunicaciones (PETIC) del año 2015 para su autorización.</p> <p>b).- No existe evidencia de que se haya gestionado y obtenido la aprobación de la Coordinadora de Sector de dicho Plan.</p> <p>c).- La difusión del PETIC a todos los involucrados del área y de la Institución, no se llevó a cabo.</p> <p>d).- Desde el tercer trimestre de 2014 a la fecha de la Auditoría, el citado Grupo de Trabajo, no ha sesionado, por lo tanto, no se ha informado de los avances trimestrales del PETIC..</p> <p>e).- No se tienen establecidos controles para identificar las posibles desviaciones en los avances del PETIC.</p> <p>2.- Respecto de las bases de datos que opera la Institución, se advirtió que no se encuentran formalizados los controles para la salvaguarda de la propiedad intelectual, portabilidad, recuperación de datos así como el borrado seguro, situaciones que se deben observar conforme a lo establecido en el artículo 16, fracción III del Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y en Seguridad de la Información.</p>	<p>RECOMENDACIONES</p> <p>CORRECTIVA</p> <p>El Subdirector General de Administración y Finanzas gire instrucciones a la Gerencia Tecnologías de la Información, a fin de que elabore un informe por escrito, debidamente fundado, motivado y soportado, sobre las circunstancias y consideraciones que originaron las situaciones motivo de la observación y sea proporcionando a este Órgano Interno de Control para su análisis y evaluación correspondiente.</p> <p>PREVENTIVA</p> <p>El Subdirector General de Administración y Finanzas gire instrucciones a la Gerencia Tecnologías de la Información, a fin de que establezca los mecanismos de control y supervisión para que en lo sucesivo se dé cumplimiento a la normatividad en materia de Tecnologías de la Información, respecto de los puntos siguientes:</p> <p>a).- Se presente al Grupo de Trabajo integrado para la dirección de TIC, el Plan Estratégico de Tecnologías de la Información y Comunicaciones (PETIC) para su autorización.</p> <p>b).- Se gestione y obtenga de la Coordinadora de Sector, la aprobación del Plan antes citado.</p> <p>c).- Se difunda el PETIC a todos los involucrados del área y de la Institución.</p>	<p>FECHA COMPROMISO</p> <p>ÁREAS RESPONSABLES:</p> <p><i>[Handwritten signature]</i></p> <p>C.P. Enrique Herrera Carpio. Subdirector General de Administración y Finanzas.</p> <p><i>[Handwritten signature]</i></p> <p>Lic. Enixe Axtle Suárez Gerente de Recursos Materiales y Servicios Generales, responsable de los asuntos de la Dirección de Administración</p>
<p>JEFE DE DEPARTAMENTO</p> <p><i>[Handwritten signature]</i></p> <p>LIC. BERENICE ORDAZ LARES</p>	<p>TITULAR DEL ÁREA DE AUDITORÍA INTERNA</p> <p><i>[Handwritten signature]</i></p> <p>C.P. FELIPE LIMA RODRÍGUEZ</p>	<p>ELABORÓ: BOL SUPERVISÓ: FLR INICIO: 18/12/2015 TÉRMINO: 18/12/2015</p> <p>I.C.E. Ernesto Telesforo Curiel Zárate Gerente de Tecnologías de la Información.</p> <p>000266</p> <p>2-4 18</p>

2-4
20-22

2-3-2
1-3



ÓRGANO INTERNO DE CONTROL EN
TELEVISIÓN METROPOLITANA, S.A. DE C.V.
CÉDULA DE OBSERVACIONES



SFP

SECRETARÍA DE
LA FUNCIÓN PÚBLICA

ENTE: TELEVISIÓN METROPOLITANA, S.A. DE C.V.	SECTOR: EDUCACIÓN	HOJA No. 2 de 2
ÁREA AUDITADA: SUBDIRECCIÓN GENERAL DE ADMINISTRACIÓN Y FINANZAS.	CLAVE DE LA ENTIDAD: 11425	NÚMERO DE AUDITORIA: 06/2015
CLAVE DE PROGRAMA Y DESCRIPCIÓN DE LA AUDITORÍA: 4.0.0. "SISTEMA DE INFORMACIÓN Y REGISTRO"		NÚMERO DE OBSERVACION: 2
		MONTO FISCALIZABLE:
		MONTO FISCALIZADO:
		MONTO POR ACLARAR: N/A
		MONTO POR RECUPERAR: N/A
		RIESGO:

OBSERVACIONES	RECOMENDACIONES	FECHA COMPROMISO
<p>FUNDAMENTO LEGAL:</p> <p>Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como establecer el Manual Administrativo de Aplicación General en dichas materias, Artículo 16, fracción III; y su Anexo Único siguiente:</p> <p>"Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, apartados: I.A. Proceso de Planeación Estratégica, actividades PE 1 Establecer la Gobernabilidad de las Operaciones de la UTIC, Actividad PE 3 Validar, aprobar, comunicar y adecuar, de ser necesario el PETIC, PE 4 Dar seguimiento a la planeación estratégica de TIC.</p>	<p>d).- Se reúna periódicamente el referido Grupo de Trabajo, donde se informe de los avances trimestrales del PETIC.</p> <p>e).- Se establezcan los controles para identificar las posibles desviaciones en los avances del PETIC.</p> <p>Así mismo, con relación a las bases de datos que opera la Institución, se formalicen los controles para la salvaguarda de la propiedad intelectual, portabilidad, recuperación de datos así como el borrado seguro.</p>	<p>Fecha: <u>16/12/15</u></p> <p>Fecha compromiso: <u>23/02/16</u></p>

