29 de noviembre de 2024

1050001-2024-0512

NOMBRE DEL INFORME

38. SEGUIMIENTO ESTRATEGIA DE GOBIERNO Y SEGURIDAD DIGITAL – DECRETO 1008 DE 2018 MINTIC, MIPG, RESOLUCIONES 1164/2020 y 0813/2022

Dirigido a

Dr. DANIEL JOAQUIN RODRIGUEZ MORALES, Gerente de Tecnología
Dr. ANDRÉS FRANCISCO BOADA ICABUCO, Director Servicios de Informática

María Nohemí Perdomo Ramírez
Jefe Oficina de Control Interno y Gestión

Edwin Fernando Bermúdez Mahecha
Líder del Seguimiento / Informe de Ley

Carlos Henry Tellez Mora
Equipo de Seguimiento / Informe de Ley

CONTENIDO

1. OBJETIVO

Evaluar la gestión de implementación de la Política de Gobierno Digital en la EAAB-ESP, para dar cumplimiento a los lineamientos establecidos en la normatividad aplicable.

2. ALCANCE

Este seguimiento evaluó la gestión y cumplimiento de los lineamientos definidos para la implementación de la Política de Gobierno Digital en la EAAB – E.S.P., a fecha de corte 31 octubre de 2024.

3. CRITERIOS

- Normatividad vigente externa e interna
- Autodiagnóstico Departamento Administrativo de la Función Pública – DAFP o Formulario Único de Reporte de Avance de Gestión - FURAG 2021
- Recomendaciones MINTIC resultados FURAG 2021 o Planes de acción definidos para Gobierno Digital y Plan Maestro de Tecnología o Modificaciones a los Planes y sus justificaciones.
- Informe de Seguimiento y Evaluación a la implementación MIPG EAAB-ESP 2022 o Documentación soporte publicada en la herramienta GRC Archer para el Plan de Gobierno
- Digital MIPG 2022 o Presentación modificaciones Plan Maestro de Tecnología (PMT) 2022 Comité Institucional de Gestión y Desempeño (CIGD)
- Resultados Índice de Desempeño Institucional (IDI) Formulario Único de Avance a la Gestión -FURAG 2021

Normatividad

- Decreto 1008/2018 Política de Gobierno Digital o Manual de Gobierno Digital – MINTIC
- Política de Gobierno Digital – MINTIC
- Modelo Integrado de Planeación y Gestión – MIPG
- Resolución 1164/2020 Adopción MIPG-CIGD
- Resolución MinTIC 1519 del 2020
- Política de Gestión Gobierno Digital – EAAB-ESP
- Ley 2052 Racionalización de Trámites
- MPEE0305P-05 “Plan de adecuación y sostenibilidad MIPG
- MPEE0300M03-01 “Manual MIPG EAAB E.S.P.”

4. ÁREAS OBJETO DE SEGUIMIENTO O INFORME DE LEY

Gerencia de Tecnología, Dirección Servicios de Informática.

5. DESARROLLO DEL INFORME

En la actualidad, el gobierno digital se presenta como una herramienta clave para mejorar la calidad de vida de los ciudadanos, al fortalecer la confianza pública mediante un Estado más accesible, eficiente e inteligente. El uso de tecnologías de la información y las comunicaciones permite una gestión pública más cercana y transparente, ofreciendo a la ciudadanía acceso rápido y directo a la información y servicios gubernamentales.

Las estrategias de gobierno digital buscan, entre otros objetivos, facilitar el acceso a la información y agilizar los trámites, aumentando la eficiencia del sector público, promoviendo la interoperabilidad entre entidades gubernamentales y estableciendo controles que contribuyan a la prevención de la corrupción. Estos avances permiten una administración más moderna y efectiva.

No obstante, el éxito de estas estrategias depende en gran medida de la seguridad digital, ya que la protección de la información compartida es fundamental para evitar riesgos de vulnerabilidad, robo o mal uso de datos. Por esta razón, las políticas de gobierno y seguridad digital deben ir de la mano, ya que la confianza en el entorno digital es esencial para cumplir con los objetivos de un gobierno más cercano y eficiente.

5.1 Desarrollo del seguimiento

Al interior de la Empresa, la estrategia de Gobierno y Seguridad Digital se encuentra desarrollada a través de la implementación del Modelo Integrado de Planeación y Gestión (MIPG) y cuenta con la ejecución de actividades asociadas a tres planes y dos dimensiones del MIPG, cuyo avance fue verificado a través del aplicativo Archer e información remitida por la Dirección de Servicios de Informática.

5.1.1 MIPG 2024

5.1.1.1 Dimensión Gestión con valores para resultados

5.1.1.1.1 Política de Gobierno Digital

Esta política de Gestión fue revisada en el Comité Institucional de Gestión y Desempeño No. 9 del 18 de diciembre de 2019 y aprobada en el comité corporativo No. 2 de la EAAB el 16 de enero de 2020, creada con el objetivo de promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para facilitar la gestión de la Empresa y acceso a los servicios de la Entidad y mejorar la comunicación con los grupos de interés.

