INFORME DEFINITIVO EVALUACIÓN INDEPENDIENTE PROCEDIMIENTO GESTIÓN DE LOS SERVICIOS DE TI.

DIEGO MAURICIO ECHEVERRI ARANGO
Jefe de Oficina de Control Interno

YUDY LISET JIMENEZ CANO
Técnico Operativo 1

OFICINA DE CONTROL INTERNO

MEDELLÍN, DICIEMBRE DE 2022

TABLA DE CONTENIDO

pág.

LISTA DE CUADROS

pág.

LISTA DE ILUSTACIONES

pág.

INTRODUCCION

Para una organización uno de sus activos más valiosos es la información, de tal manera que poder preservar la confidencialidad, la integridad y la disponibilidad de la información se ha convertido en una de las necesidades más apremiantes para cualquier empresa, por lo cual identificar, analizar y gestionar las amenazas y vulnerabilidades que se configuran en riesgos de seguridad de la información, está dentro de las prioridades de las diversas organizaciones; no obstante, este proceso no se puede desligar de los medios tecnológicos usados para acceder, compartir, gestionar, trasladar y almacenar la información; así es como la seguridad informática es imprescindible en la gestión de riesgos de seguridad y privacidad de la misma.

Debido a las actualizaciones de softwares, la implementación de nuevas tecnologías, la mejora continua en estándares de seguridad y buenas prácticas, la aparición de nuevas amenazas cibernéticas y la normatividad que establecen los gobiernos para garantizar un adecuado manejo de la información y una apropiada interacción en el ciberespacio, es necesario que las organizaciones de forma permanente estén gestionando mejoras y actualizaciones en seguridad digital.

Por lo esbozado anteriormente, la Oficina de Control Interno de la Contraloría General de Medellín, en cumplimiento de las funciones asignadas en la Ley 87 de 1993 y en virtud del rol de evaluación y seguimiento asignado a través del artículo 17 del Decreto 648 del 2017, realiza el presente informe de evaluación a las medidas adoptadas en Seguridad Digital, Seguridad y Privacidad de la Información y Transición al Protocolo IPv6 en Convivencia con el Protocolo IPv4, con corte al 30 de diciembre de 2022, teniendo en consideración los lineamientos impartidos por MinTIC en el Anexo 3 de la Resolución 1519 del 2020, en la Guía de Transición de IPv4 a IPv6 de la Resolución 1126 de 2021 y en las Guías del MinTIC para el Modelo de Seguridad y Privacidad de la Información.

CRITERIOS DE LA AUDITORIA

Para la realización de la presente evaluación independiente, se tiene como referente los siguientes criterios de auditoría:

- Plan Estratégico de Tecnologías de la Información y Comunicaciones (PETI) vigente de la C.G.M.
- Procedimientos SIGI que sean pertinentes.
- Resolución 1519 de 2020 del MicTIC (Anexo3), Condiciones mínimas técnicas y de seguridad digital.
- Resolución 1126 de 2021 del MicTIC, Por la cual se establecen lineamientos para la adopción del protocolo IPv6 y se modifica la Resolución 2710 de 2017.
- Guías del MinTIC para el Modelo de Seguridad y Privacidad de la Información.
- Decreto 1078 de 2015, Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1008 del 14 de 2018 Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".
- 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.
- Ley 80 de 1993 Por la cual se expide el Estatuto General de Contratación de la Administración Pública.
- Norma ISO 27001 - Gestión de la seguridad de la información, y su Anexo A.
- Decreto 1474 de 2017 – Dirección de Gobierno Digital.
- Ley 603 de 2000, llamada en algunos casos como ley de licencias de Software (o Ley para cumplimiento de las licencias de Software).

OBJETIVOS DE LA EVALUACION

3.1 OBJETIVO GENERAL

Evaluar la adecuada documentación, implementación y ejecución de las medidas establecidas por la Dirección de Desarrollo Tecnológico de la Contraloría General de Medellín, para dar cumplimiento a las Condiciones Mínimas Técnicas y de Seguridad Digital solicitadas por el MinTIC en el Anexo 3 de la Resolución 1519 del 2020 y a la Guía de Transición de IPv4 a IPv6 de la Resolución 1126 de 2021.

3.2 OBJETIVOS ESPECIFICOS

- Revisar el progreso en el proceso de autodiagnóstico para la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) en la C.G.M.
- Realizar la verificación y seguimiento a la implementación de los controles determinados para satisfacer los requerimientos solicitados por el MinTIC en el Anexo 3 de la Resolución 1519 del 2020, que están distribuidos en: 26 requerimientos de seguridad digital y 6 requerimientos de código fuente.
- Verificar si se desarrollaron conforme a los lineamientos proporcionados mediante la Resolución 1126 de 2021 del MinTIC, el proceso de transición del protocolo IPv4 al IPv6.

ALCANCE

La Evaluación Independiente se realizará a las gestiones adelantadas para la vigencia 2022, periodo comprendido entre 01 de enero y el 30 de diciembre, respecto a la implementación y el cumplimiento de lo establecido por MinTIC en el Anexo 3 de la Resolución 1519 del 2020 y en la Resolución 1126 de 2021 del proceso de transición al protocolo IPv6 en convivencia con el protocolo IPv4 y se verificará el avance en la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI)**.**

No obstante, se podrán incorporar hechos adicionales que se evidencien en la auditoria y que estén por fuera del periodo definido en el alcance, hechos que quedarán habilitados para la evaluación que se adelante. En los casos que sea necesario ampliar información, se tomaran muestras de soportes o transacciones de otras vigencias.