ELABORÓ: BOL
SUPERVISÓ: FLR
INICIO: 18/12/2015
TÉRMINO: 18/12/2015

2-4
19
000267

TITULAR DEL ÁREA DE AUDITORÍA INTERNA

C.P. FELIPE LIMA RODRÍGUEZ

JEFE DE DEPARTAMENTO

LIC. BERENICE ORDAZ LARES

2-3-2
1-3

ÓRGANO INTERNO DE CONTROL EN TELEVISIÓN METROPOLITANA S.A. DE C.V.
 AUDITORÍA: 06/2015 "SISTEMA INTEGRAL DE INFORMACIÓN"

ÁREA AUDITADA: GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN

CONCEPTO: DESARROLLO Y APLICACIÓN DE PLANEACIÓN ESTRATÉGICA (PE) DE ACUERDO AL MAAGTCSI

ANEXO No. 3
 OBSERVACIÓN No. 1

I.- PROCESO DE GOBERNANZA		
I.A. PROCESO DE PLANEACIÓN ESTRATÉGICA		
ACTIVIDADES DEL PROCESO		
FACTOR CRÍTICO	CUMPLIÓ	OBSERVACIONES
Solicitar la intervención del titular de la Institución para establecer el grupo de trabajo para la dirección de TIC, el cual deberá integrarse por mandos superiores con capacidad de toma de decisiones sobre los objetivos, metas y proyectos institucionales de TIC, y formalizarse mediante una acta de integración y forma de operación del grupo de trabajo para la dirección de TIC.	<input checked="" type="checkbox"/>	La UTIC cuenta con el formato de la integración del grupo de trabajo correspondiente a enero del 2014, sin embargo de acuerdo al nuevo manual implementado en mayo del 2014, se requiere del acta de integración de acuerdo a las nuevas disposiciones (la cual se debe de solicitar con la caratula o cesar queda pendiente)
Definir, implementar y mantener una adecuada organización al interior de la UTIC, mediante la asignación de roles y responsabilidades para la gestión de los procesos de ésta, atendiendo a las necesidades de los procesos y proyectos de la UTIC.	<input checked="" type="checkbox"/>	Se cuenta con la designación de roles y responsabilidades para llevar a cabo los procesos y proyectos establecidos dentro de la TIC
Informar al titular de la institución acerca de los resultados, recomendaciones y acuerdos del grupo de trabajo para la dirección de TIC.	<input checked="" type="checkbox"/>	No cuentan con evidencia física referente a los presente rubro, sin embargo, en el desarrollo del manual reportando en la Plataforma de la Gestión Política TIC, el UTIC especifica que si se llevaron a cabo las actividades establecidas en el proceso a fin de dar cumplimiento a las mismas.
Determinar oportunidades en el uso de las TIC.	<input checked="" type="checkbox"/>	No cuentan con evidencia física referente a los presente rubro, sin embargo, en el desarrollo del manual reportando en la Plataforma de la Gestión Política TIC, el UTIC especifica que si se llevaron a cabo las actividades establecidas en el proceso a fin de dar cumplimiento a las mismas.
Determinar las prioridades de las iniciativas de TIC alineadas con las prioridades institucionales, así como de los programas sectoriales y especiales que le competen.	<input checked="" type="checkbox"/>	La UTIC realiza la evaluación del cumplimiento de niveles de servicio, sin embargo, la TIC informa que se esta elaborando la guía de riesgos a de la TIC
Verificar que las principales inversiones en materia de TIC se encuentren alineadas a los objetivos estratégicos de la Institución.	<input checked="" type="checkbox"/>	La autorización de los proyectos se verifican en la plataforma de la Gestión de la Política reportada por la Gerencia de tecnología de la información.
Evaluar el cumplimiento de los niveles de servicio establecidos para los servicios de TIC e identificar los riesgos de las iniciativas de TIC.	<input checked="" type="checkbox"/>	El seguimiento se realiza en base a los reportes realizados en la plataforma de la Gestión de la Política de TIC, cabe mencionar que únicamente se realizaron 2 reportes trimestrales
Autorizar los proyectos estratégicos de la Institución a integrarse en el PETIC	<input checked="" type="checkbox"/>	Respecto a los presentes factores críticos, se determina que se realizaron conforme a procesos, cabe mencionar que es la misma persona encargada de realizar las actividades correspondientes a los procesos.
Mantenerse informado del seguimiento del PETIC, conforme a lo señalado en este proceso.	<input checked="" type="checkbox"/>	Actualmente la TIC no cuenta con los criterios técnicos a fin de gestionar los riesgos, mencionar que actualmente la TIC se encuentra en la elaboración de dicho documento, sin embargo a la fecha de la aplicación del factor presente, no se encuentra aplicada el criterio establecido en el Manual Administrativo de la TIC
Establecer la coordinación necesaria con el responsable de seguridad de la información en la Institución para armonizar el gobierno de TIC, la administración de riesgos y el SGSI.	<input checked="" type="checkbox"/>	
Conocer los criterios técnicos que proponga el responsable de la seguridad de la información en la Institución para gestionar los riesgos.	<input checked="" type="checkbox"/>	

