MEMORANDO

Al contestar por favor cite estos datos
Radicado No: 20191500014243

Bogotá, D.C., 2019-12-05

PARA: ANGELA MERCEDES OSPINA DE NICHOLLS
Directora General
DE: Asesor con Funciones de Control Interno
ASUNTO: Informe de resultado auditoría al Sistema de Seguridad de la Información

Respetada Dra. Ángela.

Dando cumplimiento al plan anual de auditoría aprobado por el Comité Institucional de Coordinación de Control Interno, remito en informe ejecutivo adjunto el resultado de verificar el cumplimiento de las disipaciones de la normatividad legal vigente y de normas de calidad ISO 27001: 2013 que deben ser acogidas y aplicadas en el Sistema de Seguridad de la Información de la APC-Colombia.

La auditoría desarrollada tuvo como propósito entregar un diagnóstico sobre el avance y el cumplimiento de implementación del sistema de seguridad de la información. En el informe ejecutivo se reseñan todos los aspectos que requieren ser mejorados y los aspectos no conformes que deben ser subsanados para avanzar hacia la meta sectorial de certificación del sistema en la norma ISO 27001.

Tanto los aspectos por mejorar como las no conformidades deben llevarse a plan de mejora a través del aplicativo Brújula.

Cordialmente,

ALEX ALBERTO RODRÍGUEZ CUBIDES
Asesor con Funciones de Control Interno

Anexos:
Copia: CARLOS AUGUSTO CASTAÑO CHARRY, DIRECTOR DAF. ÁNGELA KATERINE PIÑEROS FORERO, COORDINADORA GRUPO DE GESTIÓN TI.
Proyectó: ALEX ALBERTO RODRIGUEZ CUBIDES
Revisó:

AUDITORÍA SISTEMA DE GESTIÓN SEGURIDAD DE LA INFORMACIÓN
Vigencia 2019

Objetivo de auditoría

Evaluar el cumplimiento de los requisitos del Sistema de Gestión de seguridad de la Información SGSI (ISO 27001: 2013), las políticas de Gobierno Digital y Seguridad Digital en el marco de MIPG (Decreto 1499 de 2017) y demás normatividad aplicable a la Agencia para la Cooperación Internacional de Colombia APC - Colombia; con el fin de determinar un diagnóstico de implementación del SGSI.

Alcance de auditoría

La evaluación se realizará a la gestión adelantada por la Agencia para la Cooperación Internacional de Colombia APC- Colombia del 02/01/2019 a 30/09/2019.El cumplimiento de la política de seguridad y salud en el trabajo.

Criterios de auditoría

Se tendrán como criterios los siguientes:

- Ley 594 de 2000 "Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones"
- Ley 1474 de 2011 "Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública"
- Ley 1712 de 2014 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones"
- Directiva Presidencial 02 de 2019
- Decreto 1499 de 2017 Modelo Integrado de Planeación y Gestión - MIPG.
- Norma técnica ISO 27001: 2013
- Los documentos registrados en el aplicativo Brújula, los cuales se consideran como oficiales, acorde con la versión y fecha. Un total de 43 documentos están asociados al proceso de TIC en la APC-Colombia.

Documentación aplicable

Control Interno para la presente auditoría tomó como fuente de información la documentación la registrada en el aplicativo Brújula, asociada al Sistema de Gestión de Tecnología de la Información alojada en el proceso Talento Humano. Un total de 43 documentos fueron identificados, entre formatos, guía del sistema, procedimientos, reglamentos, matrices y programas.

Equipo Auditor

Eduardo Antonio Sanguinetti Romero. Auditor líder. Jefe de Control Interno de la Agencia para la Reincorporación y Normalización.
Alex Alberto Rodríguez Cubides. Auditor

Reunión de apertura auditoría: 30-10-2019
Reunión cierre de auditoría: 28-11-2019

DESARROLLO DE LA AUDITORIA

La Auditoría Integral a este Proceso se ejecutó conforme a los procedimientos de auditoría previamente definidos en el Plan de Auditoría.
Así las cosas, en el desarrollo de esta Auditoría se adelantaron los siguientes procedimientos:

- Solicitud de información para el desarrollo de la auditoria
- Reunión de apertura de la auditoría (realizada el día 30/10/2019).
- Revisión In Situ de las actividades de la etapa de desarrollo de la auditoría (desde el 31/10/2019 hasta el 1/11/2019).
- Reunión de Cierre.

