



AUDITORÍA A LA IMPLEMENTACIÓN DE LA POLÍTICA GOBIERNO DIGITAL Y SEGURIDAD DE LA INFORMACIÓN.

Informe final de auditoría interna: AI-20-2021

Fecha de emisión: 27/10/2020

Índice general (revisar nivel descriptivo)

1. Introducción.....	1
2. Metodología	2
3. Resultados	3
4. Conclusiones	4
5. Plan de mejoramiento.....	5
6. Anexos.....	6

1. INTRODUCCIÓN

1.1 ¿Qué es la política de Gobierno Digital?

Gobierno Digital es la política pública liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC, que tiene como objetivo “Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital”.

A partir de ello, se genera un nuevo enfoque donde el Estado y los actores de la sociedad son fundamentales para el desarrollo integral del Gobierno Digital en Colombia, en donde las necesidades y problemáticas determinan el uso de las Tecnologías de la Información y las Comunicaciones (TIC) y la forma como éstas pueden aportar en la generación de valor público.

La Política de Gobierno Digital se considera como la evolución de la Estrategia de Gobierno en Línea que, en otras palabras, era el nombre con que se conocían al conjunto de acciones relacionadas con herramientas TIC para lograr una mejor participación e interacción con el ciudadano.

1.2 Propósitos de la Política

Los propósitos de la política son los siguientes:

- A. **Habilitar y mejorar la provisión de Servicios Digitales de confianza y calidad:** consiste en poner a disposición de ciudadanos, usuarios y grupos de interés, trámites y servicios del Estado que cuenten con esquemas de manejo seguro de la información, que estén alineados con la arquitectura institucional de la entidad (Arquitectura misional y Arquitectura de TI) y que hagan uso de los servicios de autenticación electrónica, interoperabilidad y carpeta ciudadana, a fin de que éstos sean ágiles, sencillos y útiles para los usuarios.

- B. Lograr procesos internos seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información: consiste en desarrollar procesos y procedimientos que hagan uso de las tecnologías de la información, a través de la incorporación de esquemas de manejo seguro de la información y de la alineación con la arquitectura institucional de la entidad (Arquitectura misional y Arquitectura de TI), a fin de apoyar el logro de las metas y objetivos de la entidad.

- C. Tomar decisiones basadas en datos a partir del aumento en el uso y aprovechamiento de la información: consiste en mejorar la toma de decisiones por parte de la entidad, ciudadanos, usuarios y grupos de interés, para impulsar el desarrollo de servicios, políticas, normas, planes, programas, proyectos o asuntos de interés público, a partir del uso y aprovechamiento de datos que incorporan estándares de calidad y seguridad en su ciclo de vida (generación, recolección, almacenamiento, procesamiento, compartición, entrega, intercambio y eliminación).

- D. Empoderar a los ciudadanos a través de la consolidación de un Estado Abierto: consiste en lograr una injerencia más efectiva en la gestión del Estado y en asuntos de interés público por parte de ciudadanos, usuarios y grupos de interés, para impulsar la gobernanza en la gestión pública, a través del uso y aprovechamiento de las tecnologías digitales.

- E. Impulsar el desarrollo de territorios y ciudades inteligentes para la solución de retos y problemáticas sociales, a través del aprovechamiento de Tecnologías de la Información y las Comunicaciones: consiste en promover el co-diseño y la implementación de iniciativas de tipo social, ambiental, político y económico, por parte de entidades públicas y diferentes actores de la sociedad, para el mejoramiento de la calidad de vida de los ciudadanos e impulsar el desarrollo sostenible, a través del uso y aprovechamiento de las TIC de manera integrada y proactiva.

1.3 Elementos de la Política

Para la implementación de la Política de Gobierno Digital, se han definido dos componentes: TIC para el Estado y TIC para la Sociedad, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales. Estos cinco elementos se desarrollan a través de lineamientos y estándares, que son los requerimientos mínimos que todos los sujetos obligados deben cumplir para alcanzar los logros de la política.

En la imagen 1, se muestra el esquema de la Política de Gobierno Digital, en la cual se muestran los componentes, propósitos y habilitadores transversales que forman su estructura y sirven de base para procesos de evaluación que buscan determinar el nivel de avance en la implementación en cada una de las entidades que, de acuerdo con la normatividad vigente, deban implementarla.