METODOLOGIA

La metodología utilizada para la realización del presente informe, consistió en lo siguiente:

- Revisión de la normatividad legal aplicable al proceso de Seguridad Digital, Seguridad y Privacidad de la Información y Transición del Protocolo IPv4 al IPv6, con el fin de definir los criterios para la evaluación.

- Observación de los soportes documentales que reposan en el software Isolución de la C.G.M. sobre la Matriz de Riesgos DAFP V5 (riesgos 32,33,34), la Política Modelo de Seguridad y Privacidad de la Información, Política Gobierno Digital, Política de Uso de Servicios Informáticos, la Gestión de los Servicios TI; y la revisión de las respuestas proporcionadas por la Dirección de Desarrollo Tecnológico en la Matriz ITA (Índice de Transparencia y Acceso a la Información) 2022 de la Procuraduría General de la Nación, en relación al Anexo 3 de Resolución 1519 del 2020, para la construcción de una lista de requerimientos de evidencia que soporten los procesos y controles implementados según el anexo citado anteriormente.

- Definición de la muestra de auditoría a incluir en la evaluación independiente.

- Solicitud de información y realización entrevistas con los funcionarios pertinentes, de acuerdo a las necesidades identificadas.

- Verificación y análisis de información aportada por los dueños del proceso.

- Ejecución de pruebas a la página web de la entidad y verificación de configuraciones en algunos equipos de cómputo para corroborar la implementación de algunas medidas respecto a la seguridad digital.

- Validación de las observaciones realizadas por el equipo auditor mediante la realización de la mesa de trabajo de cierre de auditoría.

- La auditoría incluyó planificación, ejecución y comunicación de resultados del seguimiento realizado a los objetivos enunciados en este documento para el año 2022.

REFERENCIA RESPUESTA DEL AUDITADO

La Dirección de Desarrollo Tecnológico objeto de esta auditoría, dio respuesta a la información solicitada mediante:

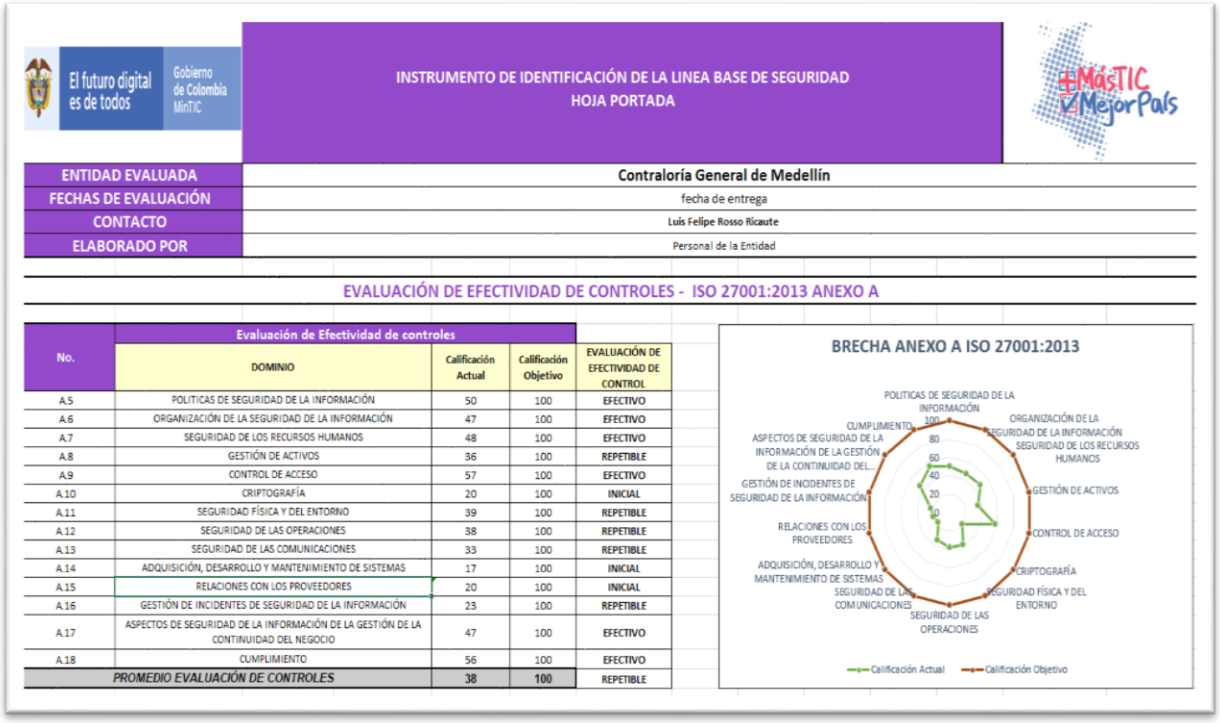
- Correo electrónico el día 24/11/2022 con el documento AVANCE MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI).docx
- Comunicación radicada bajo el No 1520 – 202200011314 radicado el 29/11/2022, en el cual expresa lo siguiente: Con el fin de dar respuesta a su memorando No. 202200011099 radicado el día 22 de noviembre de 2022, le anexo la respuesta de la Resolución 1519 del anexo No 3 correspondiente a la Dirección de Desarrollo Tecnológico. Anexos adjuntos:
  - Anexo:0000163325, título: Proyección, descripción: Respuesta
  - Anexo:0000163326, título: Proceso, descripción: Actualización Firewall
  - Anexo: 0000163327, título: Formulación, descripción: Plan de Mejoramiento
  - Anexo: 0000163328, título: Formato Excel, descripción: Log KACTUS
  - Anexo: 0000163329, título: Seguridad, descripción: Dashboard