En este punto es importante resaltar que, debido a las limitaciones de cualquier estructura de control interno, pueden ocurrir errores e irregularidades que no hayan sido detectados bajo la ejecución de los procedimientos de auditoría previamente planeados. Así las cosas, la Agencia y el Proceso son responsables de establecer y mantener un adecuado Sistema de seguridad de información y de prevenir irregularidades y materialización de riesgos.

AUDITORÍA SISTEMA DE GESTIÓN DE LA SEGURIDAD Y SALUD EN EL TRABAJO
Vigencia 2019

Positivo

- Disposición y conocimiento del Equipo de trabajo del Grupo de Tecnología de la Información para atender la auditoría.
- Establecimiento de un Grupo de TI para apoyar a la Agencia
- Se resalta la estructuración y contenido de algunos documentos
- Se cuenta con un proyecto de inversión “FORTALECIMIENTO DE LAS CAPACIDADES TECNOLÓGICAS DE LA INFORMACIÓN EN APC-COLOMBIA NACIONAL” con un presupuesto de $ 756.335.286

POR MEJORAR
CUMPLIMIENTO DE LOS REQUISITOS DE LA NORMA TÉCNICA ISO 27001: 2013

4. Contexto de la Organización

4.1 Conocimiento de la organización y de su contexto

El documento de política de seguridad digital que a la fecha de auditoría se encuentra referido por el proceso de gestión de tecnología de la información, debe ajustarse a las disposiciones del Sistema de Gestión de la Seguridad de la Información y permitir con ello una mejora en la valoración y análisis del contexto. Se deben determinar los aspectos internos y externos que pueden llegar a afectar la capacidad para lograr el objeto misional o propósito de la APC-Colombia en la implementación del Sistema de Gestión de la Seguridad de la Información como lo determina la ISO 27001:2013, numeral 4.1

4.2 Comprensión de las Necesidades y expectativas de las Partes Interesadas

En el documento A-OT-069 Políticas específicas de segundo nivel de la seguridad y privacidad de la información describe información, pero requiere que se realice revisión para determinar los requisitos legales, reglamentarios y contractuales de las partes interesadas en cumplimiento del numeral 4.2 de la norma ISO 27001:2013

4.3 Determinación del Alcance del Sistema de Gestión de Seguridad de la Información

No se tiene un manual del SGSI donde se establezca claramente el alcance del Sistema de Seguridad, además debe estar integrado al sistema de gestión de la Agencia. Se debe verificar y ajustar con este numeral 4.3 ISO 27001: del SGSI.

4.4 Sistema de Gestión de Seguridad de la Información

No se encontró un acto administrativo o documento (como el manual del SGSI) donde la Agencia APC- Colombia establece, mantiene y mejora el SGSI de acuerdo con los requisitos de la ISO 27000: 2013. Numeral 4.4.

POR MEJORAR
CUMPLIMIENTO DE LOS REQUISITOS DE LA NORMA TÉCNICA ISO 27001: 2013

5. Liderazgo

5.1 Liderazgo y compromiso

El documento de A-OT-011 Política de seguridad y privacidad de la información define el compromiso, sin embargo, se debe ajustar a lo exigido por la ISO 27000: 2013 y ser comunicado a todos los servidores públicos de la Agencia. La Alta dirección de demostrar liderazgo y compromiso, asegurando que se establezcan la política, los objetivos, asegurar los recursos, promoviendo la mejora continua, dirigiendo y apoyan a las personas para contribuir a la eficacia del SGSI.

5.2 Política

En el documento de A-OT-011 Política de seguridad y privacidad de la información se tiene definido unas políticas, sin embargo, se debe ajustar a lo exigido por la ISO 27000: 2013 y ser comunicada.