Estos elementos se articulan de la siguiente forma:

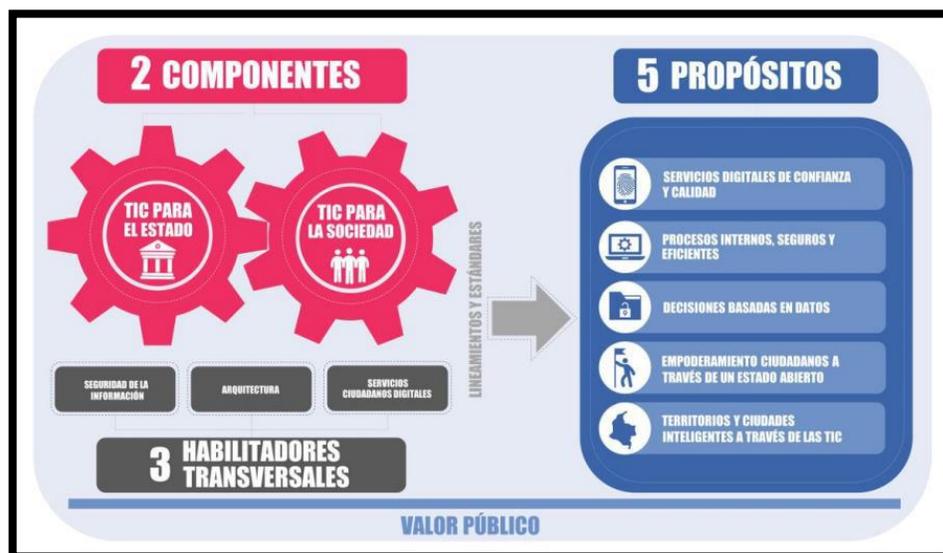


Imagen 1. Estructura de Gobierno Digital.

Fuente: Manual Gobierno Digital.

TIC para el Estado: Tiene como objetivo mejorar el funcionamiento de las entidades públicas y su relación con otras entidades públicas, a través del uso de las Tecnologías de la Información y las Comunicaciones.

TIC para la Sociedad: Tiene como objetivo fortalecer la sociedad y su relación con el Estado en un entorno confiable, que permita la apertura y el aprovechamiento de los datos públicos, la colaboración en el desarrollo de productos y servicios de valor público, el diseño conjunto de servicios, la participación ciudadana en el diseño de políticas y normas, y la identificación de soluciones a problemáticas de interés común¹.

1.4 Habilitadores Transversales

Arquitectura: busca que las entidades apliquen en su gestión un enfoque de Arquitectura Empresarial para el fortalecimiento de sus capacidades institucionales y de gestión de TI. El habilitador de Arquitectura soporta su uso e implementación en el Marco de Referencia de Arquitectura Empresarial del Estado, que es el instrumento que establece la estructura conceptual, define lineamientos, incorpora mejores prácticas y traza la ruta de implementación que una entidad pública debe realizar.

Seguridad de la información: busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad y disponibilidad y privacidad de los datos. Este habilitador se soporta en el Modelo de Seguridad y Privacidad de la Información - MSPI, que contempla 6 niveles de madurez.

Servicios Ciudadanos Digitales: busca que todas las entidades públicas implementen lo dispuesto en el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, que establece los lineamientos para la prestación de los servicios ciudadanos digitales, y para permitir el acceso a la administración pública a través de medios electrónicos.

Conforme a dicha normativa, los servicios digitales se clasifican en servicios básicos: autenticación biométrica, autenticación con cédula digital, autenticación electrónica, carpeta ciudadana e interoperabilidad, los cuales son de obligatorio uso y adopción; y servicios

¹ <https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/>

especiales, que son adicionales a los servicios básicos, como el desarrollo de aplicaciones o soluciones informáticas para la prestación de los servicios ciudadanos digitales básicas².

1.5 Resultados medición del Desempeño Institucional – 2020

El formulario Único Reporte de Avances de la Gestión - FURAG, permite establecer el nivel de avance de la implementación del Modelo Integrado de Planeación y Gestión - MIPG y del Modelo Estándar de Control Interno - MECI, junto con recomendaciones de mejora por política. Así mismo, posibilita evaluar los avances en la implementación de las políticas de Gestión y Desempeño Institucional de la vigencia anterior al reporte.