Plan Política de Gobierno Digital

Al inicio de la vigencia 2024 el Plan de Gobierno Digital de la EAAB contaba con 6 ejes temáticos: **i)** Arquitectura Empresarial, **ii)** Cultura y apropiación, **iii)** Estado abierto, **iv)** Servicios Ciudadanos Digitales, **v)** Arquitectura de TI y **vi)** Seguridad y privacidad de la información.

Plan cuya solicitud de modificación fue realizada por la Dirección Servicios de Informática el 14 de junio de 2024 a la Dirección de Calidad y Procesos justificando que de acuerdo con el autodiagnóstico era necesario priorizar temas de acuerdo con las necesidades y capacidades, que permitieran el fortalecimiento institucional en el marco de Gobierno Digital, modificando el Plan de Gobierno Digital 2024 en cuanto a actividades, medios de verificación, fechas, etc.

La nueva versión del Plan de Gobierno Digital tiene establecido 4 ejes temáticos y 8 actividades para su ejecución:
1. Arquitectura de TI
2. Estado Abierto
3. Seguridad y privacidad de la información
4. Servicios Ciudadanos Digitales

A continuación, se describen las actividades establecidas por la Dirección Servicios de Informática con relación al cumplimiento de estos ejes temáticos:

1. Arquitectura de TI

La Arquitectura de TI, busca describir la estructura y las relaciones de todos los elementos de TI de la EAAB-ESP. Se descompone en arquitectura de información, arquitectura de sistemas de información y arquitectura de los servicios de tecnología. Incluye además las arquitecturas de referencia y los elementos estructurales de la estrategia de TI (visión de arquitectura, principios de arquitectura, lineamientos y objetivos estratégicos).

Esta tiene contempladas cuatro actividades:
I) Desarrollar un mecanismo para la gestión de la demanda:

Cuyo fin es fortalecer el análisis y priorización de iniciativas TI/TO gestionadas por la Gerencia de Tecnología, asegurando una mejor evaluación y viabilidad de los proyectos.

Imagen 1. Mecanismo gestión de la demanda
Fuente: Dirección Servicios de Informática

Formulario WEB, que tendría contemplado su diligenciamiento a través de la herramienta Forms, posterior almacenamiento de las respuestas en lista de Sharepoint, tablero de control en Kanban y seguimiento por Power BI.

Siendo esta última herramienta donde se visualiza la cantidad de requerimientos, clasificación de acuerdo con la demanda, enfoque de los requerimientos (nuevos, evolutivos, adquisición o conceptos), porcentaje de avance, requerimientos por desarrollador, detalle y diagrama de Gantt.

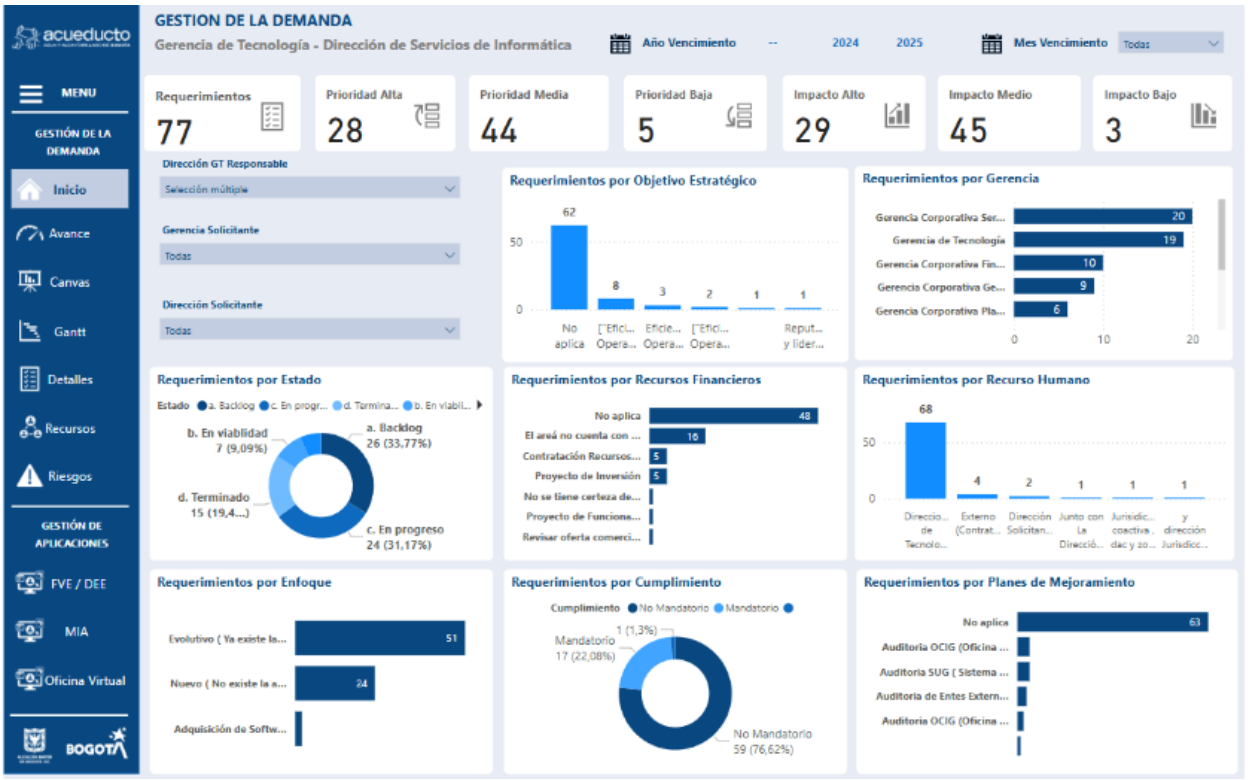

Imagen 2. Tablero Power BI
Fuente: Dirección Servicios de Informática

II) Definir el modelo de plataforma de respaldos de información en la arquitectura TI de la EAAB-ESP:

Esta actividad tiene como objetivo garantizar la integridad y disponibilidad de los datos al establecer una arquitectura de respaldos adecuada que soporte los sistemas de la EAAB-ESP.

Actualmente, la empresa cuenta con una plataforma de protección de datos **NetBackup**, que respalda información de bases de datos, máquinas físicas y virtuales, sistemas operativos, y servidores de archivos tanto de aplicaciones como de usuarios. Esta solución cubre los ambientes de desarrollo, pruebas y producción, abarcando tanto la corta como la larga retención.

La arquitectura propuesta para los respaldos contempla dos soluciones diferenciadas según el tipo de retención:

Corta retención: Se implementarán soluciones de fabricantes con herramientas de alta capacidad de almacenamiento local, lo que permitirá realizar restauraciones rápidas. Estas herramientas también cuentan con funcionalidades que aseguran la protección de la información respaldada y facilitan su integración con la infraestructura de la entidad. El volumen estimado para la corta retención es de 497.5 TB para el año 2028, calculado a partir de la tasa de crecimiento exponencial de los datos.

Larga retención: Actualmente, se utilizan cintas LTO gestionadas a través de librerías de respaldo Oracle y un procedimiento de custodia de información con una compañía externa. Sin embargo, las limitaciones de velocidad de acceso y la capacidad de almacenamiento de las cintas LTO han motivado la exploración de opciones más eficientes, como el almacenamiento en la nube o el almacenamiento por software. Estas alternativas ofrecerían ventajas en términos de rendimiento, escalabilidad y acceso rápido a la información. El volumen estimado para la larga retención es de 214 TB para el año 2018.

III) Definir el Catálogo de servicios de TI/TO de la gerencia de Tecnología:

El definir el catálogo de servicios permitirá la gestión del ciclo de vida de cada uno de los servicios alineados a la planeación estratégica, evaluación y mejora continua, permitiendo la rápida incorporación de nuevos servicios acorde a las necesidades cambiantes del negocio. Permitiendo a los usuarios de TI y TO, conocer los servicios activos y procesos que soporta cada una de las Direcciones de la Gerencia de Tecnología.

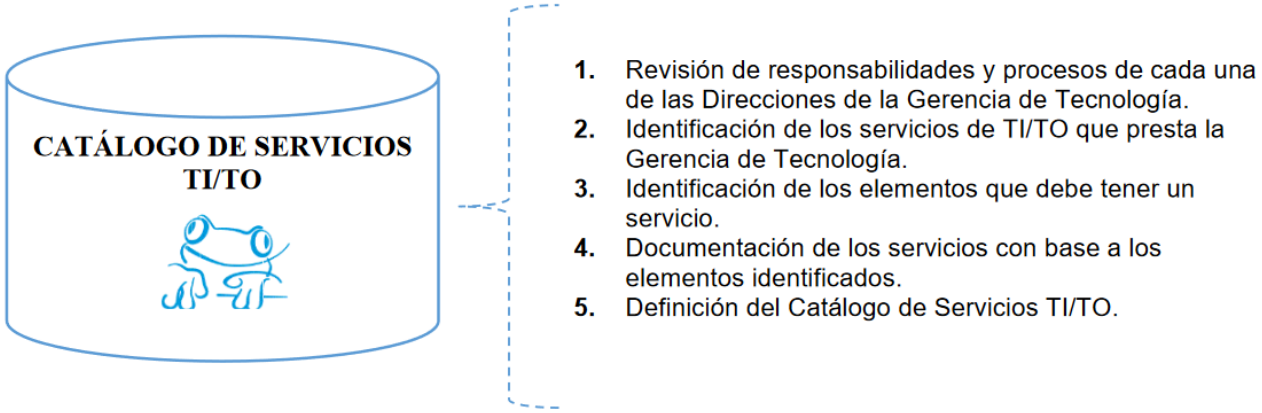

Imagen 3. Pasos para la Definición del Catálogo de Servicios de TI/TO
Fuente: Dirección Servicios de Informática

Definición que ha considera los siguientes elementos:

- Identificación de los servicios prestados.

- Identificación procesos del negocio que son soportados con los servicios de TI/TO y responsables de gestionarlos.
- Identificación usuarios internos, externos y/o grupo específico que hace uso del servicio.
- Identificación de los funcionarios responsables y técnicos de los servicios.
- Identificación de los Acuerdos de Nivel de Servicio asociados a cada servicio y los Acuerdos Nivel Operacional.