5.3 Roles, responsabilidades y autoridades en la organización

APC – Colombia tiene definidos unos roles y responsabilidades en generales en los diferentes documentos elaborados del proceso de gestión de TI, como:

- A-OT-011 Política de seguridad y privacidad de la información
- A-OT-069 Políticas específicas de segundo nivel de la seguridad y privacidad de a información
- A-OT-047 Gestión de riesgo de seguridad de la información.

Se debe estructurar y documentar los roles, responsabilidades y autoridades principales del SGSI en un documento aprobado y comunicado por la alta dirección, y las demás responsabilidades establecerlas en los instrumentos que se tengan definido como, por ejemplo, si es el caso, ajustar el manual de funciones.

POR MEJORAR

CUMPLIMIENTO DE LOS REQUISITOS DE LA NORMA TÉCNICA ISO 27001: 2013

6. Planificación

6.1 Acciones para tratar riesgos y oportunidades

6.1.1 Generalidades: La Agencia no tiene definido y estructurado un documento de los riesgos del Sistema de seguridad de la Información como lo determina esta norma ISO 27001:2013; al no tenerlos no se tiene un plan para su planificación y cumplir con este requisito: numeral 6.1.1., de la norma ISO 27001

6.1.2 Valoración de riesgos de la seguridad de la información: APC-Colombia no tiene definido y estructurado los riesgos donde se identifique al responsable, se analice, se aplique el proceso de valoración, como lo determina el numeral 6.1.2 de la ISO 27001: 2013.

6.1.3 Tratamiento de riesgos de la seguridad de la información

APC-Colombia tiene definido los siguientes documentos:

- Se debe realizar revisión y ajuste acorde con la norma ISO al documento Políticas específicas de segundo nivel de la seguridad y privacidad de la información con código A-OT-069. Documento que esta articulado con la declaración de aplicabilidad y el anexo A de la norma ISO 27001: 2013.
- A-OT-temporal 1005 Gestión de controles de seguridad y privacidad de la información: documento para dar cumplimiento a la declaración de aplicabilidad que exige la norma ISO 27001: 2013.

Para su cumplimiento y aplicación de la matriz o declaración de aplicabilidad numeral 6.1.3 literal d) y el anexo A de la ISO: 27001:2013 se presenta el siguiente diagnostico según la autoevaluación y reporte del Modelo de Seguridad y Privacidad de la Información MSPI del MINTIC:

POR MEJORAR
CUMPLIMIENTO DE LOS REQUISITOS DE LA NORMA TÉCNICA ISO 27001: 2013

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	30	100	REPETIBLE
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	44	100	EFECTIVO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	41	100	EFECTIVO
A.8	GESTIÓN DE ACTIVOS	36	100	REPETIBLE
A.9	CONTROL DE ACCESO	28	100	REPETIBLE
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	37	100	REPETIBLE
A.12	SEGURIDAD DE LAS OPERACIONES	37	100	REPETIBLE
A.13	SEGURIDAD DE LAS COMUNICACIONES	21	100	REPETIBLE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	38	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	20	100	INICIAL
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	31	100	REPETIBLE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	37	100	REPETIBLE
A.18	CUMPLIMIENTO	24	100	REPETIBLE
PROMEDIO EVALUACIÓN DE CONTROLES		**30**	**100**	REPETIBLE

Cuadro No.1. Elaborado por el Auditor Líder.

POR MEJORAR
CUMPLIMIENTO DE LOS REQUISITOS DE LA NORMA TÉCNICA ISO 27001: 2013

De los resultados del cuadro No. 1 se concluye:

- APC-Colombia solo ha avanzado en un 30% de implementación del anexo A (Controles de Seguridad) de la ISO: 27001: 2013, lo cual constituye un nivel muy bajo y en estado crítico.
- APC- Colombia requiere definir el proceso de valoración y tratamiento de riesgos. Se recomienda revisar y analizar el documento A-OT-047 Gestión de riesgo seguridad de la información, que fue elaborado en vigencia anterior y de igual forma los procedimientos relacionados.
- APC-Colombia No tiene la matriz de riesgo digital o de seguridad de la información, ni el Plan de tratamiento de los riesgos de la seguridad de la información.