000268

SUPERVISOR DE
 CONTROL INTERNO
 28/09/2015
 09/10/2015
 HOOB

ÓRGANO INTERNO DE CONTROL EN TELEVISIÓN METROPOLITANA S.A. DE C.V.
 AUDITORÍA: 06/2015 "SISTEMA INTEGRAL DE INFORMACIÓN"
 ÁREA AUDITADA: GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN
 CONCEPTO: DESARROLLO Y APLICACIÓN DE PLANEACIÓN ESTRATÉGICA (PE) DE ACUERDO AL MAAGMTICSI

2-4
18-19

I.- PROCESO DE GOBERNANZA		
I.A. PROCESO DE PLANEACIÓN ESTRATÉGICA		
ACTIVIDADES DEL PROCESO		
FACTOR CRÍTICO	CUMPLIÓ	OBSERVACIONES
Integrar los elementos regulatorios y tecnológicos que influyan o puedan influir en la ejecución de las actividades y servicios que provee la UTIC	<input checked="" type="checkbox"/>	Se establece como elementos regulatorios que influyen en el desarrollo y cumplimiento de los objetivos, tales como el MAAGTIC-SI, el acuerdo que tiene por objetivo emitir las políticas y disposiciones para la EDN, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así establecer el Manual Administrativo de Aplicación General en dicha materia y los lineamientos para la aplicación y seguimiento de las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal.
Integrar en el PETIC los objetivos estratégicos, las metas y acciones que permitan cumplir los objetivos estratégicos de TIC, considerando elementos de arquitectura empresarial.	<input checked="" type="checkbox"/>	La información correspondiente a este rubro se encuentra dado de alta en la plataforma de la Gestión de la Política TIC
Establecer en el PETIC, la relación existente entre indicadores, metas y acciones. Considerar la evaluación resultante de los indicadores de los procesos de este manual.	<input checked="" type="checkbox"/>	
Determinar el conjunto total de iniciativas y proyectos de TIC, identificando aquellos que se consideren estratégicos, e integrar cada iniciativa y proyecto de TIC, incluyendo su descripción, alcance, línea base y programa de trabajo.	<input checked="" type="checkbox"/>	
Priorizar las iniciativas y proyectos de TIC, considerando su relevancia para cumplir con los objetivos institucionales y los estratégicos de TIC.	<input checked="" type="checkbox"/>	
Estimar la inversión requerida para las iniciativas y proyectos de TIC, desagregando de ésta al menos los rubros de recursos financieros, materiales y humanos.	<input checked="" type="checkbox"/>	Respecto a los presentes puntos desarrollar dentro del proceso, el área de la TIC, otorga evidencia física de acuerdo al desarrollo e implementación de las actividades realizadas, por lo cual se determina como cumplidas de acuerdo al proceso establecido en el MAAGMTICSI y demás disposiciones establecidas.
Identificar en el PETIC un máximo de 7 iniciativas y/o proyectos de TIC que se consideren estratégicos, aplicando como criterio preferente para su identificación que aporten mayores beneficios a la población o cuenten con alto impacto en el cumplimiento de los objetivos institucionales, del Decreto y la EDN; debiendo asegurar que éstos se integren al portafolio de proyectos de TIC que se establece en el Proceso Administración de Proyectos (ADP)	<input checked="" type="checkbox"/>	
Las iniciativas y proyectos de TIC que se integren en esta actividad deberán categorizarse, de acuerdo a la optimización, la digitalización, la simplificación y la racionalización.	<input checked="" type="checkbox"/>	

ELABORÓ: AAT/MAEL
 SUPERVISÓ: BOL
 INICIO: 28/09/2015
 TÉRMINO: 09/10/2015

000269
 2-4
 21

ÓRGANO INTERNO DE CONTROL EN TELEVISIÓN METROPOLITANA S.A. DE C.V.
 AUDITORIA: 06/2015 "SISTEMA INTEGRAL DE INFORMACIÓN"
 ÁREA AUDITADA: GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN
 CONCEPTO: DESARROLLO Y APLICACIÓN DE PLANEACIÓN ESTRATÉGICA (PE) DE ACUERDO AL MAAGTICS