De acuerdo con la calificación del índice de desempeño institucional, a la fecha, generada por medio de la herramienta de reporte del DAFP, se obtuvo que, para la política de gobierno digital, la calificación para la gestión y desempeño de la vigencia 2019 correspondió a un **80.6%**.

Teniendo en cuenta que la anterior calificación asignada por el DAFP para la política de gobierno digital para el 2020, corresponde al **83.6%**, se evidencia un aumento en el avance respecto a la calificación anterior, por lo que se recomienda continuar sus implicaciones y establecer acciones enfocadas a incrementar el porcentaje de implementación de la política.

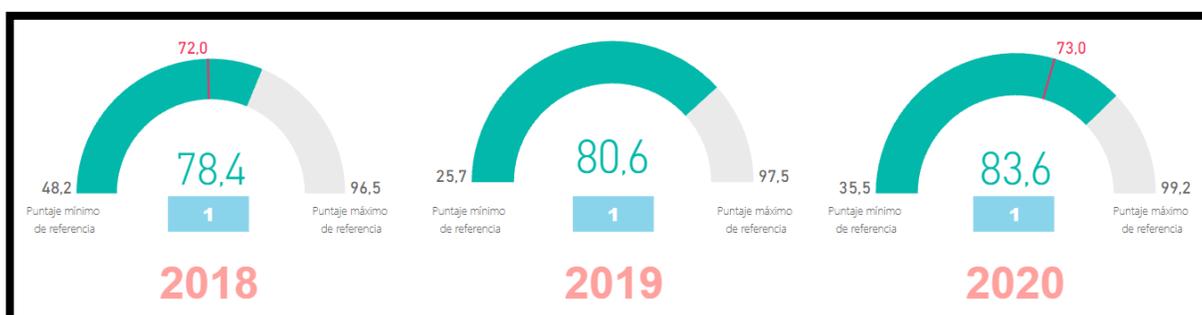


Imagen 2. Nivel de Avance de desempeño institucional de la Política de Gobierno Digital - UPRA. Vigencia 2018 – 2019 – 2020.

Fuente: <https://gobiernodigital.mintic.gov.co/portal/Mediciones/>

²<https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/Manual-de-Gobierno-Digital/>

2. METODOLOGÍA

2.1. Identificación

Aspecto evaluable (unidad auditable)	Gestión de servicios tecnológicos - Oficina Tecnologías de la Información y Comunicaciones (Oficina TIC).
Líder de proceso/jefe(s) de dependencia(s)	Luz Mery Gómez Contreras - Jefe de Oficina TIC
Objetivo de la auditoría	Evaluar la implementación, gestión y cumplimiento de la Política de Gobierno Digital, con respecto a sus tres habilitadores transversales, teniendo en cuenta la herramienta de autodiagnóstico que contiene los lineamientos establecidos por MINTIC, el modelo MIPG, resultados del FURAG, los riesgos y los controles asociados a su operación.
Alcance de la auditoría	La presente auditoría comprende la gestión de la UPRA durante la vigencia enero 2020 a julio 2021, verificando el cumplimiento del Decreto 1008 de 2018 (Lineamientos Generales de la Política de Gobierno Digital), el Manual para la Implementación de la Política de Gobierno Digital y sus criterios relacionados y transversales a la entidad.
Reunión de apertura	30 de agosto de 2021, Carta de representación Radicado 2021-3-007688.
Ejecución de auditoría	Desde: 30 de agosto 2021 Hasta: 08 de octubre 2021
Reunión de cierre	21 de octubre de 2021 Ubicación de acta.
Líder de auditoría	Asesor de control interno - Sandra Milena Ruano Reyes
Auditor	Ubaldo Enrique murgas Granados

2.2 Criterios de auditoría:

- 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”.
- Decreto 1078 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.
- Manual de Gobierno Digital.
- Lineamientos, estándares, guías, mejores prácticas y normatividad de la arquitectura de TI.
- Herramienta de Autodiagnóstico Gestión Política de Gobierno Digital MIPG - FURAG.

- Herramienta de Autodiagnóstico de MINTIC - UPRA.
- Modelo de Seguridad y Privacidad de la Información - MSPI de MINTIC
- Mapa de Riesgos Institucional 2021 - UPRA.
- Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETIC 2019 -2022.
- Marco de referencia de arquitectura empresarial del MINTIC.