Catalogo que actualmente se está documento en la herramienta Sharepoint y export a través de Excel.

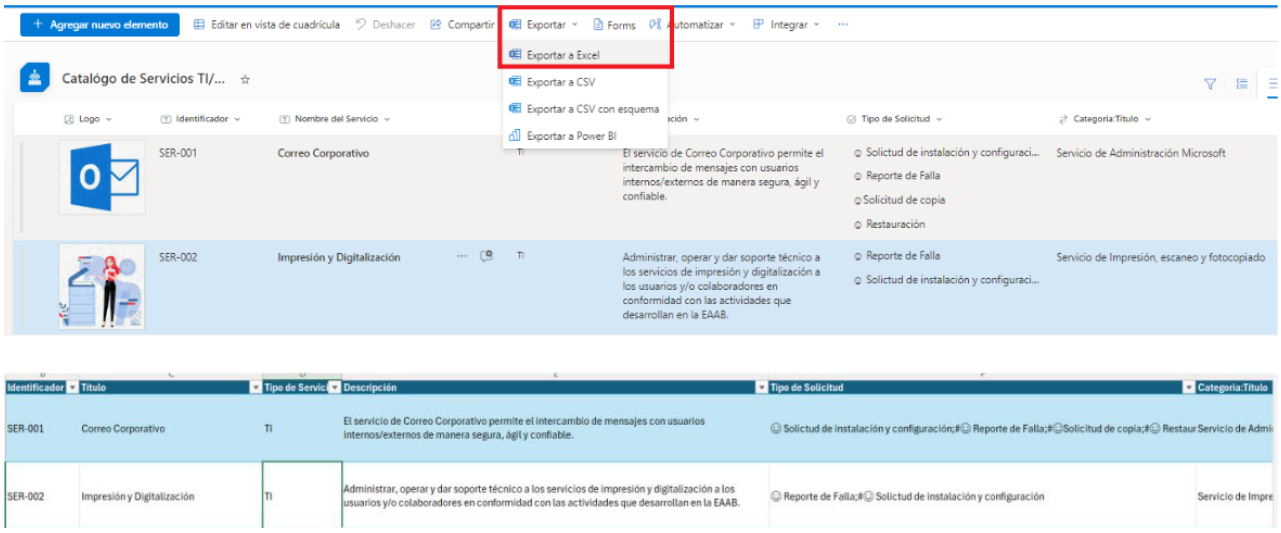

Imagen 4. Export del Catálogo de Servicios
Fuente: Dirección Servicios de Informática

IV) Fortalecer los ambientes pre-productivos para los sistemas de información, a través de la identificación de los componentes críticos que se registrarán en el catálogo:

Este catálogo está disponible a través de la herramienta de TI (BMC Digital WorkPlace), la cual permite a los usuarios internos registrar incidentes, realizar requerimientos, consultar la base de datos y hacer seguimiento a los casos.

El catálogo incluye varios tipos de servicios clasificados en categorías como: Aplicaciones de Negocio, Herramientas, Equipos de Cómputo, Aplicaciones Ofimáticas, Servicios de Red, Servicios de Seguridad Informática, Diseño del Servicio y Capacidad. Cada categoría está orientada a apoyar diferentes áreas funcionales de la empresa y está definida por un Acuerdo de Nivel de Servicio (ANS), que establece la disponibilidad y el tiempo de respuesta para la atención de incidentes y requerimientos, con metas de efectividad de al menos el 98%.

Las Aplicaciones de Negocio son servicios orientados directamente a los procesos de negocio de la EAAB-ESP y se priorizan según su impacto. Estas aplicaciones se dividen en Críticas, Altas y Medias, con horarios de servicio definidos en los ANS. De manera similar, los Servicios de Red y Herramientas son clasificados por su impacto en los procesos de negocio y se gestionan bajo los mismos principios, asegurando su disponibilidad mediante la atención de incidentes y solicitudes.

Además, la Seguridad Informática es una categoría clave dentro del catálogo, que incluye servicios como respaldo de información, antivirus, bloqueo de páginas web y asesoría en temas de seguridad. Otros servicios como Equipos de Cómputo y Capacidad también están detallados en el catálogo, donde los usuarios pueden solicitar equipos, recursos de infraestructura o diseño de nuevos servicios informáticos, garantizando así que los servicios tecnológicos estén

alineados con las necesidades del negocio y la capacidad tecnológica de la organización. Todos estos servicios se gestionan a través de la Mesa de Servicios, que actúa como punto único de contacto para la atención y seguimiento de las solicitudes.

2. Estado Abierto

El Estado Abierto, busca promover la transparencia en la gestión pública con un enfoque de apertura por defecto, y el fortalecimiento de escenarios de dialogo que promuevan la confianza social e institucional "Estrategias de Ciudades y Territorios Inteligentes".

Un aspecto clave de este eje temático es la actividad de “Definir el mecanismo de envió automático de información Geográficos a IDECA” el cual está relacionado con el flujo de datos provenientes del SIGUE (Sistema de Información Geográfico Unificado Empresarial) de la Empresa de Acueducto y Alcantarillado de Bogotá.

