|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **FECHA DE EMISIÓN DEL INFORME** | **DÍA** | 31 | **MES** | 08 | **AÑO** | 2022 |
| **PROCESO, PROCEDIMIENTO O ACTIVIDAD EVALUADA** | Política de Gobierno Digital | | | | | |
| **RESPONSABLE DEL PROCESO, PROCEDIMIENTO O ACTIVIDAD EVALUADA** | Subdirección de Gestión Corporativa | | | | | |
| **OBJETIVO GENERAL** | Verificar el avance en la implementación de la Política de Gobierno Digital en el IDPC | | | | | |
| **ALCANCE** | Primer Semestre de 2022 | | | | | |
| **CRITERIOS** | * Ley 1341 de 2009 “Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones” * Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales” * 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 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" * Manual de Gobierno Digital – MinTIC. * Guía sobre el tratamiento de datos personales en las entidades estatales – Superintendencia de Industria y Comercio. * Demás normatividad interna y externa relacionada con el objetivo del seguimiento | | | | | |
| **PRUEBAS DE AUDITORÍA** | Verificación documental y de sistemas de información | | | | | |
| **EQUIPO AUDITOR** | Eleana Marcela Páez Urrego | | | | | |
| **FECHA DE EJECUCIÓN DE LA AUDITORÍA** | Del 19 de julio al 31 de agosto de 2022 | | | | | |
| **INSUMOS** | Los resultados se fundamentan en la información entregada por la Subdirección de Gestión Corporativa el 26 de julio de 2022 con radicado 20225400102503. | | | | | |
| **LIMITACIONES DE LA EVALUACIÓN Y/O SEGUIMIENTO** | La evaluación se basa únicamente en el cumplimiento normativo, ya que, no se cuenta con personal experto que pueda realizar una evaluación a profundidad de la política. | | | | | |

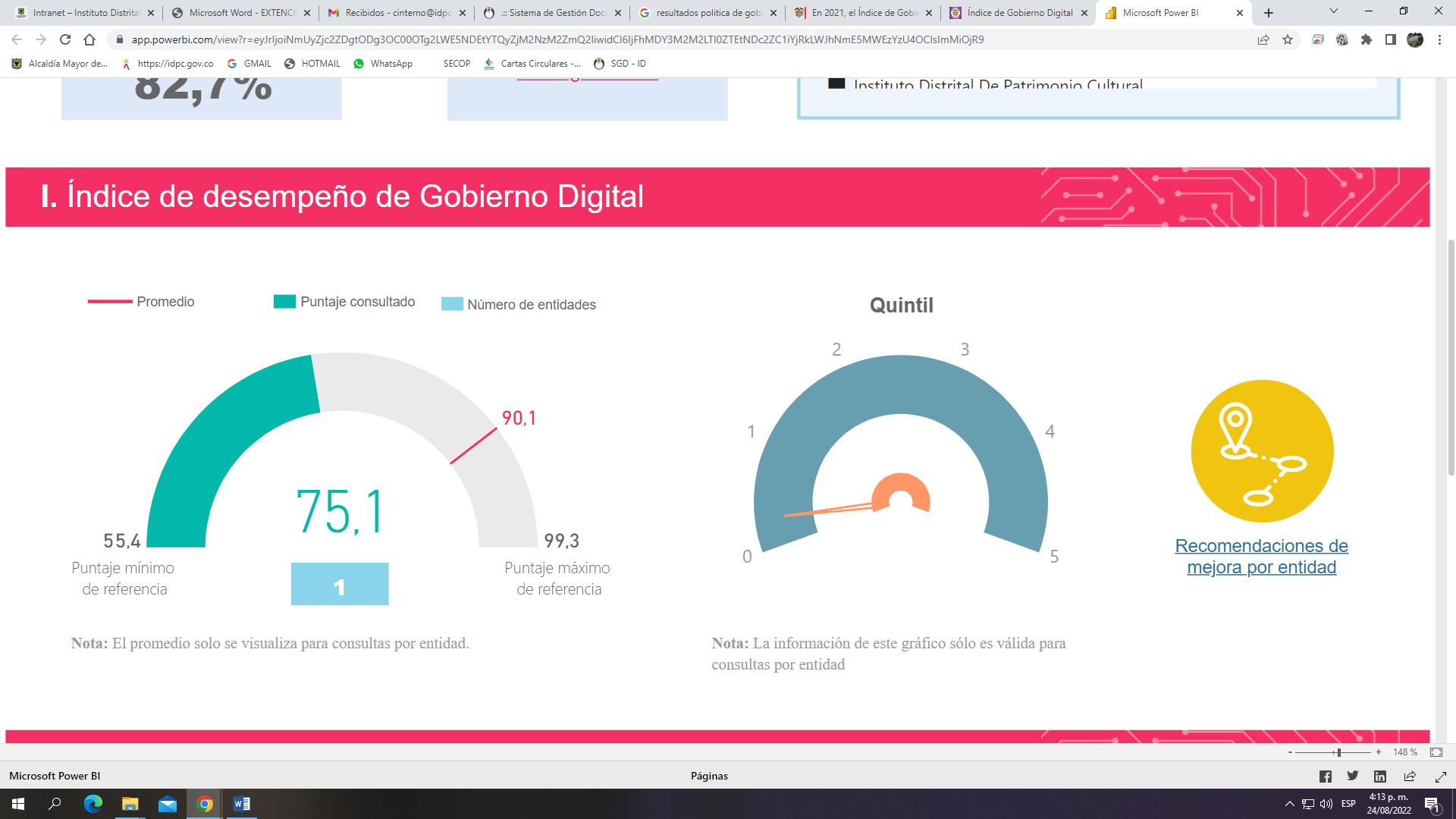
1. **RESULTADOS DE LA EVALUACIÓN Y/O SEGUIMIENTO**