2.3. Muestreo y herramientas

- Muestra: No Aplica por el tipo de auditoría de gestión y cumplimiento
- Herramientas: Microsoft TEAMS, correo electrónico, documentación del sistema de gestión SEA y carpetas compartidas ubicadas en la ruta:

U:\02.TIC\2021\AuditoriaPoliticaGobDigital\Sesion1_Arquitectura

U:\02.TIC\2021\AuditoriaPoliticaGobDigital\Sesion2_Servicios_Tecnologicos_SeguridadInformacion

U:\02.TIC\2021\AuditoriaPoliticaGobDigital\Sesion3_Interoperabilidad

U:\02.TIC\2021\AuditoriaPoliticaGobDigital\Sesion4_Autodiagnostico

Relación de documento de trabajo utilizado:

P:\01.DIRECCION_GENERAL\6.ACI\Gestión_2020 a 2021\2021\Auditoria TIC

- AI-2021-PLANI-01-ARQUITECTURA.xlsx
- AI-2021-PLANI-02-SEGURIDAD.xlsx
- AI-2021-PLANI-03-SERV_CIUDADANOS.xlsx
- AI-2021-PLANI-04-MIPG 2018-2019.xlsx
- AI-2021-PLANI-05-RECOM_MIPG_WEB.xlsx
- AI-2021-PLANI-06-SEG_DIGITAL.xlsx
- AI-2021-LCHECK-01.xlsx
- AI-2021-LCHECK-02.xlsx

3. RESULTADOS

3.1. Riesgos de Aspecto Evaluable

En el desarrollo de la auditoria se realizó seguimiento a la aplicación de los controles definidos identificados en el proceso Gestión de Servicios Tecnológicos al corte del informe relacionados con el alcance de auditoría.

La UPRA se encuentra en el proceso de implementación de la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 – diciembre de 2020.

Riesgo de definido mapa de riesgos institucional 2021 UPRA Versión 2 - 17/12/2020:

Inefectividad en la implementación de planes, programas y proyectos de tecnologías de información, para el desarrollo de procesos misionales, estratégicos, de apoyo y evaluación de la entidad.

Control 1:

El jefe de la oficina TIC, dentro del proceso de “Gestión de la Información Agropecuaria - GIA”, anualmente, deberá actualizar el Plan Estratégico de TIC, teniendo en cuenta las nuevas necesidades de planes, programas y proyectos de TIC para la UPRA y el mantenimiento de los existentes, resultado de un ejercicio de identificación y priorización con los procesos de la entidad.

Seguimiento del control:

Durante la vigencia 2020 se actualizó el Plan Estratégico TIC 2019 -2022 como consta en la página web de la entidad:

<https://www.upra.gov.co/documents/10184/111652/Anexo+10.+Plan+Estrat%C3%A9gico+de+Tecnolog%C3%ADas+de+la+Informaci%C3%B3n+y+las+Comunicaciones+PETIC+2019-2020.pdf/49807a03-8ddf-49ef-87f6-fc7006bf6672>, el cual fue actualizado el 29 de enero 2021

Para la vigencia 2021 apoyados en el Plan de Acción Institucional con fecha de última versión de enero de 2021, se puede evidenciar el detalle de las actividades e indicadores que realizara la UPRA para dar continuidad a los proyectos.

Se encontró el monitoreo al riesgo y controles remitidos a la Asesoría de planeación en los documentos soporte “Estrategias de uso y apropiación” código del documento GIA-ID-006

y documento denominado “consolidado_MEDICION_ANALISIS_INDICADORES_SG” hoja “EstrategiasUATI” los cuales se utilizan como control interno en la Oficina de TIC para el seguimiento y actualización de las actividades, estos soportes fueron compartidos en la ruta: en sistema de gestión de la entidad SEA y una vez validados se pudo evidenciar que desde la fecha de creación 31/08/2020 contienen toda la información detalle de los proyectos y su estado de avance.

Control 2:

El profesional especializado de uso y apropiación anualmente realizará un diagnóstico de las herramientas y sistemas de la Entidad frente a su aprovechamiento, con este, el direccionamiento del plan estratégico de TI y las orientaciones de la dirección, se elaborará un plan de uso y apropiación que incluya el análisis del uso, la eficiencia o la experiencia del usuario frente a los sistemas que hacen parte de la Entidad.