6.2 Objetivos de seguridad de la información y planes para lograrlo

La Agencia APC Colombia, no ha definido un documento donde se establezcan los objetivos del sistema de Seguridad de la Información y lo instrumentos para lograrlos como lo indica la ISO 27001: 2013, sólo se identificó en los documentos de A-OT-011 política de seguridad y privacidad un objetivo y la política de seguridad digital que también tienen unos objetivos.

7. Recursos. El proyecto de inversión a la fecha de desarrollo de la auditoría se observa con una baja ejecución. Sin embargo, se requiere fortalecer este requisito para la implementación, mantenimiento y mejora del sistema de gestión de seguridad de la información, así como mitigar o minimizar la materialización de los riesgos, contar con personal capacitado en la norma ISO 27001: 2013 y de recursos económicos para reforzar controles entre otros.

POR MEJORAR
CUMPLIMIENTO DE LOS REQUISITOS DE LA NORMA TÉCNICA ISO 27001: 2013

7.1 Competencia

APC-Colombia debe asegurar que el personal al que se le asignen responsabilidades en el Sistema de Gestión de la Seguridad de la Información, tenga la competencia para realizar las tareas y de advertir sobre todo lo que pueda afectar el sistema. Norma ISO 27001, numeral 7.2.2 y sus respectivos literales.

-También hay que fortalecer la competencia al grupo de Control Interno en la materia, asignando recursos para formación en auditores internos acorde con lo dispuesto en la norma ISO 27001:2013

7.3 Toma de conciencia

El personal que labora en la agencia APC Colombia no ha tomado conciencia en la aplicación de las políticas y controles establecidos en los documentos del proceso de gestión de tecnología de la información. Al realizar consultas a algunos servidores no tenían claridad y conocimiento de la política.

Se debe establecer un plan de capacitación, sensibilización y aplicación para garantizar que las personas que realizan el trabajo en la Agencia tomen conciencia y conozcan las implicaciones por no aplicar los controles del SGSI.

7.4 Comunicación

APC – Colombia tiene un documento A-OT-030 Plan se seguridad y continuidad TI, sin embargo, no se tiene un plan estratégico o de acción vigencia 2019, o plan de sensibilización o capacitación como lo determina esta norma ISO 27001: 2013.

7.5 Información documentada

Dentro del Proceso de Gestión de tecnología de la Información se ha definido 47 documentos, los cuales hacen parte de la política de seguridad y privacidad de la información y en cumplimiento de la política de digital y protección de datos. Esta documentación requiere ser ajustada y articulada con los requisitos de la ISO 27001:2013 y complementar los que hacen falta, también debe estar integrado al sistema de gestión dela Agencia.

Por Mejorar
CUMPLIMIENTO DE LOS REQUISITOS DE LA NORMA TÉCNICA ISO 27001: 2013

8. Operación

8.1 Planificación y control operacional

- ✓ No existe un plan de implementación del Sistema de Gestión de seguridad de la información, sólo está el compromiso sectorial de certificación en el 2021 en la norma ISO 27001: 2013 y unas acciones generales anual.
- ✓ Se debe establecer un plan para lograr los objetivos, así como el plan de contingencia y continuidad del negocio (documento de continuidad del negocio)
- ✓ Establecer el plan Estratégico Institucional y el PETI articulado con lo requerido para el SGSI ISO 27001: 2013.

8.2 Valoración de riesgos de la seguridad de la información

- ✓ Se tiene información de los riesgos de los procesos, pero no información documentada de los resultados de las valoraciones de los riesgos de seguridad de la información como lo exige esta norma ISO 27001: 2013, además como no se tienen los riegos identificados no hay resultado de su valoración.

Se establece en desarrollo de la auditoría que está en proceso de construcción de la matriz de los riesgos.