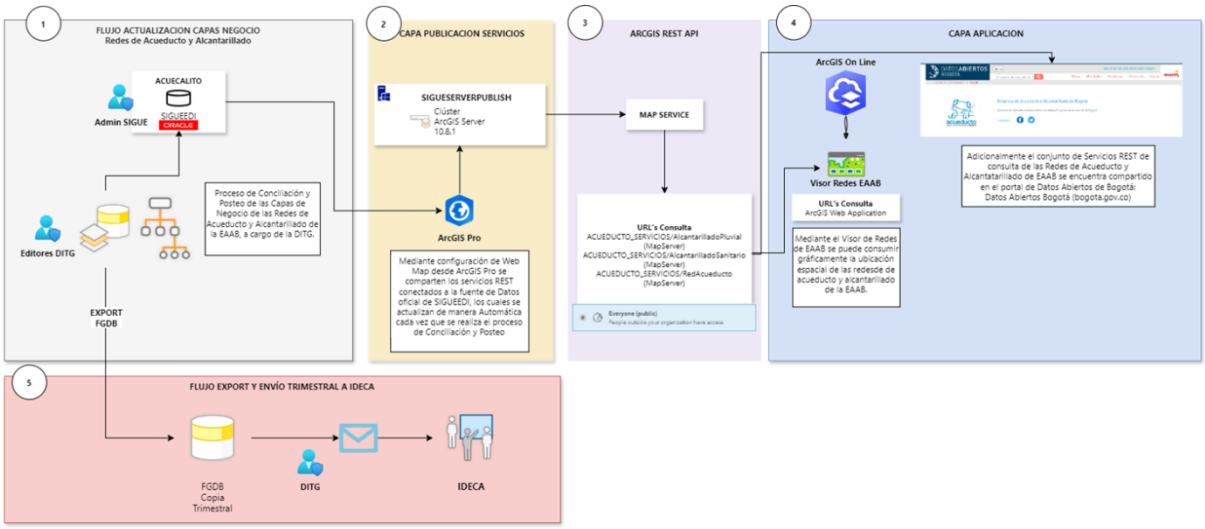

Imagen 5. Flujo de datos que se comparten con la plataforma de Datos Abiertos de IDECA
Fuente: Dirección Servicios de Informática

El proceso de actualización y envío de los datos geográficos comienza con la actualización de las **Capas Geográficas de Negocio**, que contienen la ubicación espacial de las redes de acueducto, alcantarillado pluvial y sanitario. Los datos son trabajados por el Grupo de Editores de la Dirección de Información Técnica y Geográfica (DITG) sobre bases de datos locales y luego enviados a la interlocutora del Sistema de Información Geográfico Unificado Empresarial (SIGUE) para su validación. Una vez verificados, se cargan en la **Enterprise Geodatabase (EGDB) de SIGUEEDI**. Cuando la información cumple con los estándares de calidad y consistencia, se procede a la conciliación y posteo a la versión Default de la EGDB.

Los datos geográficos actualizados son compartidos a través de servicios geográficos creados en la herramienta **ArcGIS Pro** y configurados con la Interfaz de Programación de Aplicaciones basada en Transferencia de Estado Representacional (API REST) de ArcGIS. Estos servicios permiten que la información de las redes se exponga públicamente, a través de varias URL disponibles y pueda ser consultada de manera interna y externa. Además, los datos se comparten a través de un **Visor Geográfico de Redes en ArcGIS Online** y en el Portal de Datos Abiertos de Bogotá, donde están disponibles para el público en general.

Adicionalmente, existe un flujo alterno de información que permite la extracción trimestral de los **Features Dataset** o "Conjunto de Datos de Características" de la EGDB de SIGUEEDI, los cuales se envían a los usuarios definidos por IDECA en una File Geodatabase a través de correo electrónico. Cabe destacar que cada vez que se actualizan los

datos de la EGDB y se realiza la conciliación y posteo, los servicios REST se actualizan automáticamente, garantizando que la información expuesta esté siempre al día con la última edición conciliada.

3. Seguridad y privacidad de la información

Con este eje temático se busca que las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general en todos los activos de información de las entidades del estado, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

En relación con este eje se observa en el diagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) el análisis del estado actual de la entidad y nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información

A continuación, se presenta el resultado de la evaluación realizada por MINTIC a los controles:

No.	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	90	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	73	100	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	63	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	76	100	GESTIONADO
A.9	CONTROL DE ACCESO	82	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	40	100	REPETIBLE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	73	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	84	100	OPTIMIZADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	79	100	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	57	100	EFECTIVO
A.15	RELACIONES CON LOS PROVEEDORES	60	100	EFECTIVO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	86	100	OPTIMIZADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	57	100	EFECTIVO
A.18	CUMPLIMIENTO	63,5	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		**70**	**100**	GESTIONADO

Tabla 1. Evaluación de efectividad de controles
Fuente: MSPI MINTIC 2024

Siendo la calificación más baja el dominio técnico de criptografía con una calificación de 40 sobre 100.