Seguimiento del control:

En la verificación de los controles la Oficina de TIC, mediante un documento de uso interno llamado “Artefacto_actualizacionPETIC_2021.xlsx”, se detallan cada una de las necesidades de TI detectadas, con el fin de darle trámite de actualización, mantenimiento a los proyectos de TI, también se cuenta con un documento denominado “TableroIndicador_SeguimientoPETIC.xlsx”, donde se realiza el seguimiento de los proyectos en ejecución.

Se evidenció un formato denominado “ESTRATEGIAS DE USO Y APROPIACIÓN” código del documento GIA-ID-006 y documento denominado “consolidado_MEDICION_ANALISIS_INDICADORES_SG” hoja “EstrategiasUATI”, donde se realiza la gestión y seguimiento de cada de las estrategias definidas para la implementación de uso y apropiación de la entidad.

3.2. OBSERVACIONES

3.2.1 Habilitador Arquitectura TI- Falta de institucionalización de documentos y registros de la política de gobierno digital en el sistema de gestión de la UPRA.

Hecho: El proceso Gestión de Servicios Tecnológicos de la oficina de TIC cuenta con documentos de uso interno llamados “*Plan de transformación digital*” y “*Arquitectura de referencia*”, los cuales no han sido aprobados, socializados y formalizados en el sistema de gestión a través de SEA.

Causa posible: Falta de seguimiento a la actualización oportuna de documentos y/o registros relacionada con la implementación de la Política de Gobierno Digital.

Consecuencia: Desconocimiento de los lineamientos establecidos en los documentos citados por parte del personal de la oficina de TICS para la ejecución y desarrollo de las actividades técnicas aplicables a la entidad.

Criterio: Anexo 2, dominio servicios tecnológicos, segmentación elementos Habilitantes: Arquitectura del Manual de la Política de Gobierno Digital del MINTIC.

Recomendaciones: Formalizar y socializar los documentos en el Sistema de gestión a través de SEA y realizar seguimiento a las necesidades de actualización de registros del proceso relacionado con la implementación de la política de Gobierno Digital de manera periódica.

3.2.2 Habilitador Arquitectura TI- Falta de seguimiento a las recomendaciones identificadas en los reportes generados en la medición de desempeño institucional - FURAG - en el ítem recomendaciones de la política de Gobierno Digital.

Hecho: En la verificación de la herramienta de medición de desempeño institucional - FURAG vigencia 2020, se observaron unas recomendaciones en el ítem de gobierno digital no se evidenciaron acciones de control específicas en la presente auditoria.

Las recomendaciones son las siguientes:

- La entidad cumple 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 línea³.
- La entidad cumple en todas las secciones de la página web oficial de la entidad, con el criterio de usabilidad de contar con diferentes hojas de estilo para su correcta

³<https://app.powerbi.com/view?r=eyJrIjoizGE2MzQ1YTQtYWl3ZC00YTdiLWJkY2ltNzI2YmU3YzQ1ZTk5liwidCI6IjU1MDNhYWMyLTdhMTUtNDZhZi1iINTlwlTJhNjc1YWQxZGYxNiIsImMiOiR9&pageName=ReportSection396d1cd03a850a004c59>

navegación (pantalla, móvil, impresión). En caso de que el sitio web sea responsivo sólo requiere formato de impresión⁴.

Causa posible: Falta de seguimiento a las recomendaciones definidos en los reportes generados en la medición de desempeño institucional - FURAG - en el ítem recomendaciones de la política de Gobierno Digital.

Consecuencia: Inefectividad de los controles implementados para el desarrollo de las actividades definidas en los reportes generados en la medición de desempeño institucional - FURAG - en el ítem recomendaciones de la política de Gobierno Digital

Criterio: Medición de desempeño institucional - FURAG - ítem Gobierno Digital.

Recomendaciones: Realizar seguimiento a los reportes generados en la medición de desempeño institucional - FURAG - en el ítem recomendaciones de la política de Gobierno Digital.

3.2.3 Habilitador Seguridad de la Información- Retraso en la ejecución de actividades programadas en el documento de plan de tratamiento de riesgos⁵ que soporta la gestión vigencia 2021.

Hecho: Se verificó el desarrollo de las actividades programadas en el Plan de tratamiento de riesgos de seguridad y privacidad de la información presentado en la auditoria, se evidenció que existen acciones y actividades vencidas relacionadas con la implementación de la Política de Gobierno Digital con respecto al habilitador de seguridad.