El presente informe contiene los resultados y recomendaciones del FURAG en cuanto a la política Gobierno Digital, la revisión del Modelo de Seguridad y Privacidad de la Información, de protección de datos personales y de activos de información.

* 1. **RESULTADOS Y RECOMENDACIONES FURAG**

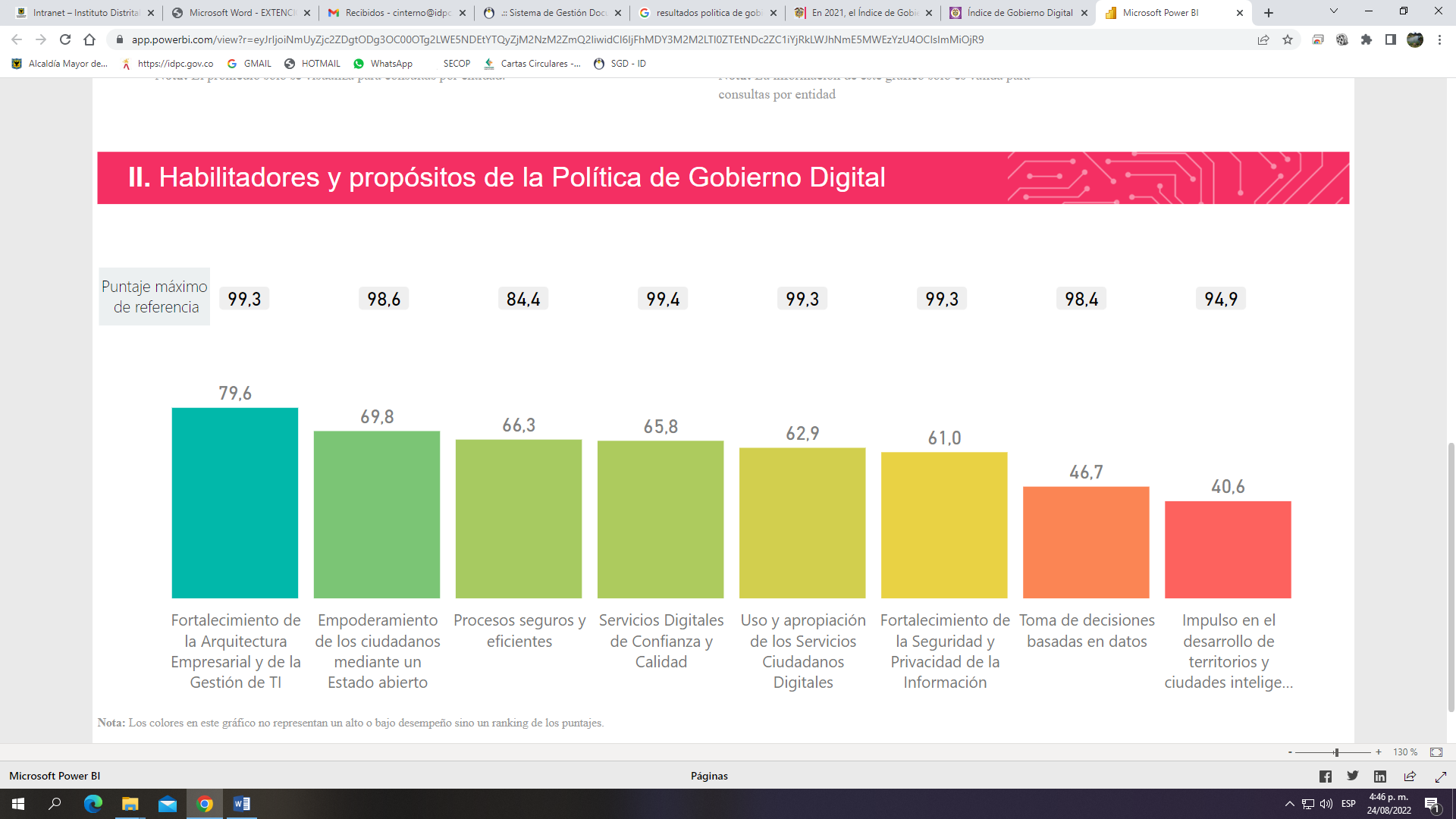
De acuerdo con lo reportado por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC en los resultados de Gobierno Digital 2021, la Entidad cuenta con un puntaje de 75.1 en el Índice de Gobierno Digital (Gráfico 1), donde los habilitadores con puntajes inferiores a 50 son toma de decisiones basadas en datos e impulso en el desarrollo de territorios y ciudades inteligentes (Gráfico 2).