ANEXO No. 3
OBS. 1

2-4
18-19

I.- PROCESO DE GOBERNANZA		I.A. PROCESO DE PLANEACIÓN ESTRATÉGICA	
ACTIVIDADES DEL PROCESO		CUMPLIÓ	OBSERVACIONES
FACTOR CRÍTICO			
Revisar y validar el PETIC.		PARCIALMENTE	En relación a la revisión realizada a la implementación del PETIC, se determina que si se llevo a cabo la revisión y validación del PETIC debido a que se encuentra dado de alta en la Gestión de la Política TIC, sin embargo la TIC no presenta el documento firmado donde se corrobora la revisión y validación de PETIC.
Presentar el PETIC para la autorización del grupo de trabajo para la dirección de TIC, así como gestionar la aprobación de la Institución coordinadora de sector que le corresponda.		<input checked="" type="checkbox"/>	En la revisión de la implementación del Manual Administrativo de la TIC, se identifica que en la TIC no se realiza la presentación y autorización del PETIC ante el grupo de trabajo, así mismo no se cuenta con la autorización de la Institución Coordinadora del sector correspondiente.
Registrar el PETIC, una vez cumplido el factor crítico anterior, en el sistema informático al que se alude en la regla 7 del presente proceso.		<input checked="" type="checkbox"/>	Se verifica el cumplimiento del registro y autorización del PETIC en el sistema de la Gestión política de TIC de acuerdo a lo establecido en el proceso.
Verificar que se obtenga la autorización del PETIC por parte de la Unidad, utilizando para ello el sistema informático al que se alude en la regla 7 del presente proceso.		<input checked="" type="checkbox"/>	No se cuenta con la confirmación de la difusión del PETIC a las personas involucradas dentro del proceso.
Diffundir el PETIC a todos los involucrados en la UTIC y en la Institución.		<input checked="" type="checkbox"/>	
Dar seguimiento al avance del PETIC y reportarlo trimestralmente a la Unidad, previa aprobación del titular de la UTIC por medio del sistema informático aludido en la regla 7 del presente proceso		<input checked="" type="checkbox"/>	De los reportes establecidos trimestralmente, únicamente dos fueron dados de alta en la plataforma de la Gestión de la Política TIC, correspondiente al ejercicio 2014.
Informar trimestralmente al grupo de trabajo para la dirección de TIC, así como a las instancias que se determinan en el Acuerdo, sobre el cumplimiento del PETIC, así como de la situación de los indicadores en el tablero de seguimiento de la planeación estratégica de TIC y de sus indicadores.		<input checked="" type="checkbox"/>	La TIC informa que si se llevó a cabo el informe al grupo referente al cumplimiento del PETIC, sin embargo, no se cuenta con evidencia física de dicha información.
Identificar, registrar y administrar las acciones correctivas en caso de desviación en el avance real del PETIC, verificando el cumplimiento de sus indicadores.		<input checked="" type="checkbox"/>	La TIC informa que durante el ejercicio del 2014, no existieron desviaciones por lo cual no se realizaron acciones correctivas, sin embargo, de acuerdo a los datos que con los cuales identifican las desviaciones no presentan información o movimientos de datos reales registrados durante el ejercicio 2014.
Verificar que los indicadores de los procesos de este manual se encuentren actualizados de acuerdo a la periodicidad del indicador, efectuar su evaluación y difundir los resultados.		PARCIALMENTE	

SI CUMPLIÓ

NO CUMPLIÓ

Total de reactivos: 28 (100%)
 Reactivos cumplidos: 20 (71.4%)
 Reactivos no cumplidos: 8 (28.6%)

LABORÓ: AAT/MAEL
 SUPERVISO: BOL
 INICIO: 28/09/2015
 TÉRMINO: 09/10/2015

HOJA 3 DE 3

000270

2-4
22



ÓRGANO INTERNO DE CONTROL EN TELEVISIÓN METROPOLITANA, S.A. DE C.V.
CÉDULA DE OBSERVACIONES

SFP
SECRETARÍA DE LA FUNCIÓN PÚBLICA



<p>ENTE: TELEVISIÓN METROPOLITANA, S.A. DE C.V. ÁREA AUDITADA: SUBDIRECCIÓN GENERAL DE ADMINISTRACIÓN Y FINANZAS. CLAVE DE PROGRAMA Y DESCRIPCIÓN DE LA AUDITORÍA: 4.0.0. "SISTEMA DE INFORMACIÓN Y REGISTRO"</p>	<p>SECTOR: EDUCACIÓN CLAVE DE LA ENTIDAD: 11425</p>	<p>HOJA No. 1 de 2 NÚMERO DE AUDITORIA: 06/2015 NÚMERO DE OBSERVACIÓN: 3 MONTO FISCALIZABLE: MONTO FISCALIZADO: MONTO POR ACLARAR: N/A MONTO POR RECUPERAR: N/A RIESGO:</p>
---	---	---