Causa posible: Débil seguimiento, control y actualización sobre las actividades definidas en el plan de tratamiento de riesgos.

4

<https://app.powerbi.com/view?r=eyJrIjoieZGE2MzQ1YTQtYWI3ZC00YTdiLWJkY2ltNzI2YmU3YzQ1ZTk5liiwidCI6IjU1MDNhYWMyLTdhMTUtNDZhZi1iINTlwlTJhNjc1YWQxZGYxNiIsImMiOiR9&pageName=ReportSection396d1cd03a850a004c59>

⁵ 11. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2021

Consecuencia: Incumplimiento de actividades programadas para ejecutar durante la vigencia 2021 definidas en el documento plan de tratamiento de riesgos de seguridad y privacidad de la información.

Criterio: Documento plan de tratamiento de riesgos de seguridad y privacidad de la información, Política de Gobierno Digital del MINTIC, Habilitador de Seguridad de la información, el cual señala que las entidades deben garantizar el seguimiento y la actualización de las actividades que garanticen la ejecución e implementación de la política de gobierno digital.

Recomendaciones: Revisar la planeación de actividades y priorizar su desarrollo durante la vigencia 2021, llevando a cabo las acciones que se requieran.

3.2.4 Habilitador Seguridad de la Información- Falta de seguimiento a los controles con calificación menor identificados en la herramienta de evaluación del MSPI.

Hecho: En la verificación de la herramienta de evaluación de MSPI con corte marzo del presente año, se observaron controles con una calificación “MENOR” en hoja madurez MSPI. Lo anterior no es coherente con la calificación de evaluación de efectividad de controles y no existe información de las razones de la calificación y su tratamiento.

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES

ID REQUISITO	HOJA	ELEMENTO
R14	Administrativas	AD.5.1.1
R38	Administrativas	AD.7.1
R39	Administrativas	AD.7.2
R42	Administrativas	AD.6.2

ID REQUISITO	HOJA	ELEMENTO
R41	PHVA	E.1
		E.2
		E.3
		M.1
R46	PHVA	M.2

ID REQUISITO	HOJA	ELEMENTO
R29	Técnicas	T.5.1

R33	Técnicas	T.6.3
R52	Técnicas	T.4.7

Causa posible: Falta de seguimiento a los controles de calificación “MENOR” definidos en el Instrumento de Evaluación de MSPI (Modelo de Seguridad y Privacidad de la Información) para la medición del nivel de madurez de la entidad.

Consecuencia: Inefectividad de los controles implementados sobre las actividades relacionadas en el instrumento de evaluación de MSPI vigencia 2021.

Criterio: Instrumento de Evaluación de MSPI (Modelo de Seguridad y Privacidad de la Información) para la medición del nivel de madurez vigencia 2021, con el cual la entidad desarrolla un autodiagnóstico de los controles definidos.

Recomendaciones: Realizar seguimiento a la aplicación y a los resultados del Instrumento de Evaluación de MSPI para garantizar la adecuada implementación del Modelo de seguridad y privacidad de la información.

Las observaciones y recomendaciones generadas por la Asesoría de Control Interno en sus informes tienen como fin la mejora de los aspectos evaluados, por lo que se espera sean consideradas por los responsables como un instrumento que contribuye a la realización de ajustes, correcciones o mejoras oportunas, previas a posibles pronunciamientos de organismos externos de control.

4. Oportunidades de Mejoras

La construcción de un Modelo o Plan de continuidad de negocio el cual es un procedimiento documentado que guía y orienta a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel pre-definido de operación debido una vez presentada / tras la interrupción⁶.

Nota: Típicamente, esto incluye los recursos, servicios y actividades necesarios para garantizar la continuidad de las funciones críticas del negocio. [Fuente: ISO 22301].