8.3 Tratamiento de riesgos de la seguridad de la información

- ✓ Se tiene información de los riesgos de los procesos, pero no información documentada de los resultados del tratamiento de los riesgos de seguridad de la información como lo exige esta norma ISO 27001: 2013, además como no se tienen los riegos identificados no hay resultado de su tratamiento.

Por Mejorar
CUMPLIMIENTO DE LOS REQUISITOS DE LA NORMA TÉCNICA ISO 27001: 2013

9. Evaluación del desempeño

9.1 Seguimiento, medición, análisis y evaluación

- ✓ APC-Colombia no tiene definido el mecanismo para realizar el seguimiento, medición, análisis y evaluación del Sistema de Gestión de Seguridad de la información, sólo cuenta con propuestas de indicadores para las políticas de seguridad digital y del proceso de gestión de tecnología de información como las evaluaciones y resultados del Modelo de Seguridad y privacidad de la información **MSPI** – Calificación del **30%** de avance, del **FURAG** – Política de seguridad digital del **73.9%** y Gobierno digital el **78%** y un autodiagnóstico del **29,4%** de avance.
- ✓ No se ha definido un plan de mejora o de acción para mitigar y fortalecer las debilidades encontradas.
- ✓ Se debe estructurar y definir los indicadores y los mecanismos para realizar el seguimiento, medición, análisis y evaluación del Sistema de Gestión de Seguridad de la información como lo establece la ISO 27001: 2013 numeral 9.1

9.2 Auditoría Interna

- ✓ APC- Colombia tiene definido dentro de su estructura el Control Interno y el Proceso de Evaluación control y seguimiento con su información documentada.
- ✓ También programó dentro de su plan anual de auditorías, la auditoria al SGSI, al cual se ejecutó y se presenta este informe.
- ✓ Se requiere fortalecer el equipo de trabajo del grupo de Control Interno en recurso humanos y competencia – Certificación en el sistema de gestión de seguridad de la información. SGSI ISO 27001: 2013 para ejecutar las auditorías internas.

Por Mejorar
CUMPLIMIENTO DE LOS REQUISITOS DE LA NORMA TÉCNICA ISO 27001: 2013

9.3 Revisión por la Dirección

✓ APC-Colombia no posee información documentada para cumplir con este requisito.

10. Mejora

✓ APC-Colombia no posee información documentada para cumplir con este requisito.

Resultado de la verificación de los numerales de la Norma ISO 27001: 2013

Una vez verificado el cumplimiento de los requisitos de la norma técnica ISO 27001: 2013 para la implementación del Sistema de Gestión de la Seguridad de la Información en la Agencia APC- Colombia, **punto 5.1 de este documento**, se presenta el siguiente diagnóstico:

5.2 CUMPLIMIENTO DE LOS REQUISITOS DE LA POLITICA DE SEGURIDAD DIGITAL

La Agencia APC Colombia tiene definido dentro del Proceso de Gestión de Tecnología de la Información 47 documentos como se manifestó en el punto anterior; Sin embargo, es importante revisar y si es el caso, ajustar dicha documentación, además que sea coherente y articulada con el Sistema de Gestión de la Seguridad de la Información ISO 27001: 2013.

En esto momento se encuentra implementado la política se seguridad y privacidad de la información el MSPI, la política de seguridad digital y de datos personales.