Revisión que comprendía los siguientes instrumentos de evaluación:

- **Criptografía:** Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización Garantizar la seguridad del teletrabajo y el uso de los dispositivos móviles
- **Controles criptográficos:** Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.
- **Política sobre el uso de controles criptográficos:** Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.

- **Gestión de llaves:** Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.

4. Servicios Ciudadanos Digitales

Este eje temático busca brindar las capacidades necesarias para garantizar el adecuado flujo de información e interacción entre los sistemas de información de las entidades, permitiendo el intercambio, la integración e intercambio de información, con el propósito de facilitar el ejercicio de sus funciones constitucionales y legales, acorde con los lineamientos del Marco de Interoperabilidad.

La actividad estipulada para este eje temático es “Definir la Arquitectura TI de Interoperabilidad entre sistemas de información de la EAAB-ESP.” y su gestión se encuentra detallada en el informe de arquitectura TI de interoperabilidad entre sistemas de información de la EAAB E.S.P.

Este informe contiene el detalle de los lineamientos para la creación de servicios y bases para el desarrollo y operación de aplicaciones distribuidas y basadas en la Web, así como la adopción e integración de los principios de DevSecOps en cada etapa del ciclo de vida del desarrollo de software para asegurar que las aplicaciones y servicios se construyan en un entorno de seguridad.

Infraestructura en la Nube y en Local (On-Premise)
La Empresa de Acueducto y Alcantarillado de Bogotá (EAAB) ha decidido utilizar una infraestructura tecnológica híbrida que combina soluciones en la nube y en sus instalaciones locales, con el objetivo de mejorar la eficiencia, seguridad y escalabilidad de sus servicios.

Uso de la Nube Azure
La EAAB planea implementar una infraestructura en la nube utilizando Azure, que es una plataforma ofrecida por Microsoft. Azure proporcionará herramientas avanzadas que permitirán a la EAAB gestionar y desarrollar servicios de manera más flexible y eficiente. Entre los servicios que se utilizarán se incluyen:

- **Azure API Management:** Una herramienta para gestionar cómo los diferentes servicios y aplicaciones se comunican entre sí.
- **Azure Kubernetes Service (AKS):** Ayudará a organizar y administrar aplicaciones que se ejecutan en contenedores, facilitando su despliegue y escalabilidad.
- **Azure DevOps:** Una plataforma que apoya en la planificación, desarrollo, prueba y despliegue de software, haciendo más ágil el proceso de creación de nuevas funcionalidades y servicios.

Infraestructura Local (On-Premise)
Para garantizar la seguridad y disponibilidad de los servicios, la EAAB también utilizará recursos tecnológicos que se encuentran dentro de sus instalaciones. Estos son:

1. **Oracle OLCNE:** Es una solución que ayuda a gestionar aplicaciones que se ejecutan dentro de contenedores en sus servidores locales, mejorando la eficiencia.
2. **VMware Tanzu:** Esta plataforma ayudará a coordinar y gestionar esos contenedores, asegurando que todo funcione de manera ordenada y eficiente.
3. **Servidores de Aplicaciones:** La EAAB utilizará varios servidores para gestionar las aplicaciones que ejecutan los servicios, tales como:
   a. IIS (Internet Information Services)
   b. Apache HTTP Server
   c. Apache Tomcat
   d. IBM WebSphere Application Server

Integración de DevSecOps
La EAAB también integrará un enfoque de seguridad dentro del proceso de desarrollo de sus servicios, conocido como DevSecOps. Este enfoque asegura que la seguridad no sea algo que se revise solo al final, sino que esté presente desde las primeras etapas del desarrollo hasta la implementación final y operación de los servicios, reduciendo riesgos y vulnerabilidades.

Alta Disponibilidad y Escalabilidad
La infraestructura de la EAAB se diseñará para garantizar que sus servicios estén siempre disponibles, incluso en caso de fallos o problemas técnicos. Para ello, se utilizarán clústeres de servidores tanto en la nube como en las instalaciones locales. Esto permitirá distribuir las cargas de trabajo de manera eficiente y garantizar que los servicios se mantengan operativos en todo momento. Además, se implementarán estrategias avanzadas de recuperación ante desastres y se utilizarán contenedores para mejorar la capacidad de los sistemas de adaptarse a cambios y crecer según las necesidades.

5.1.1.2 Dimensión Decreto 612

5.1.1.2.1 Plan de Seguridad y Privacidad de la Información

Este plan se ejecuta a través de 4 ejes temáticos, cada uno de ellos con actividades definidas y susceptibles de verificación de avance en el aplicativo ARCHER. Los ejes temáticos son:
1. Gestión de Continuidad del Negocio
2. Gestión de Incidentes
3. Política de Seguridad de la Información
4. Seguridad de las operaciones

A continuación, se describen las actividades establecidas por la Dirección Servicios de Informática con relación al cumplimiento de estos ejes temáticos:

1. Gestión de Continuidad del Negocio

Este eje temático tiene asociadas dos actividades:

Ejecutar pruebas de recuperación a un (1) sistema crítico:
Actividad eliminada en la sesión N°15 del Comité Corporativo de la Empresa realizado el 29 de agosto de 2024.