**Gráfico 1.** Índice de Desempeño Institucional de Gobierno Digital



**Fuente:** Resultados de Gobierno Digital 2021, MinTIC

**Gráfico 2**. Habilitadores y propósitos de la Política de Gobierno Digital



**Fuente:** Resultados de Gobierno Digital 2021, MinTIC

En este mismo sentido, MinTIC generó algunas recomendaciones para cada uno de los habilitadores y propósitos (tabla 1), las cuales fueron comparadas con el PETI y Plan de Seguridad de la Información, con el fin de garantizar que las mismas hayan sido tenidas en cuenta para la mejora del índice de gobierno digital.

**Tabla 1.** Comparación recomendaciones Gobierno Digital Vs. Actividades programadas IDPC

| **Habilitador o propósito** | **Recomendación** | **Actividad programada IDPC** |
| --- | --- | --- |
| Fortalecimiento de la arquitectura empresarial y de la gestión de TI | Aplicar una metodología para la gestión de proyectos de TI de la entidad, que incluya seguimiento y control a las fichas de proyecto a través de indicadores. | Avanzar en la implementación del dominio de uso y apropiación del Modelo de Arquitectura Empresarial (MRAE) con el fin de desarrollar una cultura que permita la adopción y uso de la tecnología en el IDPC |
| Definir herramientas tecnológicas para la gestión de proyectos de TI de la entidad. |
| Actualizar el catálogo de componentes de información. |
| Actualizar las vistas de información de la arquitectura de información para todas las fuentes. |
| Implementar procesos o procedimientos que aseguren la integridad, disponibilidad y confidencialidad de los datos para mejorar la gestión de los componentes de información de la entidad. |
| Incluir características en los sistemas de información de la entidad que permitan la apertura de sus datos de forma automática y segura. |
| Definir el esquema de soporte y mantenimiento de los sistemas de información, aprobarlo mediante el comité de gestión y desempeño institucional, implementarlo y actualizarlo mediante un proceso de mejora continua de acuerdo con los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones. |
| Implementar un plan de aseguramiento de la calidad durante el ciclo de vida de los sistemas de información que incluya criterios funcionales y no funcionales. |
| Definir y aplicar una guía de estilo en el desarrollo de los sistemas de información de la entidad e incorporar los lineamientos de usabilidad definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones. |
| Actualizar visitas de despliegue, conectividad y almacenamiento de la arquitectura de infraestructura de TI de la entidad. |
| Documentar e implementar un plan de continuidad de los servicios tecnológicos mediante pruebas y verificaciones acordes a las necesidades de la entidad. |
| Implementar una estrategia de uso y apropiación para todos los proyectos de TI teniendo en cuenta estrategias de gestión del cambio para mejorar el uso y apropiación de las tecnologías de la información (TI) en la entidad. |
| Hacer uso de contratos de Asociaciones Público Privadas (APP) relacionados con Tecnologías de la Información y las Comunicaciones. |
| Fortalecimiento de la seguridad y privacidad de la información | Identificar los riesgos de seguridad y privacidad de la información de la entidad, aprobarlos mediante el comité de gestión y desempeño institucional, valorarlos y actualizarlos mediante un proceso de mejora continua. | Actualizar los lineamientos y políticas del Modelo de Privacidad y Seguridad de la Información con el fin de garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad.  Evaluar el estado de implementación del Sistema General de Seguridad de la Información.  Gestionar los riesgos de seguridad de la Información del IDPC. |
| Uso y apropiación de los servicios ciudadanos digitales | Utilizar la plataforma de interoperabilidad (PDI) para los servicios de la entidad. | No se encuentra |
| Utilizar el estándar de lenguaje común de intercambio de información para los servicios de la entidad. |
| Certificar los servicios de la entidad en el uso del estándar de lenguaje común de intercambio de información. |
| Utilizar la plataforma de interoperabilidad (PDI) para los servicios de la entidad que están certificados en el uso del estándar de lenguaje común de intercambio de información. |
| Servicios digitales de confianza y calidad | Habilitar funcionalidades que permitan a los usuarios hacer seguimiento al estado de los otros procedimientos administrativos disponibles en línea o parcialmente en línea. | Fortalecer el acceso de los ciudadanos a la administración pública mediante el uso de soluciones tecnológicas. |
| Cumplir con todos los criterios de accesibilidad web del anexo 1 de la Resolución 1519 de 2020, para todos los trámites de la entidad disponibles en línea y parcialmente en línea. |
| Cumplir con todos los criterios de accesibilidad web del anexo 1 de la Resolución 1519 de 2020, para todos los otros procedimientos de la entidad disponibles en línea y parcialmente en línea. |
| Cumplir los criterios de usabilidad web para todos los trámites de la entidad que están disponibles en línea y parcialmente en línea. |
| Cumplir los criterios de usabilidad web para todos los otros procedimientos administrativos de la entidad que están disponibles en línea y parcialmente en línea. |
| Promocionar los trámites disponibles en línea y parcialmente en línea para incrementar su uso. |
| Promocionar los otros procedimientos administrativos disponibles en línea y parcialmente en línea para incrementar su uso. |