⁶ https://mintic.gov.co/gestionti/615/articles-5482_G10_Continuidad_Negocio.pdf

5. CONCLUSIONES

- ✓ El resultado del índice de desempeño de la política de gobierno digital 2020, se encuentra en un 83% y se pudo evidenciar que presenta un avance significativo con relación a la vigencia (2019), una vez se validaron los documentos soporte recopilados en la presente auditoría y comparados con los que se encuentran registrados en la herramienta de autodiagnóstico FURAG - MIPG año 2020.
- ✓ Existen aspectos a mejorar en el proceso de implementación de la política de gobierno digital en los tres habilitadores transversales mencionados en cada una de las observaciones y la mayoría están relacionadas con la formalización de los controles de forma integral para soportar el cumplimiento de los criterios, aplicando una estructura metodológica para el cumplimiento de la política.
- ✓ Cada uno de los planes de acción definidos para la implementación y cumplimiento de la política de gobierno digital requieren considerar los resultados de las herramientas de autodiagnóstico de MINTIC (MSPI) y las recomendaciones generadas en los resultados de FURAG – MIPG vigencia 2020, los cuales sirven como elementos de seguimiento y control necesarios para asegurar la gestión institucional.

5. PLAN DE MEJORAMIENTO

De acuerdo con lo establecido en el manual operativo del Modelo Integrado de planeación y Gestión corresponde a los jefes definir las acciones pertinentes para asegurar la no repetición de las debilidades encontradas en desarrollo del ejercicio de auditoría.

Por lo anterior, es necesario remitir el correspondiente plan de mejoramiento a más tardar siete (7) días hábiles y junto con el formato publicado en el SEA llamado “PLAN DE MEJORAMIENTO” Código de documento PEC-FT-005. Se debe anexar el correspondiente análisis de causas. Las acciones deben considerar el tiempo para su desarrollo y la implementación en la gestión para su posterior seguimiento por parte de la Asesoría de Control Interno.

7. GLOSARIO

ARQUITECTURA DE TI: De acuerdo con el Marco de referencia de Arquitectura empresarial del Estado, define la estructura y las relaciones de todos los elementos de T.I. de una organización. Se descompone en arquitectura de información, arquitectura de sistemas de información y arquitectura de servicios tecnológicos. Incluye además las arquitecturas de referencia y los elementos estructurales de la estrategia de T.I. (visión de arquitectura, principios de arquitectura, lineamientos y objetivos estratégicos).

ACTIVO DE INFORMACIÓN: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

CONFIDENCIALIDAD: Se refiere a que la información solo puede ser conocida por individuos autorizados.

CONTINUIDAD DE NEGOCIO: Proceso general de gestión que identifica amenazas potenciales a una organización y el impacto que se podría causar a la operación de negocio que en caso de materializarse. La gestión de la continuidad del negocio provee un marco de trabajo para la construcción de la resiliencia organizacional, con capacidad de respuesta efectiva que salvaguarde los intereses de las partes interesadas, reputación, marca y actividades de creación de valor.

DATOS ABIERTOS: Son aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

DISPONIBILIDAD DE LA INFORMACIÓN: Se refiere a la seguridad que la información puede ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.

GOBIERNO DIGITAL: De forma general, consiste en el uso de las tecnologías digitales como parte integral de las estrategias de modernización de los gobiernos para crear valor público. Esto depende de un ecosistema de actores gubernamentales, ONGs, empresas, asociaciones ciudadanas e individuos que dan soporte a la producción de y acceso a datos, servicios y contenido a través de interacciones con el gobierno. En Colombia, Gobierno Digital es la política pública liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones -Ministerio TIC, que tiene como objetivo “Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital”.

INTEGRIDAD: Se refiere a la garantía de que una información no ha sido alterada, borrada, reordenada, copiada, etc., bien durante el proceso de transmisión o en su propio equipo de origen.

MANUAL DE GOBIERNO DIGITAL: Documento que define los lineamientos, estándares y acciones a ejecutar por parte de los sujetos obligados de la Política de Gobierno Digital en Colombia, el cual es elaborado y publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones, en coordinación con el Departamento Nacional de Planeación.

MARCO DE INTEROPERABILIDAD: Es el conjunto de principios, políticas y recomendaciones que busca facilitar y optimizar la colaboración entre organizaciones privadas y entidades del Estado para intercambiar información y conocimiento, en el marco de los procesos de negocio, con el propósito de facilitar la entrega de servicios a ciudadanos, empresas y a otras entidades para intercambiar información, aporte de documentos y datos en línea.

SERVICIOS CIUDADANOS DIGITALES: Es el conjunto de servicios que brindan capacidades y eficiencias para optimizar y facilitar el adecuado acceso de los usuarios a la administración pública a través de medios electrónicos. Estos servicios se clasifican en básicos y especiales.