- Correo electrónico el día 05/12/2022 con el documento Diagnostico_IPV6.pdf

6.1 AVANCE MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La información es el activo más preciado e importante para cualquier entidad y, por tanto, la CGM ha tomado todas las precauciones necesarias, para mantenerla y preservarla. Para ello, la entidad ha venido desarrollando y evolucionando en su modelo de seguridad y privacidad de la información (MSPI), soportado en tres pilares fundamentales: confidencialidad, integridad y disponibilidad; así como adoptando buenas prácticas en cuanto a la gestión y administración de las TI.

Ilustración 1 Evaluación De Efectividad De Controles - ISO 27001:2013 Anexo A



El futuro digital es de todos — Gobierno de Colombia MinTIC

INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD
HOJA PORTADA

#MásTIC MejorPaís

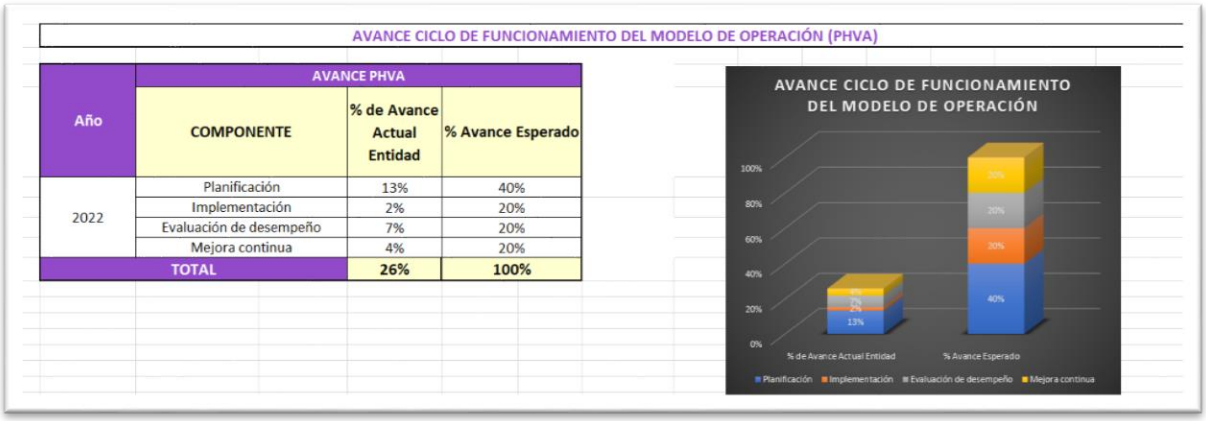
ENTIDAD EVALUADA	Contraloría General de Medellín
FECHAS DE EVALUACIÓN	fecha de entrega
CONTACTO	Luis Felipe Rosso Ricaute
ELABORADO POR	Personal de la Entidad

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	50	100	EFECTIVO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	47	100	EFECTIVO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	48	100	EFECTIVO
A.8	GESTIÓN DE ACTIVOS	36	100	REPETIBLE
A.9	CONTROL DE ACCESO	57	100	EFECTIVO
A.10	CRIPTOGRAFÍA	20	100	INICIAL
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	39	100	REPETIBLE
A.12	SEGURIDAD DE LAS OPERACIONES	38	100	REPETIBLE
A.13	SEGURIDAD DE LAS COMUNICACIONES	33	100	REPETIBLE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	17	100	INICIAL
A.15	RELACIONES CON LOS PROVEEDORES	20	100	INICIAL
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	23	100	REPETIBLE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	47	100	EFECTIVO
A.18	CUMPLIMIENTO	56	100	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		38	100	REPETIBLE

Fuente: La Dirección de Desarrollo Tecnológico CGM

Ilustración 2 Avance Ciclo De Funcionamiento Del Modelo De Operación (PHVA)