| Procesos seguros y eficientes | Mejorar y automatizar los procesos de la entidad teniendo en cuenta las definiciones (lineamientos, guías, herramientas y mejores prácticas) del marco de referencia de arquitectura empresarial. | Avanzar en la implementación del dominio de uso y apropiación del Modelo de Arquitectura Empresarial (MRAE) con el fin de desarrollar una cultura que permita la adopción y uso de la tecnología en el IDPC |
| Toma de decisiones basadas en datos | Utilizar técnicas de analítica de datos para predecir comportamientos o hechos de la entidad (analítica predictiva). | No se encuentra |
| Utilizar técnicas de analítica de datos para soportar la toma de decisiones en la entidad (analítica prescriptiva). |
| Utilizar tecnologías emergentes de cuarta revolución industrial para mejorar la prestación de los servicios de la entidad, como tecnologías de desintermediación, DLT (Distributed Ledger Technology), cadena de bloques (Blockchain) o contratos inteligentes, entre otros. |
| Utilizar tecnologías emergentes de cuarta revolución industrial como el análisis masivo de datos (Big data) para mejorar la prestación de los servicios de la entidad. |
| Utilizar tecnologías emergentes de cuarta revolución industrial como la inteligencia artificial (AI) para mejorar la prestación de los servicios de la entidad. |
| Utilizar tecnologías emergentes de cuarta revolución industrial como el internet de las cosas (IoT) para mejorar la prestación de los servicios de la entidad. |
| Utilizar tecnologías emergentes de cuarta revolución industrial como la robótica para mejorar la prestación de los servicios de la entidad. |
| Utilizar tecnologías emergentes de cuarta revolución industrial como la automatización robótica de procesos para mejorar la prestación de los servicios de la entidad. |
| Desarrollar programas de capacitación que permitan a los servidores públicos de la entidad conocer y apropiar las tecnologías de la cuarta revolución industrial. |
| Hacer uso de técnicas de machine learning para la experimentación, producción y toma de decisiones estratégicas. |
| Formular el Plan de Transformación Digital (entendido en los términos del artículo 147 del PND y bajo los lineamientos del Marco de Transformación Digital), aprobarlo en el comité de gestión y desempeño institucional, y actualizar el PETI conforme a las iniciativas, proceso y áreas priorizadas para la transformación digital. |
| Mejorar los conjuntos de datos abiertos de la entidad teniendo en cuenta las necesidades de los usuarios, con el propósito de aumentar su nivel de satisfacción. |
| Empoderamiento de los ciudadanos mediante un Estado abierto | Cumplir, en todas las secciones de la página web oficial de la entidad, con el criterio de accesibilidad: Permitir saltar bloques que se repiten. (regla CC10) | Implementar estrategia de Datos Abiertos con el fin de garantizar la adecuada disposición de datos relevantes para los grupos de valor del IDPC, en el marco de la implementación y sostenibilidad de la política de Gobierno Digital |
| Cumplir, en todas las secciones de la página web oficial de la entidad, con el criterio de accesibilidad: Desde una letra hasta un elemento complejo utilizable. (regla CC31) |
| Cumplir, en todas las secciones de la página web oficial de la entidad, con el criterio de accesibilidad: Foco visible al navegar con tabulación. (regla CC17) |
| Cumplir, en todas las secciones de la página web oficial de la entidad, con el criterio de accesibilidad: Objetos programados. (regla CC30) |
| Cumplir, en todas las secciones de la página web oficial de la entidad, con el criterio de usabilidad "Ruta de migas" que permite conocer la ruta recorrida por el usuario en la navegación del sitio. |
| Cumplir, en todas las secciones de la página web oficial de la entidad, con el criterio de usabilidad "Navegación global consistente" para conservar en todos los sitios de navegación el mismo diseño gráfico. |
| Cumplir, en todas las secciones de la página web oficial de la entidad, con el criterio de usabilidad "Enlaces bien formulados" que indica claramente el contenido al cual conducen y no tienen textos como "ver más", "clic aquí", entre otros. |
| Cumplir, en todas las secciones de la página web oficial de la entidad, con el criterio de usabilidad "Ancho del cuerpo de texto" que establece que el cuerpo de texto no debe superar los 100 caracteres por línea. |
| Cumplir, en todas las secciones de la página web oficial de la entidad, con el criterio de usabilidad "Vínculos visitados" que indica al usuario cuando ha visitado contenidos de la página. |
| Cumplir, en todas las secciones de la página web oficial de la entidad, con el criterio de usabilidad de disponer ejemplos en los campos de los formularios del sitio web. |
| Mantener actualizados todos los conjuntos de datos abiertos de la entidad que están publicados en el catálogo de datos del Estado Colombiano www.datos.gov.co. |
| Emplear diferentes medios digitales en los ejercicios de participación realizados por la entidad. |
| Impulso en el desarrollo de territorios y ciudades inteligentes | Implementar iniciativas de ciudades y territorios inteligentes de acuerdo teniendo en cuenta lo establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones. | No se encuentra |
| Identificar y priorizar la infraestructura y servicios de internet de las cosas (IoT) que requiere o se necesita para adelantar iniciativas de ciudad o territorio inteligente. |
| Estructurar la arquitectura de la infraestructura de internet de las cosas (IoT) a desplegar en la ciudad o territorio. |
| Instalar y desplegar sensores y redes de internet de las cosas (IoT) en la ciudad o territorio. |
| Analizar y explotar los datos capturados por medio de dispositivos de internet de las cosas (IoT). |