OBSERVACIONES	RECOMENDACIONES	FECHA COMPROMISO
<p><u>GUÍAS INSTIUCIONALES EN MATERIA DE TECNOLOGÍAS DE LA INFORMACIÓN DESACTUALIZADAS.</u></p> <p>Como resultado de la verificación efectuada a las disposiciones en materia de Tecnologías de la Información y Comunicaciones, y en la Seguridad de la Información, existentes en la Normateca Interna de la Entidad, se identificaron en el apartado de documentos vigentes, 27 Guías en la materia que nos ocupa, correspondientes a igual número de procesos que conformaban el anterior Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones, y en la Seguridad de la Información (MAAGTICSI), siendo que el Manual actual publicado en el Diario Oficial el 8 de mayo de 2014, sólo se integra de 9 procesos, por lo que resulta importante actualizar las citadas Guías a fin de que coadyuven a la homologación de los procesos definidos en la normatividad vigente.</p> <p>Asimismo, del análisis efectuado a las referidas Guías, se determinó que varias de ellas integran parcialmente un proceso del MAAGTICSI actualizado, es decir que un proceso se compone de fragmentos de 3 o 4 Guías, situación que resulta impráctica y confusa para los usuarios de dichos documentos. (Anexo 1)</p>	<p>CORRECTIVA:</p> <p>El Subdirector General de Administración y Finanzas gire instrucciones a la Gerencia Tecnologías de la Información, para que a la brevedad realice lo siguiente:</p> <p>Lleve a cabo un análisis de las Guías en materia de Tecnologías de la Información y Comunicaciones, y en la Seguridad de la Información, para que aún y cuando no es obligatoria su emisión, resulta importante contar con documentos actualizados que coadyuven a la implementación y cumplimiento del MAAGTICSI, procediendo a su reingeniería, mejora continua, fusión o baja en su caso, a fin de que las guías sean acordes a los 9 procesos que integran el referido Manual vigente, una vez realizadas las actividades descritas, se gestione su revisión, aprobación y autorización ante las instancias competentes, así como se realice su difusión para su implementación.</p> <p>PREVENTIVA:</p> <p>En lo sucesivo, la Gerencia de Tecnologías de la Información deberá dar seguimiento constante a la normatividad interna que regula la operación del área que dirige, con la finalidad de mantenerla acorde con las actualizaciones que disponen las instancia externas, en materia de Tecnologías de la Información y Comunicaciones, y Seguridad de la Información.</p>	<p>ÁREAS RESPONSABLES:</p> <p><i>[Signature]</i> C.P. Enrique Herrera Carpio. Subdirector General de Administración y Finanzas.</p> <p><i>[Signature]</i> Lic. Enixe Axtle Suárez Gerente de Recursos Materiales y Servicios Generales, responsable de los asuntos de la Dirección de Administración</p>

ELABORÓ: BOL
SUPERVISÓ: FLR
INICIO: 18/12/2015
TÉRMINO: 18/12/2015

I.C.E. Ernesto Telesforo Curiel Zárate
Gerente de Tecnologías de la Información.

TITULAR DEL ÁREA DE AUDITORÍA INTERNA

JEFE DE DEPARTAMENTO

[Signature]
LIC. BERENICE ORDAZ LAÑES

[Signature]
C.P. FELIPE LIMA RODRÍGUEZ

000271

L-4
25-29

L-3-1
1-3

L-4
23

SFP

SECRETARÍA DE LA FUNCIÓN PÚBLICA



ÓRGANO INTERNO DE CONTROL EN TELEVISIÓN METROPOLITANA, S.A. DE C.V. CÉDULA DE OBSERVACIONES



LA CONACULTA

ENTE: TELEVISIÓN METROPOLITANA, S.A. DE C.V.

ÁREA AUDITADA: SUBDIRECCIÓN GENERAL DE ADMINISTRACIÓN Y FINANZAS.

CLAVE DE PROGRAMA Y DESCRIPCIÓN DE LA AUDITORÍA: 4.0.0. "SISTEMA DE INFORMACIÓN Y REGISTRO"

SECTOR: EDUCACIÓN

CLAVE DE LA ENTIDAD: 11425

HOJA No. 2 de 2
NÚMERO DE AUDITORIA: 06/2015
NÚMERO DE OBSERVACIÓN: 3
MONTO FISCALIZABLE:
MONTO FISCALIZADO:
MONTO POR ACLARAR: N/A
MONTO POR RECUPERAR: N/A
RIESGO:

OBSERVACIONES

RECOMENDACIONES

FECHA COMPROMISO

FUNDAMENTO LEGAL:

Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, 9 procesos en materia de TIC y Seguridad de la Información.

-Guías Internas Operativas de la Gerencia de Tecnologías de Información en Televisión Metropolitana, S.A. de C.V. 27 guías en materia de TIC y Seguridad de la Información.

Fecha: 16/12/15

Fecha compromiso: 23/02/16

ELABORÓ: BOL
SUPERVISÓ: FLR
INICIO: 18/12/2015
TÉRMINO: 18/12/2015

007272

JEFE DE DEPARTAMENTO

[Signature]

LIC. BERENICE ORDAZ LARES

TITULAR DEL ÁREA DE AUDITORÍA INTERNA

C.P. FELIPE LIMA RODRIGUEZ

2-4
20-27

23-1
1-3

2-4
24

ÓRGANO INTERNO DE CONTROL EN TELEVISIÓN METROPOLITANA S.A. DE C.V.
AUDITORÍA: 06/2015 "SISTEMA INTEGRAL DE INFORMACIÓN"
ÁREA AUDITADA: GERENCIA DE TECNOLOGÍA DE LA INFORMACIÓN
CONCEPTO: RELACION DE LOS PROCESOS DE ADMINISTRACIÓN DEL MAAGTICSI CON LAS GUÍAS INSTITUCIONALES