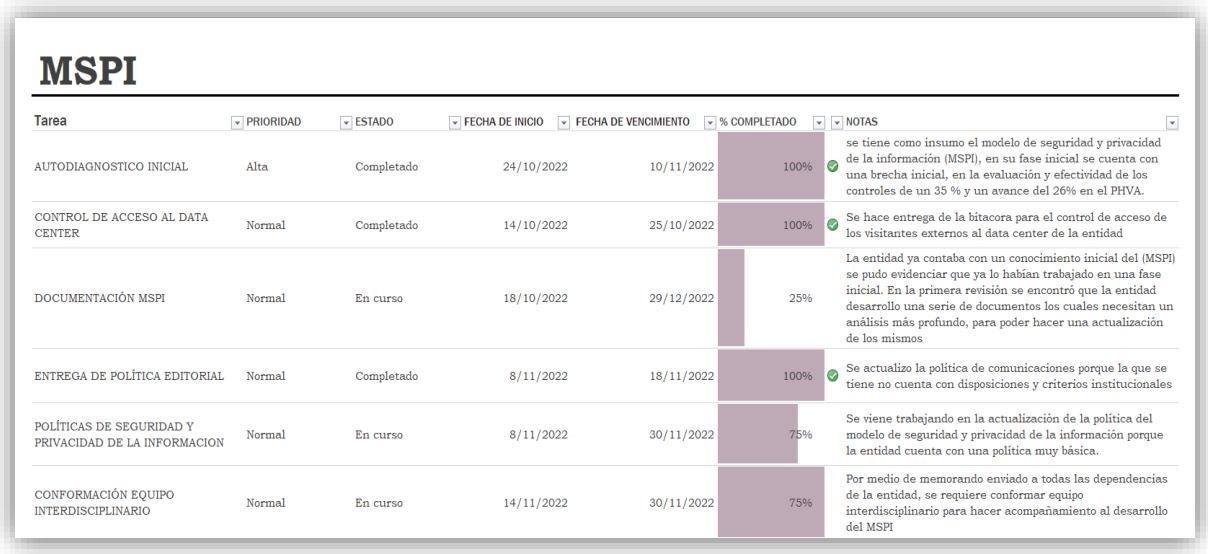


AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2022	Planificación	13%	40%
	Implementación	2%	20%
	Evaluación de desempeño	7%	20%
	Mejora continua	4%	20%
TOTAL		26%	100%

Fuente: La Dirección de Desarrollo Tecnológico

Ilustración 3 Avance Actual Del MSPI Contraloría General De Medellín



MSPI

Tarea	PRIORIDAD	ESTADO	FECHA DE INICIO	FECHA DE VENCIMIENTO	% COMPLETADO	NOTAS
AUTODIAGNOSTICO INICIAL	Alta	Completado	24/10/2022	10/11/2022	100%	se tiene como insumo el modelo de seguridad y privacidad de la información (MSPI), en su fase inicial se cuenta con una brecha inicial, en la evaluación y efectividad de los controles de un 35 % y un avance del 26% en el PHVA.
CONTROL DE ACCESO AL DATA CENTER	Normal	Completado	14/10/2022	25/10/2022	100%	Se hace entrega de la bitacora para el control de acceso de los visitantes externos al data center de la entidad
DOCUMENTACIÓN MSPI	Normal	En curso	18/10/2022	29/12/2022	25%	La entidad ya contaba con un conocimiento inicial del (MSPI) se pudo evidenciar que ya lo habían trabajado en una fase inicial. En la primera revisión se encontró que la entidad desarrollo una serie de documentos los cuales necesitan un análisis más profundo, para poder hacer una actualización de los mismos
ENTREGA DE POLÍTICA EDITORIAL	Normal	Completado	8/11/2022	18/11/2022	100%	Se actualizo la política de comunicaciones porque la que se tiene no cuenta con disposiciones y criterios institucionales
POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	Normal	En curso	8/11/2022	30/11/2022	75%	Se viene trabajando en la actualización de la política del modelo de seguridad y privacidad de la información porque la entidad cuenta con una política muy básica.
CONFORMACIÓN EQUIPO INTERDISCIPLINARIO	Normal	En curso	14/11/2022	30/11/2022	75%	Por medio de memorando enviado a todas las dependencias de la entidad, se requiere conformar equipo interdisciplinario para hacer acompañamiento al desarrollo del MSPI

Fuente: La Dirección de Desarrollo Tecnológico

Se tiene proyectado para el año 2023 evaluar y desarrollar las guías, políticas y manuales que apliquen para la entidad, estos documentos son suministrados por el ministerio de las TIC como guías para el desarrollo de las mismas; evaluar los controles de la norma ISO27002 los cuales están contenidos en el anexo A y aplicarlos.

La forma de aplicar estas guías es que a medida que se va desarrollando el modelo de seguridad y privacidad de la información (MSPI) se van incluyendo y desarrollando para poder culminar en un Sistema de Gestión de la Seguridad de la Información (SGSI) a 2024.

6.2 RESPUESTA DE LA RESOLUCIÓN 1519 DEL ANEXO NO 3

Respecto a la información proporcionada por la Dirección de Desarrollo Tecnológico expondremos los siguientes ítems: de la sección de Condiciones de Seguridad Digital, los ítems 5 y 19; y de la sección de código fuente los ítems del 1 al 6.

Cuadro 1 Matriz ITA - Condiciones de Seguridad Digital - Ítem 5

DESCRIPCIÓN	AVANCES	OBSERVACIONES
5. Proteger la integridad del código, mediante: (i) la validación exhaustiva de: inputs, variables post y get (no enviar parámetros sensibles a través del método get), Cookies (habilitar atributos de seguridad como Secure y HttpOnly), y, cabeceras HTTP; (ii) la sanitización de los parámetros de entrada: es decir, que cuando se reciba la información de dichas variables se eliminen etiquetas, saltos de línea, espacios en blanco y otros caracteres especiales que comúnmente conforman un script, además de la restricción de formatos y tamaños de subidas de archivos; (iii) la sanitización y escape de variables en el código; (iv) verificación estándar de las Políticas de Origen de las cabeceras; y (v) la verificación y comprobación del token de CSRF (cuando aplique).	100%	Las aplicaciones con que cuenta la entidad se adquirieron bajo los estándares de calidad exigidos en cuanto a seguridad para mantener los mejores parámetros de funcionamiento y evitando los riegos de seguridad que nos puedan afectar como institución, así mismo la entidad garantiza la continuidad de los mismos esquemas de seguridad adquiriendo año tras año los mantenimientos adecuados de los aplicativos que continuar minimizando los riesgos con las nuevas amenazas que se encuentran.