**Fuente:** Elaboración propia a partir de recomendaciones Gobierno Digital (MinTIC) y POA (IDPC)

De la tabla anterior se evidencia que los dos propósitos con menor puntaje en el índice de gobierno digital, no cuentan con actividades programadas por el IDPC, que conlleven a la mejora en la medición del índice.

Ahora bien, en cuanto a la ejecución de estas actividades en el POA, de acuerdo con el seguimiento realizado por la Asesoría de Control Interno a esta herramienta, se evidencia que se cuenta con 20 tareas asociadas a las 6 actividades mencionadas anteriormente, de las cuales 13 no estaban programadas para ejecutarse en el primer semestre, 6 se han venido cumpliendo de acuerdo con lo programado y 1 no se ejecutó, aun estando programada, que corresponde a ‘*Realizar capacitaciones sobre el uso y apropiación de las Tecnologías de la Información y Seguridad de la Información’*.

* 1. **MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

En revisión del Modelo de Seguridad y Privacidad de la Información y en concordancia con el habilitador ‘*Fortalecimiento de la seguridad y privacidad de la información*’ el IDPC ha venido desarrollando las siguientes actividades, de acuerdo con las 4 fases definidas por MinTIC:

* + 1. **Fase de Diagnóstico**

De acuerdo con el lineamiento ‘*Identificar a través de la herramienta de autodiagnóstico (Análisis GAP) el estado actual de la Entidad respecto a la Seguridad y privacidad de la Información’*, el IDPC diligenció la herramienta de autodiagnóstico de seguridad digital, el cual contiene diferentes recomendaciones a tener en cuenta para la mejora del Modelo, las cuales deben ser tenidas en cuenta.

* + 1. **Fase de planeación:**

De acuerdo con el lineamiento de MinTIC, los documentos que se deben generar en esta fase son:

* *Alcance MSPI*: El IDPC cuenta con el Manual de Políticas de Seguridad y Privacidad de la Información, el cual contempla de manera general el alcance del modelo.
* *Acto administrativo con las funciones de seguridad y privacidad de la información*: Dentro del Manual de Políticas de Seguridad y Privacidad de la Información del IDPC, se encuentran las responsabilidades.
* *Política de seguridad y privacidad de la información*: El Manual de Políticas de Seguridad y Privacidad de la Información contiene la política.
* *Documento de roles y responsabilidades asociadas a la seguridad y privacidad de la información*: Dentro del Manual de Políticas de Seguridad y Privacidad de la Información del IDPC, se encuentran los roles y responsabilidades. De igual manera, se cuenta con protocolo de roles y responsabilidades.
* *Procedimiento de inventario y Clasificación de la Información e infraestructura crítica*: Se cuenta con este procedimiento en Versión 01 del 18 de Noviembre 2021.
* *Metodología de inventario y clasificación de la información e infraestructura crítica*: Esta metodología no se encuentra claramente definida en el IDPC.

**Respuesta proceso:**

Las metodología utilizada corresponde a la establecida en los modelos de gestión incorporados en el MSPI y los instrumentos entregados por MINTIC <https://gobiernodigital.mintic.gov.co/692/articles-5482_G5_Gestion_Clasificacion.pdf> el cual esta aplicado en las tablas de inventario diligenciados en el IDCP

**Valoración respuesta:**

Se modifica el comentario, quedando: "Se hace uso de la metodología establecida por el Gobierno Nacional, evidenciando su aplicación en el Inventario de Activos de Información".

* *Procedimiento de gestión de riesgos de seguridad de la información*: Si bien se menciona que se adhieren a los lineamientos emitidos por el Gobierno Nacional en esta materia, no se cuenta con un procedimiento establecido formalmente para el IDPC.

**Respuesta proceso:**

En relación con "Procedimiento de gestión de riesgos de seguridad de la información: Si bien se  menciona que se adhieren a los lineamientos emitidos por el Gobierno Nacional en esta materia, no se cuenta con un procedimiento establecido formalmente para el IDPC" La definición de un procedimiento en la gestión de riesgos de seguridad está incorporado en las definiciones de la oficina asesora de planeación del IDCP, siendo decisión de este no publicar un procedimiento específico para los riesgos de seguridad de la información, por tanto la definición de esta actividad estar sujeto a la consideración de la oficina asesora de planeación de la entidad.

**Valoración respuesta:**

Teniendo en cuenta la respuesta, se modifica el comentario, quedando: "En el procedimiento Administración de Riesgos, se menciona que se adhieren a los lineamientos emitidos por el Gobierno Nacional en esta materia".