PROCESOS ESTABLECIDOS POR EL MAAGTICSI	GUÍAS INSTITUCIONALES	GUÍAS QUE SE RELACIONAN CON LOS 9 PROCESOS DEL MAAGTICSI	MANTIENE RELACIÓN	COMENTARIOS
1.- PROCESO DE PLANEACIÓN ESTRATÉGICA DE TECNOLOGÍAS DE LA INFORMACIÓN	GUÍA DE PLANEACIÓN ESTRATÉGICA DE TECNOLOGÍAS DE LA INFORMACIÓN	Guía del establecimiento del modelo de gobierno de TIC.	<input checked="" type="checkbox"/>	La presente guía se relaciona con el proceso de planeación estratégica debido a que contiene el desarrollo del grupo de trabajo de la UTIC para el cumplimiento de los objetivos Institucionales.
		Guía para la determinación de la dirección tecnológica.	<input checked="" type="checkbox"/>	La presente guía forma parte de la formación del grupo del trabajo tecnológico, así como el alcance, objetivo, roles y las responsabilidades del grupo de trabajo.
		Guía para la operación del sistema de gestión y mejora de los procesos de la unidad de tecnología de la información y comunicación.	<input checked="" type="checkbox"/>	Esta guía se relaciona con el proceso de planeación estratégica debido a que establece los controles para dar seguimiento y cumplimiento a las actividades desarrolladas en el proceso de la planeación estratégica, así como la identificación de las posibles desviaciones, implementación de mejoras y el seguimiento de las mismas.
		Guía de administración de la operación.	<input checked="" type="checkbox"/>	La guía se relaciona con el proceso de planeación estratégica debido a que se lleva un control de las operaciones realizadas para realizar las diferentes actividades a fin de dar cumplimiento a lo establecido en el proceso mencionado.
		Guía de administración de riesgos.	<input checked="" type="checkbox"/>	No se encuentra ninguna guía de administración de riesgos en los procesos institucionales, cabe mencionar que se encuentra en proceso de elaboración.
		Guía de administración del portafolio de proyectos de tecnología de la información y comunicación.	<input checked="" type="checkbox"/>	La presente guía se relaciona con el proceso de planeación estratégica debido a que desarrolla las iniciativas, los programas y los proyectos de la Tecnología de la Información
		Guía de administración de la evaluación de tecnologías de la información y comunicación.	<input checked="" type="checkbox"/>	La guía se relaciona con el presente proceso debido a que establece los indicadores a fin de dar seguimiento y realizar la evaluación de la aplicación de la planeación estratégica, así como los resultados, el avance y el cumplimiento de los objetivos.
		Guía de administración de la evaluación de tecnologías de la información y comunicación.	<input checked="" type="checkbox"/>	La guía se relaciona con el presente proceso debido a que establece los indicadores a fin de dar seguimiento y realizar la evaluación presupuestaria, así como los resultados, el avance y el cumplimiento de los objetivos en base a los presupuestos.
		Guía de planeación estratégica de tecnología de la información y comunicación.	<input checked="" type="checkbox"/>	La presente guía se relaciona con la elaboración y el reporte de los avances en materia del presupuesto otorgada para el desarrollo de los proyectos autorizados para la UTIC.
		Guía de administración de la operación	<input checked="" type="checkbox"/>	La guía de Operaciones se relaciona con el presente proceso debido a que se lleva un control e indicadores, a fin de identificar desviaciones existentes en cuestión presupuestaria.
2.- PROCESO DE ADMINISTRACIÓN DEL PRESUPUESTO Y LAS CONTRATACIONES (APCT)	GUÍA DE ADMINISTRACIÓN DE PRESUPUESTOS DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN	Guía de administración de riesgos.	<input checked="" type="checkbox"/>	No se encuentra ninguna guía de administración de riesgos en los procesos institucionales, cabe mencionar que se encuentra en proceso de elaboración.
		Guía de administración del portafolio de proyectos de tecnología de la información y comunicación.	<input checked="" type="checkbox"/>	La presente guía se relaciona con el proceso de presupuestos debido a que desarrollo los proyectos estratégicos con los cuales se realiza el presupuesto de la UTIC.
		Guía de administración del portafolio de servicios de TIC.	<input checked="" type="checkbox"/>	Mantiene relación con el proceso de Administración de presupuestos debido a que establece los compromisos y costos de los servicios necesarios para mantener el funcionamiento de la institución.
		Guía de administración de dominios tecnológicos.	<input checked="" type="checkbox"/>	La guía se relaciona con los costos que se presentan en la implementación de los dominios tecnológicos implementados por la UTIC a fin de dar cumplimiento a los objetivos Institucionales.
		Guía de mantenimiento de infraestructura.	<input checked="" type="checkbox"/>	La presente guía se relaciona con el proceso de presupuestos debido a que se debe de estimar los costos, los beneficios y vida útil que se le brinde al mantenimiento de la infraestructura.
		Guía de administración del portafolio de servicios de TIC.	<input checked="" type="checkbox"/>	La presente guía se relaciona con el proceso de (ADS) en base a los servicios proporcionados por la UTIC en la cual se establecen los servicios, se realizan actualizaciones a la categoría de servicios, se evalúan las inversiones y riesgos, se definen criterios de evaluación y se reportan los resultados obtenidos a fin de mantener un adecuado funcionamiento de la Institución la cual permita la toma de decisiones estratégicas.
		Guía de diseño de servicios de tecnologías de la información y comunicación.	<input checked="" type="checkbox"/>	La presente guía se relaciona con el proceso de (ADS) con la modificación o diseño de los servicios proporcionados por la TIC, a fin de que se considere aspectos relevantes como el diseño de soluciones, la capacidad de la infraestructura, la disponibilidad y continuidad de servicios proporcionados.
		Guía de operación de la mesa de servicios.	<input checked="" type="checkbox"/>	La Guía de Operación de Servicios de la UTIC se relaciona con el proceso de (ADS) de acuerdo a la atención brindada a los usuarios de los activos y servicios, a fin de atender sus solicitudes y proceder a brindar la atención de las mismas para dar soluciones a sus requerimientos.