DIAGNOSTICO SEGÚN LA AUDITORIA REALIZADA A LA AGENCIA APC - COLOMBIA	
NORMA ISO 27001: 2013 Y ANEXO A	
FECHA: 30/10/2019 AL 01/11/2019	
Requisito	**Calificación**
4 Contexto de la organización	**67,50**
4.1 Entendiendo la organización y su contexto	90
4.2 -Comprensión las necesidades y expectativas de las partes interesadas	90
4.3 Determinación del alcance del sistema de gestión de seguridad de la información	90
4.4 Sistema de gestión de seguridad de la información	-
5 Liderazgo	**83,33**
5.1 Liderazgo y compromiso	90,00
5.2 Política	80,00
5.3 Roles de organización, responsabilidades y autoridades	80,00
6 Planeación	**50,00**
6.1 Acciones para abordar los riesgos y oportunidades	50,00
6.1.1 Consideraciones generales	50,00
6.1.2 Evaluación de riesgos de seguridad de la información	50,00
6.1.3 tratamiento de riesgos de seguridad de la información	50,00
6.2 los objetivos de seguridad de información y la planificación para alcanzarlos	50,00
7Soporte	**54,00**
7.1 Recursos	40,00
7.2 Competencia	50,00
7.3 Toma de Conciencia	50,00
7.4 Comunicación	50,00
7.5 Información documentada	80,00
8 Operación	**6,67**
8.1 Planificación y control operacional	20,00
8.2 Valoración de riesgos de seguridad de la información	-
8.3 Tratamiento de riesgos de seguridad de la información	-
9 Evaluación del desempeño	**33,33**
9.1 Seguimiento, medición, análisis y evaluación	20,00
9.2 Auditoría Interna	80,00
9.3 Revisión por la dirección	-
10 Mejora	**-**
10.1 No conformidad y acción correctiva	-
TOTAL AVANCE	42,12

Conclusión de la verificación de los numerales de la Norma ISO 27001: 2013

1. No se identificó la aplicación de controles para:

- Entrada y salidas de bienes
- El DATA CENTER puertas abierta y entrada sin autorización.
- Contratación con ente externo - Cinta de seguridad para garantizar la continuidad del negocio, esto se constituye como un riesgo extremo alto.
- Documento de continuidad del negocio.
- Políticas aplicables para los aplicativos SARA, BRUJULA y el sistema de cooperación CICLOPE

2. No se cuenta con un plan estratégico institucional y con el PETI 2018 – 2022. Planes que deben ir articulados con los requisitos del SGSI
3. No existe un plan de implementación del Sistema de Gestión de seguridad de la información, sólo está el compromiso sectorial de certificación en el 2021 en la norma ISO 27001: 2013 y unas acciones generales anual.
4. La matriz de activo de información No está actualizada y articulada con los requisitos del Sistema de Gestión de Seguridad de la Información SGSI.
5. No se tiene establecido la arquitectura de TI.
6. No se tiene la matriz de riesgo digital o de seguridad de la información, ni el Plan de tratamiento de los riesgos de la seguridad de la información.
7. No se ha formulado ni diseñado la matriz de los riegos de seguridad digital.
8. No se tiene un manual del SGSI que establezca el alcance del Sistema de Seguridad. El manual además debe estar integrado al sistema de gestión de la Agencia. Se debe verificar y ajustar con el numeral 4.3 de la ISO 27001: del SGSI.

Conclusión de la verificación de los numerales de la Norma ISO 27001: 2013

5.3 CUMPLIMIENTO DE LOS REQUISITOS DE LA POLITICA DE GOBIERNO DIGITAL

La Agencia APC Colombia se encuentra en construcción de la política de gobierno digital y aplica las disposiciones de la ley 1712 de 2014; además presenta un avance del 78% según reporte FURAG.

En conclusión, la agencia no ha dado total cumplimiento a esta política.

No Conformidades

1. Sistema de Gestión de la Seguridad de la Información: La Agencia Presidencial de Cooperación Internacional, APC-Colombia, No ha definido y aplicado toda la documentación del Sistema de Gestión de Seguridad de la Información según los requisitos de la norma técnica ISO: 27001:2013, como se evidenció en los avances de los informes de autodiagnóstico 29.4%, el modelo de seguridad y privacidad de la información MSPI 30%, y resultado de la auditoria aplicada 42.12%.