* *Plan de tratamiento de riesgos de seguridad de la información*: El plan de tratamiento de riesgos de seguridad de la información fue aprobado en el mes de enero de 2022. De igual manera, la matriz de riesgos de seguridad digital fue aprobada en el mes de junio de 2022 en Comité Institucional de Gestión y Desempeño.
* *Declaración de aplicabilidad*: Este documento no se ve tan claramente en los adoptados en el Sistema Integrado de Gestión del IDPC.

**Respuesta proceso:**

La declaración de aplicabilidad esta publicado en el sitio http://10.20.100.31/intranet/gestion-de-sistemas-de-informacion-y-tecnologia/ elaborada bajo los criterios del MSPI y la norma ISO 27001:2013, el instrumento fue actualizado en junio de 2022.

**Valoración respuesta:**

Al revisar nuevamente la documentación del proceso, se evidencia que esta se encuentra definida como un formato, por lo cual no se tuvo en cuenta en el seguimiento preliminar, sin embargo, con la aclaración se modifica el comentario quedando "Se cuenta con formato Declaración de aplicabilidad aprobado en el mes de junio de 2022".

* *Manual de políticas de Seguridad de la Información*: Se cuenta con Manual de políticas de seguridad de la información, el cual se encuentra en versión 2 del 19 de noviembre 2021.
* *Plan de capacitación, sensibilización y comunicación de seguridad de la información*: Se cuenta con Plan de capacitación, sensibilización y comunicación de seguridad de la información, en versión 1 del 30 de agosto de 2021.
  + 1. **Fase de operación:**

Dentro de esta fase, la guía de MinTIC establece como documentos:

* Plan de implementación de controles de seguridad y privacidad de la información
* Evidencia de la implementación de los controles de seguridad y privacidad de la información

Si bien, durante la vigencia se han venido entregando tips de seguridad digital mediante la intranet del IDPC, teniendo en cuenta que la aprobación de la matriz de riesgos de seguridad digital se dio en el mes de junio, no es posible evaluar la implementación de los controles con este corte.

* + 1. **Fase de Evaluación de desempeño:**

De acuerdo con el lineamiento, la evaluación se debe realizar con base en los indicadores definidos, para lo cual, se evidencia la existencia de algunos, sin embargo, no se cuenta con la medición, pese a que el proceso manifiesta entregarlo. Adicionalmente, no se toman en cuenta los propuestos en la Guía de Modelo de Seguridad y Privacidad de la Información de MinTIC.

De igual manera, se establece la necesidad de la ejecución de auditorías internas al sistema, las cuales no se han podido realizar, teniendo en cuenta la ausencia de personal certificado en esta materia que pueda llevarla a cabo.

**Respuesta proceso:**

El proceso de gestión de sistemas de información y tecnología dentro de los indicadores establecidos se encuentran algunos que están relacionados con el MSPI, y el seguimiento se ha realizado en la matriz correspondiente. En cuanto a las auditorías internas no es la clara la observación.

**Valoración respuesta:**

Se remite seguimiento de indicadores, por lo cual se retira este aparte de la observación, sin embargo, se mantiene lo relacionado a la auditoría interna, ya que esta no ha sido realizada.

* + 1. **Fase de Mejoramiento Continuo:**

En este punto, el IDPC ha venido incluyendo en su POA las actividades que han considerado pertinentes para el mejoramiento del Modelo de Seguridad y Privacidad de la Información, sin embargo, aún se encuentran algunas debilidades que son susceptibles de incorporación en los planes de acción.

* 1. **PROTECCIÓN DE DATOS PERSONALES**

Teniendo como base la Guía sobre el tratamiento de datos personales en las entidades estatales expedida por la Superintendencia de Industria y Comercio, la cual se encuentra alineada con lo establecido en la Ley 1581 de 2012 y contiene 24 recomendaciones, se realizó revisión de cada una de estas en cuanto a su inclusión en el IDPC.