ELABORÓ: AAT/MAEL
SUPERVISÓ: BOL
INICIO: 28/09/2015
TÉRMINO: 09/10/2015

2-4
25

000273

ÓRGANO INTERNO DE CONTROL EN TELEVISIÓN METROPOLITANA S.A. DE C.V.
AUDITORÍA: 06/2015 "SISTEMA INTEGRAL DE INFORMACIÓN"
ÁREA AUDITADA: GERENCIA DE TECNOLOGÍA DE LA INFORMACIÓN
CONCEPTO: RELACION DE LOS PROCESOS DE ADMINISTRACIÓN DEL MAAGTICSI CON LAS GUÍAS INSTITUCIONALES

PROCESOS ESTABLECIDOS POR EL MAAGTICSI	GUÍAS INSTITUCIONALES	GUÍAS QUE SE RELACIONAN CON LOS 9 PROCESOS DEL MAAGTICSI	MANTIENE RELACION	COMENTARIOS
5.- PROCESO DE ADMINISTRACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ASI)	GUIA DE ADMINISTRACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Guía para el apoyo técnico para la contratación de soluciones tecnológicas de tecnología de la información y comunicación.	<input checked="" type="checkbox"/>	La presente guía se relaciona con el proceso de (ASI) de acuerdo a los requerimientos de las soluciones tecnológicas, debido a que forma parte de la guía de apoyo en el seguimiento y desarrollo de la información, mediante la implementación de los sistemas de seguridad.
		Guía de desarrollo de soluciones tecnológicas de tecnología de la información y comunicación.	<input checked="" type="checkbox"/>	La presente guía se relaciona con el proceso de (ASI) debido a que de acuerdo a las soluciones tecnológicas establecidas por la TIC se determinan los procesos de seguridad social aplicables a las soluciones tecnológicas.
		Guía de calidad de las soluciones tecnológicas de tecnología de la información y comunicación.	<input checked="" type="checkbox"/>	Las presentes guías se relacionan ya que de acuerdo a la implementación de la información se realizan las revisiones de calidad desarrolladas en la guía, a fin de obtener un buen resultado en los componentes y productos de las soluciones estratégicas.
		Guía de administración de cambio.	<input checked="" type="checkbox"/>	La presente guía se relaciona con el proceso (ASI), en base a los accesos, registros, la evaluación, la ejecución y revisión de los cambios establecidos en los sistemas de la UTIC a fin de mantener una seguridad en la información de la Institución.
		Guía de liberación y entrega.	<input checked="" type="checkbox"/>	La presente guía se relaciona con el proceso de (ASI) en relación a la seguridad implementada en la entrega de los paquetes de liberación como pueden ser un número secuencial a fin de mantener un control e identificación de cada uno de los paquetes liberados.
		Guía de transmisión y habilitación de la operación.	<input checked="" type="checkbox"/>	La guía se relaciona con el presente proceso con el establecimiento de los controles que permitan identificar las soluciones tecnológicas de la institución a fin de confirmar que las transmisiones de la operación y soporte de las soluciones tecnológicas eviten riesgos o fallas en la interrupción de los servicios de la Institución.
		Guía para la determinación de la dirección tecnológica.	<input checked="" type="checkbox"/>	La presente guía se relaciona con el proceso de Administración de proyectos en cuanto a la integración del grupo de trabajo para desarrollar los proyectos autorizados para la UTIC a fin de que mantengan un adecuado control en la selección, el desarrollo, la aplicación y el uso de la infraestructura de la UTIC para cumplir con los objetivos de la institución.
		Guía de planeación estratégica de tecnología de la información y comunicación.	<input checked="" type="checkbox"/>	La presente guía se relaciona con la autorización de los proyectos autorizados para el desarrollo de los mismos dentro de la UTIC a fin de ser aplicados a los procesos sustanciales de la Institución.
		Guía de administración de la operación.	<input checked="" type="checkbox"/>	Se relaciona con el proceso de Administración de proyectos para mantener la estabilidad y la continua operación de la infraestructura a fin de establecer las acciones a seguir para la programación, ejecución y seguimiento de la operación a fin de dar cumplimiento a los proyectos.
		6.- PROCESO DE ADMINISTRACIÓN DE PROYECTOS	GUIA DE ADMINISTRACIÓN DE PROYECTOS DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN	Guía de administración de riesgos.
Guía para la operación del sistema de gestión y mejora de los procesos de la unidad de tecnología de la información y comunicación.	<input checked="" type="checkbox"/>			La presente guía se relaciona con el proceso en cuanto al establecimiento de un sistema de mejora en la aplicación de los proyectos desarrollados por la Institución a fin de monitorear y evaluar los procesos a desarrollar para el cumplimiento de los objetivos institucionales.
Guía de administración del portafolio de proyectos de tecnología de la información y comunicación.	<input checked="" type="checkbox"/>			La presente guía se relaciona con el establecimiento de la visión de los proyectos que generen beneficios para la institución, así como mantener iniciativas y programas a fin de optimizar los recursos institucionales.
Guía de administración de la evaluación de tecnologías de la información y comunicación.	<input checked="" type="checkbox"/>			Las presentes guías se relacionan en base al establecimiento de sistemas que permitan la evaluación de la operación y servicios mediante el establecimiento de acciones de mejora para revertir o corregir desviaciones en el cumplimiento de los proyectos así como de los objetivos.
7.- PROCESO DE ADMINISTRACIÓN DE PROVEEDORES	GUIA DE ADMINISTRACIÓN DE PROVEEDORES DE BIENES Y SERVICIOS DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN	Guía de administración del presupuesto de tecnologías de la información y comunicación.	<input checked="" type="checkbox"/>	La presente Guía mantiene relación con el proceso de Administración de proveedores en relación con la elección de los proveedores más aptos en el cumplimiento de los objetivos institucionales, tomando como prioridad el presupuesto para el cumplimiento de los presentes objetivos, así como la priorización de los proyectos sustanciales de la institución.
		Guía de administración del portafolio de servicios de TIC.	<input checked="" type="checkbox"/>	El proceso de Administración de Proveedores se relaciona con la presente guía, de acuerdo a los servicios proporcionados para mantener el funcionamiento de la Institución los cuales aporten beneficios para el cumplimiento de los objetivos.
		Guía de administración para las contrataciones de tecnología de la información y comunicación.	<input checked="" type="checkbox"/>	La presente guía se relaciona con el costo de la contratación de bienes y servicios que se requieren para las iniciativas de la UTIC, a fin de coadyuvar en las atribuciones así como en los procedimientos de contratación de la UTIC.
		Guía para el apoyo técnico para la contratación de soluciones tecnológicas de tecnología de la información y comunicación.	<input checked="" type="checkbox"/>	Las presentes guías se relacionan con el apoyo técnico para la contratación y seguimiento de la UTIC, mediante acciones coordinadas con las unidades responsables para la realización de los procedimientos de contratación de la Institución, considerando los requerimientos y restricciones identificadas.