Realizar un autodiagnóstico de los controles de seguridad definidos en la norma técnica ISO 27001:2022:
Esta actividad se encuentra programada para su desarrollo durante noviembre de 2024, a la fecha de realización de este seguimiento aún no se cuenta con soporte documental o evidencia verificable del avance de esta.

2. Gestión de Incidentes,

Este eje temático tiene asociada la actividad de **Planificar y ejecutar un simulacro de amenaza de ciberseguridad controlada.**

Actividad que se encuentra programada para su desarrollo durante noviembre de 2024, a la fecha de realización de este seguimiento no se cuenta con soporte documental o evidencia verificable del avance de esta.

3. Política de seguridad de la Información

Este eje temático cuenta con una actividad asociada:

Sensibilizar en las temáticas de seguridad digital:
En el aplicativo ARCHER se reporta la proyección de ejecución de la actividad; en la Escuela de Formación Virtual donde ya se encuentra disponible el curso Protección de Datos Personales, como se reportó en el autocontrol realizado en agosto de 2024 en el cual se manifiesta el aprovechamiento de esta herramienta, además de la invitación a participar del curso a través del correo electrónico institucional.

4. Seguridad de las Operaciones

Este último eje temático contaba con la actividad de 'Gestionar análisis de vulnerabilidades ante algunas instancias de ciberseguridad del gobierno nacional', actividad que fue eliminada en la sesión N°15 del Comité Corporativo de la Empresa realizado el 29 de agosto de 2024.

5.1.1.2.2 Plan de tratamiento de riesgos de Seguridad y Privacidad de la Información

Este plan se ejecuta a través de 1 eje temático, el cual tiene una actividad definida y susceptible de verificación de avance en el aplicativo ARCHER.

El eje temático se denomina Seguridad de las operaciones, el cual tiene asociada una actividad:

1. Capacitar a los líderes de procesos en la identificación de riesgos de la seguridad y privacidad de la información.

Respecto a la actividad propuesta, la Dirección Servicios de Informática solicito modificación el 14 de junio de 2024, modificando actividad, medios de verificación, fechas, entre otros. Estableciendo como nuevo plazo de ejecución el período del 1 al 30 de noviembre de 2024, al revisar el soporte de ejecución de esta actividad se observó 47 documentos entre los que se cuenta con 42 ayudas de memoria de reuniones con diferentes áreas cuyo tema corresponde a la 'Actualización de Activos de Información'. Sin embargo, el medio de verificación y evidencia aportada no corresponde a la actividad propuesta.

5.1.2 Índice de Desempeño Institucional

Verificados los resultados de la Medición del Desempeño Institucional correspondiente a la vigencia 2023, se encontró lo siguiente:

Para la vigencia 2023 la Dimensión 3 de MIPG Gestión para resultados con valores, se identifican las políticas 7 Gobierno Digital y 8 Seguridad Digital cuyos resultados se relacionan a continuación:

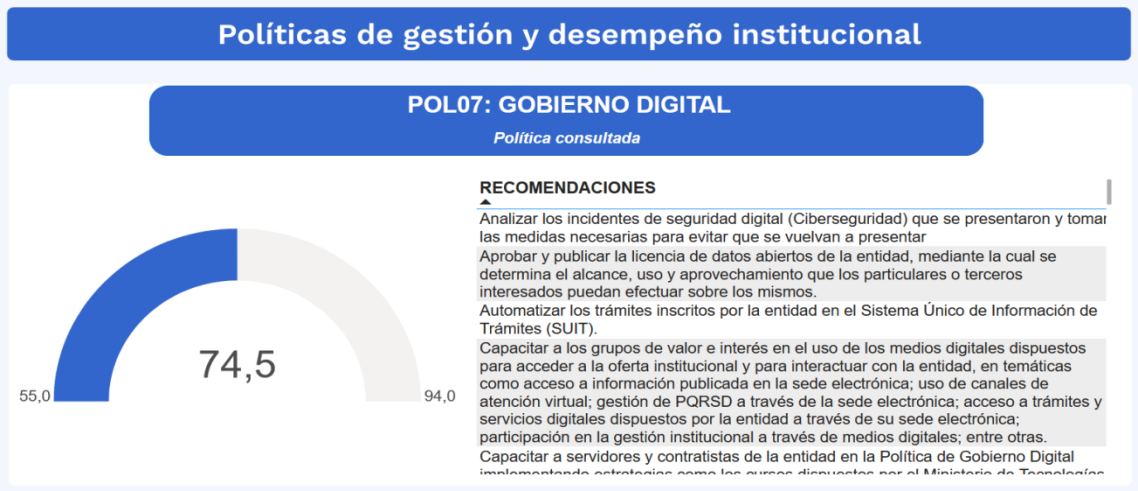

Imagen 6. Política 7 Gobierno Digital
Fuente: https://www1.funcionpublica.gov.co/web/mipg/resultados-medicion

En la Imagen 7 se observa que el resultado obtenido es de 74,5, sin embargo, el valor de referencia del grupo par de comparación es de 94,0; este resultado corresponde a las valoraciones más bajas dentro de la dimensión Gestión para resultados con valor; adicionalmente, se realizaron más de 50 recomendaciones asociadas a la política de Gobierno Digital.