* *Tenga presente que la Ley 1581 de 2012 aplica al Tratamiento de Datos Personales que realicen las entidades estatales*: En cumplimiento de lo establecido en la Ley, el IDPC expidió la Resolución 659 de 2018, la cual adopta el Manual de Políticas y Procedimientos para el Tratamiento y Protección de Datos Personales, sin embargo, este manual no se encuentra como un documento controlado dentro del Listado Maestro de Documentos.
* *Antes de realizar Tratamiento de datos efectúe un estudio de impacto de privacidad*: Si bien se cuenta con una política de tratamiento de datos en la Entidad, no se evidencia que se haya desarrollado el estudio o evaluación de riesgos específicos para los derechos y libertades de los Titulares de los Datos Personales.
* *Incorpore legalidad, privacidad, ética, seguridad y responsabilidad demostrada desde el diseño y por defecto*: El Manual del IDPC se encuentra establecido con el fin que sea tenido en cuenta el tratamiento de datos personales previo a la obtención de los mismos. Sin embargo, es necesario fortalecer su aplicación al interior de la Entidad.
* *Informe de manera clara y transparente las finalidades específicas del Tratamiento de los datos*: La información correspondiente al tratamiento de datos personales se encuentra publicado en la página web del IDPC, de igual manera, en el formato lista de asistencia de participantes, se incluyen notas informando a la ciudadanía dónde consultar la política, previo a la obtención de los datos.
* *Trate únicamente los datos estrictamente necesarios*: Las finalidades del tratamiento de datos personales, se encuentra claramente establecida en el Manual y en la página Web.
* *No olvide que la recolección de datos personales sin autorización no implica la desprotección del derecho de hábeas data de los titulares*: En el formato establecido para recolección de datos de ciudadanía, se encuentra expresa la nota de autorización.
* *Efectúe un diagnóstico de cumplimiento de la Ley 1581 de 2012*: No se evidencia la evaluación de la aplicación de la política de tratamiento de datos personales.
* *Use los formatos modelo de la SIC para el cumplimiento de la Ley 1581 de 2012*: Actualmente el IDPC cuenta con unos formatos incluidos en el Manual de Tratamiento de Datos, sin embargo, estos no han sido aplicados en su totalidad, como es el caso de la inclusión de una nota alusiva al tratamiento de datos en los mensajes de difusión masiva.
* *Recolecte datos de forma lícita, utilizando medios que dejen evidencia para demostrar el cumplimiento de la ley*: En el formato establecido para recolección de datos de ciudadanía, se encuentra expresa la nota de autorización.
* *Clasifique los Datos Personales*: La clasificación de datos personales se encuentra establecida en la política de tratamiento de datos, adicionalmente, se encuentra en actualización el índice de activos de información, en el cual se identifican los datos personales.
* *Tenga en cuenta las pautas especiales para recolectar huellas dactilares, o recolectar datos relativos al estado de salud de las personas (Datos Sensibles)*: No se cuenta con este tipo de datos.
* *Cumpla los requisitos para poder recolectar y tratar Datos Personales de niñas, niños y adolescentes (NNA)*: En la Resolución 659 de 2018, que adopta el Manual de Políticas y Procedimientos para el Tratamiento y Protección de Datos Personales, se encuentra definido en el artículo 8 el tratamiento de datos personales de menores de edad, así como en el numeral 3.3 de la política.
* *Exija el respeto de la regulación de protección de datos y de su Política de Tratamiento de Datos Personales a los terceros que contrata (Encargados del Tratamiento) para que le presten, entre otros, servicios de seguridad privada y de computación en la nube*: Si bien dentro de las cláusulas generales del contrato de vigilancia se encuentra “guardar estricta reserva y confidencialidad de toda la información relacionada con el INSTITUTO o sus contratistas, de la cual tenga conocimiento por razón de las actividades que desarrolla”, no está explícito el tema de tratamiento de datos personales, ni la aplicación de la política interna.
* *Adopte medidas para garantizar los principios sobre Tratamiento de Datos Personales (TDP) en las entidades estatales*: Las medidas se encuentran acogidas mediante Resolución 659 de 2018, la cual adopta el Manual de Políticas y Procedimientos para el Tratamiento y Protección de Datos Personales
* *Respete los derechos de los Titulares de los datos e implemente mecanismos efectivos para el ejercicio de los mismos*: Los derechos de los titulares se encuentran descritos en el numeral 4.1 del Manual de Políticas y Procedimientos para el Tratamiento y Protección de Datos Personales
* *Ubique avisos de privacidad en sitios fácilmente visibles*: No se evidencia la publicación de avisos de privacidad en las porterías de la Entidad.
* *Sitúe avisos para informar a las personas que están siendo videovigiladas*: No se evidencia la publicación de avisos que informen a las personas que están siendo videovigiladas en la Entidad.
* *Garantice la seguridad de los Datos Personales y esté preparado para actuar frente a eventuales incidentes de seguridad*: No se evidencia en el IDPC documento o plan dirigido a afrontar los incidentes de seguridad que afecten los Datos Personales bajo su custodia o posesión.
* *Elimine los Datos Personales tan pronto cumplan la finalidad para la cual fueron tratados*: La política no incluye expresamente lo relacionado con la supresión de los datos personales.
* *Garantice la confidencialidad de la información*: Los contratos cuentan con cláusula de confidencialidad.
* *Implemente estrategias de Responsabilidad Demostrada (Accountability) frente al Tratamiento de Datos Personales*: No se evidencia la capacitación del personal de manera periódica en materia de tratamiento de datos personales.
* *Registre las Bases de Datos ante el RNBD*: Dentro del Manual de Políticas y Procedimientos para el Tratamiento y Protección de Datos Personales se encuentra contemplado el registro de bases de datos del IDPC.
* *Incremente y mantenga la confianza de los Titulares de Datos Personales*: No se cuenta con actividades que ayuden a fortalecer la confianza de los titulares de datos personales.
* *Tenga presente la regulación de datos en los procesos de interoperabilidad, circulación o entrega de Datos Personales*: En el numeral 5 del Manual de Políticas y Procedimientos para el Tratamiento y Protección de Datos Personales se encuentran definidos los procedimientos para la entrega de información de datos personales.