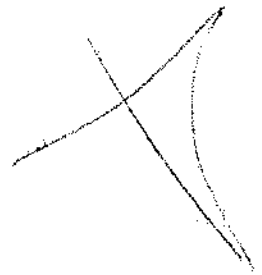
ELABORÓ: AAT/MAEL
SUPERVISÓ: BOL
INICIO: 28/09/2015
TÉRMINO: 09/10/2015

L-4)
26
00274

L-4)
23-24

PROCESOS ESTABLECIDOS POR EL MAAGTICSI	GUÍAS INSTITUCIONALES	GUÍAS QUE SE RELACIONAN CON LOS 9 PROCESOS DEL MAAGTICSI	MANTIENE RELACION	COMENTARIOS
8.- PROCESO DE ADMINISTRACIÓN DE LA OPERACIÓN	GUÍA DE ADMINISTRACIÓN DE LA OPERACIÓN	Guía para la administración de ambiente físico. Guía de mantenimiento de infraestructura.	<input checked="" type="checkbox"/>	La presente guía se relaciona con el proceso de Operación en base al establecimiento de controles en el centro de datos para el aseguramiento de los servicios, así como el mantenimiento e instalación de los equipos, a fin de protegerlos de la vulnerabilidad y riesgos físicos externos. La presente guía se relaciona en el establecimiento de programas de aprovisionamiento de la infraestructura tecnológica que ayude a alcanzar los niveles de capacidad para garantizar la continuidad de los servicios.
9.- PROCESO DE OPERACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN Y DEL ERISC (OPSEC)	GUÍA DE OPERACIÓN DE LOS CONTROLES DE LA SEGURIDAD DE LA INFORMACIÓN (ERISC)	Guía de administración de la seguridad de la información.	<input checked="" type="checkbox"/>	La guía correspondiente al presente proceso, mantiene una relación con la Guía de Administración de la Seguridad de la Información, debido a que ambas establecen criterios para mantener el control y seguridad de la información dentro de los procesos establecidos en el MAAGTICSI.
	GUÍA DE ADMINISTRACIÓN DEL CONOCIMIENTO		<input checked="" type="checkbox"/>	Las presentes guías no contienen una relación directa con los 9 procesos establecidos en el actual MAAGTICSI, sin embargo se relacionan con la Guía de Administración de Dominios Tecnológicos, la cual se encuentra relacionada con el proceso de Administración de presupuesto de la TIC.
	GUÍA PARA EL APOYO DE LA CAPACITACIÓN DEL PERSONAL LÚTIC		<input checked="" type="checkbox"/>	

2-4
23-24



ELABORÓ: AAT/MAEL
SUPERVISÓ: BOL
INICIO: 28/09/2015
TÉRMINO: 09/10/2015

2-4
27

001275