Fuente: La Dirección de Desarrollo Tecnológico

Todos los aplicativos de la CGM operan con los elementos de seguridad, como validación de contraseñas, unas en sus propios repositorios y otras contra el directorio activo de la entidad, así mismo los proveedores garantizan que la operatividad a través de actualizaciones que corrigen fallas que podrían inferir en riesgos de seguridad de los aplicativos, y en este sentido la dirección de desarrollo tecnológico realiza los contratos correspondientes con los proveedores del software para adquirir dichos parches y poder garantizar la funcionalidad de los aplicativos.

De igual manera en los contratos de realizados se coloca como obligación del contratista:

"*14) Obligación sobre Seguridad Informática: El Contratista con la firma del presente contrato, se obliga a dar cumplimiento a las políticas y normas de seguridad informática de la Contraloría General de Medellín, incorporadas en el Sistema de Integral Gestión, al cual podrá acceder, a través del Portal web de la Entidad www.cgm.gov.co por la opción Información Corporativa-Sistemas de*

Información-Isolución y allí aparecen las credenciales de acceso: usuario: consultas clave CGM12345. Una vez haya ingresado, dar clic en la opción documentación, opción manuales y allí encontrará el Manual Políticas de Operación de la Entidad (numeral 38). La trasgresión a los 3 reglamentos o directrices, dará lugar a la aplicación de las sanciones correspondientes, sin perjuicio de la responsabilidad civil, penal o disciplinaria que recaiga sobre la Contratista."

Lo anterior pone a disposición de la CGM una serie de herramientas contractuales para exigir el cumplimiento de las políticas de seguridad.

Cuadro 2 Matriz ITA - Condiciones de Seguridad Digital - Ítem 19

DESCRIPCIÓN	AVANCES	OBSERVACIONES
19. Revisar las recomendaciones de seguridad en la guía de desarrollo seguro de aplicaciones y Servicios Web Seguros de la Open Web Application Security Project (OWASP).	N/A	La entidad no desarrolla sus propias aplicaciones web.

Fuente: La Dirección de Desarrollo Tecnológico

Cuadro 3 Matriz ITA - Programación del Código Fuente - Ítems 1 al 6

PROGRAMACIÓN DEL CÓDIGO FUENTE		
DESCRIPCIÓN	**AVANCES**	**OBSERVACIONES**
1. Realizar análisis estático del código con el objetivo de identificar vulnerabilidades que se encuentra en la programación de las aplicaciones.	N/A	La entidad no realiza desarrollos propios, las aplicaciones son adquiridas a terceros y se mantienen actualizadas año tras año con la adquisición de actualizaciones de seguridad y de mejora a los mismos proveedores
2. Cumplir con la estandarización de código fuente para portales web, siguiendo las buenas prácticas del W3C (World Web Wide Consortium), de forma que permita la correcta visualización de la información a los usuarios.	N/A	La entidad no realiza desarrollos propios, las aplicaciones son adquiridas a terceros y se mantienen actualizadas año tras año con la adquisición de actualizaciones de seguridad y de mejora a los mismos proveedores

3. Adoptar validadores HTML y CCS para la continua revisión del sitio web y su mejora continua, a través de las buenas prácticas del W3C (World Web Wide Consortium).	N/A	La entidad no realiza desarrollos propios, las aplicaciones son adquiridas a terceros y se mantienen actualizadas año tras año con la adquisición de actualizaciones de seguridad y de mejora a los mismos proveedores
4. Cumplir con los estándares definidos para la integración al Portal Único del Estado Colombiano GOV.CO, incluyendo la validación de la codificación, en caso de que les aplique.	N/A	La entidad no realiza desarrollos propios, las aplicaciones son adquiridas a terceros y se mantienen actualizadas año tras año con la adquisición de actualizaciones de seguridad y de mejora a los mismos proveedores
5. Incluir lenguaje común de intercambio para la generación y divulgación de la información y datos estructurados y no estructurados dispuestos en medios electrónicos, como los sitios web de los sujetos obligados y el Portal Único del Estado Colombiano GOV.CO, en caso de que les aplique.	N/A	La entidad no realiza desarrollos propios, las aplicaciones son adquiridas a terceros y se mantienen actualizadas año tras año con la adquisición de actualizaciones de seguridad y de mejora a los mismos proveedores
6. Implementar un sistema de control de versiones (Git), que permitan planear y controlar la vida de la aplicación, y en una fase a mediano plazo poder implementar un sistema de integración, cambio y despliegue continuo	N/A	La entidad no realiza desarrollos propios, las aplicaciones son adquiridas a terceros y se mantienen actualizadas año tras año con la adquisición de actualizaciones de seguridad y de mejora a los mismos proveedores

Fuente: La Dirección de Desarrollo Tecnológico

6.3 RESPUESTA DE LA RESOLUCIÓN 1126 DE 2021

Respecto al proceso de transición del protocolo IPv4 al IPv6, expondremos el "Informe de Cumplimiento De IPv6 – Diagnostico" contenido en el "Plan de Transición del Protocolo IPv4 a IPv6" proporcionado por la Dirección de Desarrollo Tecnológico, donde se evidencia que elementos soportan el protocolo IPv6 y cuáles no.

INFORME DE CUMPLIMIENTO DE IPV6 - DIAGNOSTICO

En este apartado se analiza el cumplimiento de los inventarios realizados por grupo de grandes elementos.