**Respuesta proceso:**

Dentro del presupuesto del año 2023 se dejó contemplado la contratación del Oficial de protección de datos personales para dar cumplimiento a esta observación.

**Valoración respuesta:**

Teniendo en cuenta la respuesta se mantienen las observaciones.

* 1. **ACTIVOS DE INFORMACIÓN**

De acuerdo con la guía para la gestión y clasificación de activos de información, se separa en 2 ámbitos, la gestión de activos y la clasificación de los mismos.

* + 1. **Gestión de activos de información:**

Se encuentra dividido en definición, revisión, actualización y publicación. Todos estos temas se encuentran materializados en la matriz de activos de información la cual fue aprobada por el Comité de Gestión y Desempeño en el mes de noviembre de 2021 y se encuentra publicada en la página Web.

Esta matriz se encuentra en actualización por parte de cada uno de los procesos, con el acompañamiento de los procesos Gestión Documental y Gestión de Sistemas y Tecnologías de la Información y Comunicaciones.

* + 1. **Clasificación de activos de información:**

La clasificación de los activos se encuentra a partir de la confidencialidad, integridad y disponibilidad. Esto puede ser evidenciado dentro de la matriz de activos de información.

Adicionalmente, se menciona el etiquetado de activos de información, sin embargo, este tema no ha sido evidenciado en la documentación del IDPC.

**Respuesta proceso:**

Teniendo en cuenta que el etiquetado de activos de información corresponde al proceso de gestión documental se enviara la observación para que se tenga en cuenta y se de cumplimiento.

**Valoración respuesta:**

Teniendo en cuenta la respuesta se mantiene la observación.

1. **FORTALEZAS EVIDENCIADAS**
   1. Se incluyó la mayoría de las recomendaciones generadas como resultado de la medición del índice de gobierno digital.
   2. Se han venido actualizando los lineamientos internos en materia de seguridad y privacidad de la información.
   3. Se formalizaron los riesgos de seguridad digital.
   4. Se cuenta con política de tratamiento de datos personales, la cual es pública en la página Web de la Entidad.
   5. La matriz de activos de información se está actualizando por parte de cada uno de los procesos, con el acompañamiento de los procesos Gestión Documental y Gestión de Sistemas y Tecnologías de la Información y Comunicaciones.
2. **OBSERVACIONES**
   1. Si bien se han venido incluyendo las recomendaciones generadas en la medición del índice de gobierno digital dentro del Plan de Acción del proceso Gestión de Sistemas de Información y las Tecnologías, no fueron programadas actividades que permitan mejorar la evaluación de los dos propósitos que se encuentran por debajo de 50 puntos.
   2. En materia de Evaluación del Desempeño del Modelo de Seguridad y Privacidad de la Información, no se evidencia la ejecución de auditorías internas.
   3. El Manual de Políticas y Procedimientos para el Tratamiento y Protección de Datos Personales no se encuentra como un documento controlado dentro del Listado Maestro de Documentos. Adicionalmente, no se está cumpliendo a cabalidad.
   4. Para la generación del Manual de Políticas y Procedimientos para el Tratamiento y Protección de Datos Personales no se tuvo en cuenta la evaluación de riesgos específicos para los derechos y libertades de los Titulares de los Datos Personales.
   5. No se evidencia la publicación de avisos de privacidad en las porterías de la Entidad, ni de aviso de videovigilancia.
   6. No se observa en el IDPC documento o plan dirigido a afrontar los incidentes de seguridad que afecten los Datos Personales bajo su custodia o posesión.
   7. En relación con el etiquetado de activos de información, no ha sido evidenciado en la documentación del IDPC.
3. **NO CONFORMIDADES DETECTADAS**

No se evidencian No Conformidades para el período evaluado.

1. **CONCLUSIÓN GENERAL**

El IDPC de manera general, ha venido avanzando en el cumplimiento de la política de Gobierno Digital, sin embargo, aún se encuentran algunas debilidades que requieren ser atendidas para la mejora continua del Modelo Integrado de Planeación y Gestión.

1. **RECOMENDACIONES**
   1. Tomar en cuenta las recomendaciones generadas en la medición del Índice de Gobierno Digital, priorizando aquellos habilitadores o propósitos cuya evaluación es la más baja.
   2. Continuar con la ejecución de las actividades de cada una de las fases del Modelo de Seguridad y Privacidad de la Información.
   3. Realizar la evaluación de riesgos específicos para los derechos y libertades de los Titulares de los Datos Personales y con base en sus resultados actualizar, de ser necesario, el Manual de Políticas y Procedimientos para el Tratamiento y Protección de Datos Personales, incluyéndolo como parte del Sistema Integrado de Gestión.
   4. Verificar las recomendaciones y formatos generados por la SIC en materia de tratamiento de datos personales, identificando aquellos que sean susceptibles de aplicación en el IDPC.
   5. Generar plan dirigido a afrontar los incidentes de seguridad que afecten los Datos Personales bajo su custodia o posesión, verificando la guía para la gestión de incidentes de seguridad en el tratamiento de datos personales, generada por la SIC.
   6. Continuar la actualización de los activos de información.
   7. Incluir el etiquetado de activos de información.