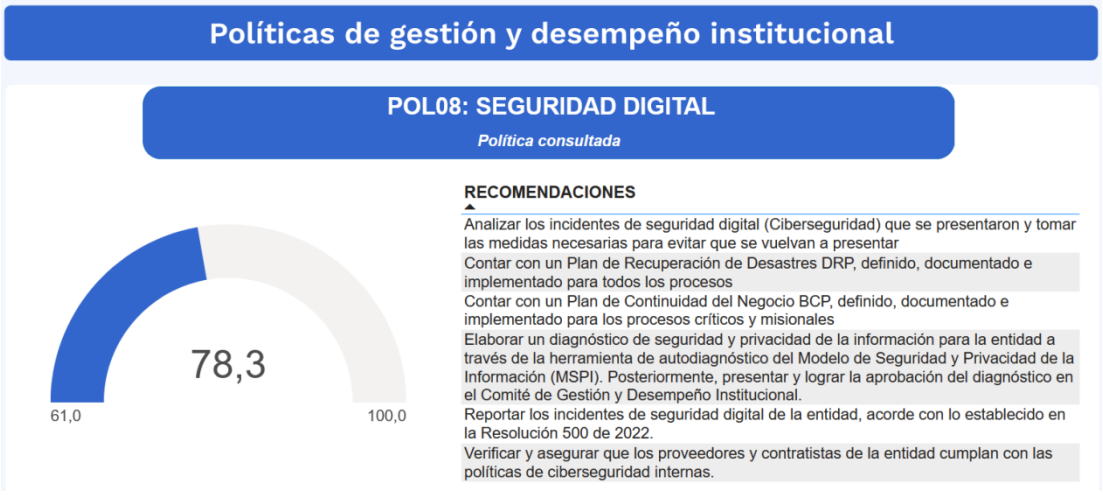

Imagen 8. Política 8 Seguridad Digital
Fuente: https://www1.funcionpublica.gov.co/web/mipg/resultados-medicion

En la Imagen 8 se observa que el resultado obtenido es de 78,3, sin embargo, el valor de referencia del grupo par de comparación es de 100,0; este resultado corresponde a las valoraciones más bajas dentro de la dimensión Gestión para resultados con valor; adicionalmente, de esta valoración del desempeño institucional del informe del Departamento Administrativo de la Función Pública (DAFP) se realizaron 6 recomendaciones a la Empresa asociadas a la política de Seguridad Digital.

5.2 Comunicaciones de alertas tempranas

Durante el seguimiento no se emitieron comunicaciones de alertas tempranas

6. RESULTADOS

6.1 FORTALEZAS

- ✓ **Desarrollo Integral del Modelo de Gobierno Digital:** La empresa ha implementado el Modelo Integrado de Planeación y Gestión (MIPG), con actividades bien estructuradas en áreas clave como Arquitectura de TI,

Seguridad y Privacidad de la Información, y Servicios Ciudadanos Digitales, lo que demuestra un enfoque integral para fortalecer su infraestructura tecnológica.

- ✓ **Transparencia y Gestión Abierta:** El eje de "Estado Abierto" promueve la transparencia, facilitando el acceso público a datos geográficos actualizados a través de plataformas como IDECA y ArcGIS, lo que fortalece la confianza social e institucional.

6.2 OBSERVACIONES

En el desarrollo del seguimiento correspondiente no se generaron observaciones

6.3 RECOMENDACIONES

No.	RECOMENDACIONES GENERALES	RESPONSABLE(S)
1	Se recomienda fortalecer la implementación de actividades programadas y seguimiento a los avances mediante la creación de cronogramas detallados con plazos concretos y documentación de avances en tiempo real.	Dirección Servicios de Informática
2	Se sugiere trabajar en las recomendaciones efectuadas en la medición del desempeño institucional del Departamento Administrativo de la Función Pública asociadas a las políticas 7 y 8 de la Dimensión 3 de MIPG.	Dirección Servicios de Informática
3	Se sugiere validar el medio de verificación propuesto e información cargada en la herramienta de seguimiento y control Archer de manera que esta coincida.	Dirección Servicios de Informática
4	Se recomienda mejorar la capacitación en seguridad informática, enfocándose particularmente en la implementación de controles criptográficos y la gestión de llaves, ya que los resultados de la evaluación del MSPI indicaron debilidades en estas áreas. Adicionalmente, se debería avanzar con la actualización y ejecución de las actividades relacionadas con la protección de la información, como los simulacros de amenazas cibernéticas, para asegurar que la entidad esté preparada ante posibles riesgos.	Dirección Servicios de Informática

Firmado por EDWIN FERNANDO BERMUDEZ MAHECHA
el 29/11/2024 a las 11:36:13 COT

Edwin Fernando Bermúdez Mahecha
Líder Seguimiento / Informe de Ley

Firmado por MARIA NOHEMI PERDOMO RAMIREZ
el 29/11/2024 a las 12:53:32 COT

María Nohemí Perdomo Ramírez
Jefe Oficina Control Interno y Gestión