- **Redes de comunicaciones:** Se verifico que el 100% de los elementos que componen este grupo es compatible con la implementación IPV6.
- **Sistemas de Almacenamiento:** Se verifico que el 100% de los elementos que componen este grupo es compatible con la implementación IPV6.
- **Aplicativos de Software:** Se realizó la verificación con los fabricantes de los aplicativos los cuales emitieron conceptos favorables de la compatibilidad de los mismos con la implementación IPV6.
- **Sistemas de Seguridad:** En este grupo se presentan los elementos biométricos y cámaras de seguridad, al analizar el detalle de los firmwares soportados por cada elemento se tiene lo siguiente:
    - Biométricos: Los elementos de Biometría con que cuenta la entidad no soportan de marca Soyal no presentan soporte para la implementación IPV6.
    - Cámaras de Seguridad: los elementos de video vigilancia con que cuenta la entidad no presentan un manejo adecuado del protocolo IPV6, sin embargo, al validar con el fabricante especifico que este comportamiento seria mejorado en un firmware liberado más adelante, por lo tanto, su compatibilidad es parcial.
- **Equipos de Cómputo:** Se verifico que el 100% de los elementos que componen este grupo es compatible con la implementación IPv6.
- **Telefonía:** Se verifico que los servidores de telefonía soportan la implementación de IPV6. Sin embargo, los teléfonos IP en su actual versión del software no soportan la implementación de IPv6.

RESULTADOS DE LA EVALUACIÓN

Para dar cumplimento a los objetivos propuestos en la evaluación independiente, se revisaron las medidas implementadas por la Dirección de Desarrollo Tecnológico de la Contraloría General de Medellín, respecto al Anexo 3 de la Resolución 1519 de 2020 y a la Resolución 1126 de 2021, detallamos a continuación los resultados:

La Dirección de Desarrollo Tecnológico de la CGM mediante la Matriz ITA (Índice de Transparencia y Acceso a la Información) 2022 de la Procuraduría General de la Nación, en relación al Anexo 3 de Resolución 1519 del 2020, notificó que de los 26 requerimientos en seguridad digital, fueron implementados en la entidad 24 ítems con un cumplimiento del 100%, de igual manera, informó que 2 de los requerimientos en seguridad digital no le aplicaban a la entidad, debido a que dentro de su proceso administrativo de servicios de TI, no realizan desarrollo de software.

Acode con la información suministrada por la Dirección de Desarrollo Tecnológico de la CGM para esta auditoría, se constató la adecuada implementación y ejecución de medidas de seguridad digital en relación a los ítems del 2 al 4, del 6 al 18 y 20 al 26 del Anexo 3 de la Resolución 1519 del 2020. Respecto al ítem 5, se encontró una fragilidad con relación a la protección de la integridad del código; lo cual se evidencia en que la entidad adquiere mantenimientos de cada software para minimizar riesgos y amenazas, pero no se hallaron soportes por parte de los proveedores que prueben el aseguramiento del código fuente, la minimización de riesgos y vulnerabilidades. Y en relación al ítem 19, tampoco no se encontraron soportes por parte del Desarrollador Web encargado de la página de la entidad, que garanticen la adopción de buenas prácticas del W3C (World Web Wide Consortium).

Frente a los ítem 1 al 6 de la sección *“Programación del Código Fuente”* del Anexo 3 de la Resolución 1519 del 2020, la Dirección de Desarrollo Tecnológico manifestó que no eran aplicables a la entidad, ya que esta *“no realiza desarrollos propios, las aplicaciones son adquiridas a terceros y se mantienen actualizadas año tras año con la adquisición de actualizaciones de seguridad y de mejora a los mismos proveedores”*. Sin embargo frente a los ítems 1, 2 y 3, no se halló un requerimiento en los contratos con los proveedores de software donde se garantice la realización de pruebas de análisis estático al código fuente y el soporte documental de estas. De igual manera falta una solicitud expresa en los contratos, referente a cumplir con la estandarización de código fuente para portales web, siguiendo las buenas prácticas del W3C y la adopción de validadores de código.

En relación a los ítems 4 y 5 de la sección *"Programación del Código Fuente"* del Anexo 3 de la Resolución 1519 del 2020, se identificó una deficiencia contractual, ya que no se halló por escrito los requerimientos para garantizar el cumplimento por parte del proveedor de los estándares definidos para la integración al Portal Único del Estado Colombiano GOV.CO. Es de aclarar, que en la revisión de la página web de la entidad se constató el cumplimiento en lo que respecta a la publicación de datos abierto y la integración al Portal Único del Estado Colombiano GOV.CO, pero existe ese vacío en términos legales.

Respecto a la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) en la C.G.M, se encontraron avances en el proceso de Autodiagnóstico, hallando una debilidad en el aporte de evidencias. Además, han avanzado en la consolidación de un equipo interdisciplinario, que tienen proyectado ayudará a la consolidación de activos de información y a garantizar que el proceso de adopción del modelo sea trasversal a todas las dependencias de la C.G.M.