2. Política de Seguridad digital: APC – Colombia no ha definido y aplicado toda la documentación de la política de seguridad digital, como se evidenció en los siguientes casos:

a. No se identificó la aplicación de controles para:
   - ✓ Entrada y salidas de bienes
   - ✓ El DATA CENTER puertas abierta y entrada sin autorización
   - ✓ Contratación con ente externo - Cinta de seguridad para garantizar la continuidad del negocio, **esto se constituye como un riesgo extremo alto**.
   - ✓ Documento de continuidad del negocio.
   - ✓ Políticas aplicables para el SARA, CICLOPE y BRUJULA
b. No se cuenta con un plan estratégico institucional y con el PETI 2018 - 2022
c. La matriz de activos de información no está actualizada y articulada con los requisitos del Sistema de Gestión de Seguridad de la Información –SGSI- Norma ISO 27001: 2013 Anexo A.
d. No se tiene establecido la arquitectura de TI.
e. No se ha presentado ante el Comité de Gestión y Desempeño los resultados de avance de la política de seguridad y privacidad MSPI, política digital, FURAG y Autodiagnóstico con el fin de que la alta dirección tome las medidas a que haya lugar.

No Conformidades

f. Definir la medición, análisis y evaluación interna y su resultado.
g. Matriz de riegos de seguridad digital

Además, con un avance en el **FURAG 2018** del **73.90%**

Lo anterior, incumpliendo lo establecido en el Decretos 1008 de 2018, y en especial *"…Artículo 2.2.9.1.2.2. Manual de Gobierno Digital. Para la implementación de la Política de Gobierno Digital, las entidades públicas deberán aplicar el Manual de Gobierno Digital que define los lineamientos, estándares y acciones a ejecutar por parte de los sujetos obligados de esta Política de Gobierno Digital…."*, este manual incluye el Modelo de Seguridad digital.

3. Política de Gobierno digital: APC- Colombia presenta un avance del **78%** reporte **FURAG**, sin embargo, en la verificación se observó que se está construyendo un documento de política y aplicación de herramientas establecidas, no se identificó información documentada de los resultados de esta política para la vigencia 2019, es decir indicadores y/o plan de acción que permita verificar el cumplimiento de requisitos normativos y la efectividad de los controles para mitigar la materialización de los riesgos que afectan la implementación de esta política.

Lo anterior, incumpliendo lo establecido en el Decreto 1008 de 2018 y en especial *"…. Artículo 2.2.9.1.2.2. Manual de Gobierno Digital. Para la implementación de la Política de Gobierno Digital, las entidades públicas deberán aplicar el Manual de Gobierno Digital que define los lineamientos, estándares y acciones a ejecutar por parte de los sujetos obligados de esta Política de Gobierno Digital…."*.

No Conformidades

4. No se ha definido un plan de mejora o de acción para mitigar y fortalecer las debilidades encontradas como resultado de los instrumentos señalados en el numeral 6°.
5. APC-Colombia no ha dado alcance ni aplicación a los controles que se encuentran establecidos en los documentos oficiales asociados al Proceso de Gestión de TI.
6. No se ha presentado ante el Comité de Gestión y Desempeño los resultados de avance de la política de seguridad y privacidad MSPI, política digital, FURAG y Autodiagnóstico con el fin de que la alta dirección tome las medidas a que haya lugar. Artículo 2.2.9.1.3.3., Decreto 1008 de 2018.
7. APC-Colombia no tiene definido el mecanismo para realizar el seguimiento, medición, análisis y evaluación del Sistema de Gestión de Seguridad de la información, sólo cuenta con propuestas de indicadores para las políticas de seguridad digital y del proceso de gestión de tecnología de información, así como las evaluaciones y resultados del Modelo de Seguridad y privacidad de la información MSPI – Calificación del 30% de avance, del FURAG – Política de seguridad digital del 73.9% y Gobierno digital el 78% y un autodiagnóstico del 29,4% de avance.

APC-Colombia debe asegurar que el personal al que se le asignen responsabilidades en el Sistema de Gestión de la Seguridad de la Información, tenga la competencia para realizar las tareas y la de advertir sobre todo lo que pueda afectar el sistema. Norma ISO 27001, numeral 5.2.2 y sus respectivos literales

Recomendaciones

Acciones de mediano plazo

- Elaborar y solicitar plan de formación de auditores ISO 27001. Acción que permitirá fortalecer la gestión de auditoría del Proceso de Evaluación Control y Mejoramiento.

Elaboró Informe de auditoría: Eduardo Antonio Sanguinetti Romero. Auditor Líder