Con relación a la Resolución 1126 de 2021 del MinTIC, del proceso de transición del protocolo IPv4 al IPv6, la entidad avanzó en la elaboración del *"Plan de Transición del Protocolo IPv4 a IPv6"*, sin embargo, se identificó que a raíz de los cambios de personal presentados en la Dirección de Desarrollo Tecnológico, la dependencia no logró tener una continuidad en el proceso de transición, donde se materializaron muchos de los riesgos esbozados en el *"Plan de Contingencias"* del *"Plan de Transición del Protocolo IPv4 a IPv6"* que elaboro la entidad, generando retrasos en la implementación del plan de transición y dificultando el cumplimiento de los tiempos establecidos en la resolución.

RECOMENDACIONES

En algunos aspectos se identificó posibilidades de mejora, que pueden contribuir con el fortalecimiento de la seguridad digita, con base en la auditoría realizada la Oficina de Control Interno recomienda adelantarlas siguientes acciones:

Recomendación 1.
Frente a la implementación del Modelo de Seguridad y Privacidad de la Información, incluir controles que garanticen un correcto soporte documental en el proceso de Autodiagnóstico, que consta de tres etapas: Estado actual de la entidad, Identificación el nivel de madurez, Levantamiento de la información, que se desarrolla a través del diligenciamiento de la Herramienta – "Instrumento De Identificación de la Línea Base de Seguridad" dispuesta por MinTIC, que en los subprocesos Levantamiento de la Información, Administrativas, Técnicas, PHVA solicita evidencia de la implementación de requerimientos, para así mitigar el riesgo de un inadecuado autodiagnóstico.

Recomendación 2.
Para el levantamiento de "activos de información" que hace parte del proceso de Autodiagnóstico para la implementación del MSPI, se recomienda verificar con la Secretaria General de la CGM los avances realizados para dar cumplimiento a la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional 1712 de 2014, donde se realizó "El Registro de Activos de Información" de la Contraloría General de Medellín, el cual está publicado en la página de la entidad, en el botón "Transparencia y Acceso a la Información" en la sección "Datos Abiertos", con el fin de garantizar una trazabilidad de la información.

Recomendación 3

Identificar los riesgos en seguridad digital que surgen a partir de las posibles vulnerabilidades de los software y aplicaciones adquiridos con terceros, establecer el impacto de darse una materialización de estos, definir las responsabilidades por parte de los proveedores de software en los contratos, evaluar y determinar si es necesario solicitar la adquisición de pólizas de protección digital que cubran la afectación económica que puede darse.

Recomendación 4

Para fortalecer el cumplimiento del ítem 5, de la sección “Condiciones de Seguridad Digital” del Anexo 3 de la Resolución 1519 del 2020, incluir dentro de los contratos de mantenimiento que se celebran con los proveedores de los software: Mercurio, Isolución, Seven-ERP, Kactus-HCM, Gestión Transparente y los desarrolladores de la página web de la entidad, el aporte de soportes como tipos de pruebas desarrolladas por parte de estos, que evidencien el aseguramiento del código fuente de los aplicativos o los desarrollos, así como las medidas implementadas tras los hallazgos de vulnerabilidades y si se dan actualizaciones de versiones, es imprescindible que sobre estas se desarrollen nuevas pruebas. Así mismo es necesario establecer con qué frecuencia deben ser presentadas las evidencias por parte de los proveedores, ya que los riesgos de seguridad digital no son estáticos y evolucionan con los avances tecnológicos.

Recomendación 5

Solicitar a los desarrolladores de la página web de la entidad la adopción de las recomendaciones de seguridad descritos en “la guía de desarrollo seguro de aplicaciones y Servicios Web Seguros de la Open Web Application Security Proyect (OWASP)” que apliquen, con un aporte de evidencias como: tipos de pruebas desarrolladas sobre la página web de la CGM que soporten dicho proceso.

Recomendación 6

Fortalecer los conocimientos de los funcionarios de la Dirección de Desarrollo tecnológico en “buenas practicas del W3C (World Web Wide Consortium)” y en “la guía de desarrollo seguro de aplicaciones y Servicios Web Seguros de la Open Web Application Security Proyect (OWASP)”, para que puedan establecer si los controles y medidas adoptadas por los proveedores de software, son suficientes para mitigar los riesgos provenientes de los software y aplicaciones adquiridos con terceros.

Recomendación 7

Respecto al ítem 1, de la sección Programación del Código fuente del Anexo 3 de la Resolución 1519 del 2020, se recomienda solicitar en los contratos de mantenimiento con los proveedores de software pruebas de análisis estático sobre el software y las versiones de actualización y documentación de las medidas adoptadas tras la identificación de errores y vulnerabilidades, si no cuentan con estas, establecer acuerdos que permitan su implementación.

Recomendación 8
Frente a los ítems 2 y 3, de la sección Programación del Código fuente del Anexo 3 de la Resolución 1519 del 2020, se recomienda adoptar el validador de HTML, XHTML, SMIL, MathML y CSS, llamado "Markup Validation Service" del W3C (World Web Wide Consortium), que se encuentra disponible en línea en https://validator.w3.org/ (este compara el documento web con la sintaxis definida para ese lenguaje y reportar cualquier discrepancia encontrada). Y de acuerdo a los resultados obtenidos solicitar al desarrollador de la página web que realice los ajustes acorde a las recomendaciones de implementación de buenas prácticas del W3C.

De igual manera se recomienda usar el validador https://wave.webaim.org, desarrollado por la Universidad Estatal de Utah de los Estados Unidos para evaluar aspectos de accesibilidad de la página web de la Contraloría General de Medellín y solicitar al desarrollador los ajustes correspondientes.

Recomendación 9
En relación a los ítems 4 y 5, de la sección Programación del Código fuente del Anexo 3 de la Resolución 1519 del 2020, sobre "cumplir con los estándares definidos para la integración al Portal Único del Estado Colombiano GOV.CO", se recomienda a la Dirección de Desarrollo Tecnológico, realizar un acompañamiento a la Secretaria General de la CGM, respecto de la sección "4.3.2. Atributos de calidad mínimos de los portales de programas transversales del Estado", haciendo un énfasis especial en el "ítem 4.3.2.3. Seguridad y el ítem 4.3.2.5 Infraestructura tecnológica, del Anexo 4: Guía técnica de integración de portales específicos de programas transversales al portal único del Estado colombiano gov.co" de la Resolución 2893 de 2020, donde se especifican unos requerimientos en seguridad digital de la página web, además de temas de diseño, que también deben ser tenidos en cuenta en los requerimientos para el desarrollador web contratado por la entidad.

Recomendación 10
Referente a la Resolución 1126 de 2021 del MinTIC, del proceso de transición del protocolo IPv4 al IPv6, se recomienda revisar el Acuerdo Marco de Conectividad III, dispuesto por el Ministerio TIC para adquirir el pool de direccionamiento IPv6, que se encuentra en la página web de Colombia Compra Eficiente, así mismo tener presente que el MinTIC dispuso "un equipo de expertos dispuestos a apoyar y resolver permanentemente las dudas del proceso de transición de IPv4 a IPv6 a todas las entidades que lo soliciten, por medio de los correos: soporteccc@mintic.gov.co , fcontre@mintic.gov.co , jtorres@mintic.gov.co" .

Además, es imprescindible que la Dirección de Desarrollo Tecnológico gestione de carácter urgente los recursos necesarios para implementar el "Plan de Transición del Protocolo IPv4 A IPv6" desarrollado por la entidad, teniendo presente que según la resolución citada anteriormente las entidades territoriales "deberán culminar el proceso de transición al protocolo IPv6 en convivencia con el protocolo IPv4 a más tardar el 31 de diciembre del año 2022". Debido a la premura con la que se requiere dar cumplimiento a la resolución, es importante revisar con otras Entidades de Gobierno que hayan implementado el protocolo IPv6, como desarrollaron el proceso, para aprovechar esos conocimientos y poder acotar tiempos.

Recomendación 11

Es necesario seleccionar al menos dos funcionarios adscritos a la Dirección de Desarrollo Tecnológico, los cuales tengan como responsabilidad verificar que la dependencia si avance en dar cumplimiento a los requerimientos de la normatividad vigente que compete a esta área, para que no se vuelvan a presentar retrasos en procesos que afecten la entidad, debido a cambios generados en el cargo de Director Administrativo de la Dirección de Desarrollo Tecnológico.

CONCLUSIÓN

La innovación constante en la tecnología que nos rodea, implican para las entidades públicas el cumplimiento de nuevas normatividades, que buscan garantizar esas condiciones en seguridad digital para salvaguardar los activos de información y propiciar las condiciones necesarias para que cada una de las organizaciones del Estado tenga una adecua interacción con la ciudadanía, que facilite el acceso a la información. Es de anotar que las entidades públicas se ven en la necesidad de adoptar no solo procesos de renovación en hardware y software, sino que estos cambios permanentes involucran una gestión constante en riesgos de: seguridad digital, seguridad y privacidad de la información; además de un alto compromiso por parte de los funcionarios encargados de implementar dichos cambios dentro de la organización para que estos se materialicen.

Es así, como durante esta Evaluación Independiente a las medidas establecidas por la Dirección de Desarrollo Tecnológico de la CGM, para dar cumplimiento a las Condiciones Mínimas Técnicas y de Seguridad Digital solicitadas por el MinTIC en el Anexo 3 de la Resolución 1519 del 2020, se pudo evidenciar el cumplimiento de los requerimientos solicitados en dicho anexo, hallando también algunas oportunidades de mejora, para fortalecer unos procesos respecto a la gestión de riesgos, que se generan a partir de las condiciones de seguridad de los softwares proveídos por terceros.

Cabe resaltar que durante la auditoria se evidencio el compromiso de la dependencia por propiciar para la Contraloría General de Medellín las mejores condiciones en seguridad digital, así como la disposición para brindar las respuestas y los soportes requeridos para dar cumplimiento al objetivo esta Evaluación Independiente; no obstante se identificaron dificultades para la implementación del proceso de Transición del protocolo IPv4 a IPv6 de la Resolución 1126 de 2021; por lo cual es necesario que se adopten las medidas de mejora y se procure con la mayor celeridad dar cumplimiento a esta resolución, puesto que el plazo vence el 31 de diciembre de 2022, y “entre las consecuencias de la no oportuna adopción del protocolo IPv6 están la desconexión de los servicios de internet o, en su defecto, un internet limitado para las entidades que hagan caso omiso a su despliegue, además de las sanciones establecidas en el Artículo 6 de la Resolución 2710 de 2017”.

Además, frente a la implementación del Modelo de Seguridad y Privacidad de la Información en la entidad se generó la alerta de fortalecer el aporte de evidencias que requiere el proceso de autodiagnóstico, para lograr obtener unas bases

adecuadas que garanticen una idónea planeación de acuerdo a las necesidades de la entidad, sin embargo es de resaltar el interés y la disposición para avanzar en la implantación por parte del personal de dependencia de Desarrollo Tecnológico.