Periodo de Ejecución

Entre el 28 de marzo y el 29 de abril de 2022, se llevó a cabo auditoría de cumplimiento a la gestión de las Política de Gobierno y Seguridad Digital, de conformidad con lo programado en el Plan Anual de Auditoria para el año 2022.

Objetivo

Establecer el nivel de implementación de las Políticas de Gobierno Digital y Seguridad Digital de la Secretaria General conforme al Decreto 1008 de 2018 y la Resolución 500 del 2021, emanadas de Ministerio de Tecnologías de la Información y las Comunicaciones y demás normatividad legal vigente que regule la materia.

Alcance

Evaluar mediante muestra selectiva de auditoría a registros y soportes el grado de avance en la implementación de las Políticas de Gobierno y Seguridad Digital, en el periodo comprendido entre el 1 de junio de 2021 y el 28 de febrero del 2022**.**

Equipo Auditor

Linda Reales Magdaniel / Profesional Especializado.
Jorge Gómez Quintero / Jefe Oficina de Control Interno

Metodología Aplicada

Para el desarrollo de la auditoría, se aplicarán técnicas de auditoria internacionalmente aceptadas mediante análisis, muestra y revisión aleatoria de documentos soporte del cumplimiento de actividades y verificación de la gestión adelanta en la implementación de la política.

Marco Normativo:

- Decreto 1008 de 2018 "Política de Gobierno Digital" emanada de MinTic (cuyas disposiciones se compilan en el Decreto 1078 de 2015, “Decreto Único Reglamentario del sector TIC”, específicamente en el capítulo 1, título 9, parte 2, libro 2), forma parte del Modelo Integrado de planeación y Gestión (MIPG).
- Resolución número 00500 de marzo 10 de 2021 emanada de MinTic, “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”. Decreto 415 de 2016.

Cra 8 No. 10 - 65
Código postal 111711
Tel: 381 3000
www.bogota.gov.co
Info: Línea 195

"Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones".

- Resolución N° 001519 de 24 de agosto de 2020, emanada de MinTic, Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos".
- Manual para la Implementación de la Política de Gobierno Digital Versión 7 de abril de 2019.
- Anexo 1 Modelo de Seguridad y Privacidad de la Información, Versión 4 de fecha 22 de febrero del 2021.
- CONPES 3854 de abril del 2016, Política de Seguridad Digital.

CONCLUSIÓN

Con el propósito de ampliar en esta ocasión la cobertura de la auditoría sobre la implementación de las Políticas de Gobierno Digital y Seguridad Digital de la Secretaria General, se adelantaron pruebas de seguimiento en relación con entregables y/o requerimientos normativos de la implementación, basados en el Manual de Gobierno Digital y el anexo 1 del Modelo de Seguridad y Privacidad de la información. Así mismo, se verificaron los avances alcanzados como resultado del FURAG vigencia 2020, en cuanto a la ejecución del plan de acción con cortes a 31 de diciembre del 2021 y primer trimestre del 2022, para avanzar en el cierre de brechas frente a dicho resultado.

Producto del seguimiento efectuado se obtuvo el siguiente resultado:

- **Entregables Normativos:** En cuanto a los entregables para las políticas de Gobierno y Seguridad Digital, se identificó para cada una de sus fases realizadas, del total de 49 entregables, el 47% (23) se cumplieron, en proceso de actualización se encuentran el 6% (3), en proceso de elaboración un 16% (8) y otros entregables/requerimientos que al corte de la auditoría febrero del 2022, no se han elaborado el 31% (15).

  De acuerdo con los avances logrados, se hace recomendable que la Oficina de Tecnologías de la Información y las Comunicaciones- OTIC, priorice los esfuerzos de los entregables considerados como la parte central del sistema, en su estructuración de la fase de planeación de la Política de Gobierno Digital con base en el autodiagnóstico y plan de acción definido para lograr el cumplimiento del Marco de Referencia de Arquitectura Empresarial, que es uno de tres habilitadores transversales.

Cra 8 No. 10 - 65
Código postal 111711
Tel: 381 3000
www.bogota.gov.co
Info: Línea 195

- **<u>Resultado Implementación Plan de Acción FURAG 2020</u>**: En relación con las acciones desarrolladas para cerrar brechas frente a resultados del FURAG, correspondiente a las políticas de Gobierno y Seguridad Digital a cierre de la vigencia 2021, se encontró que para la política de Gobierno Digital se programó 39 actividades logrando una ejecución del 85%. De las 39 actividades, 6 no se alcanzaron a culminar al cierre de año 2021, las cuales registraron un avance promedio del 55,87%, por lo cual, fue necesario reprogramar su terminación para la vigencia 2022.

  En lo que respecta a la política de Seguridad Digital, se programaron 8 actividades, de las cuales se ejecutaron siete (7) y una (1) no se ejecutó, por lo cual, se reprogramó la culminación para la vigencia 2022.

  Los planes de acción a desarrollar durante la vigencia 2022, se encontró un cumplimiento del 100% frente a lo programado para el primer trimestre. La política de Gobierno Digital contempla 16 actividades y la de Seguridad Digital 4 actividades; cabe resaltar que, de las 6 actividades reprogramadas correspondientes a la vigencia 2021 y programadas para el 2022, dos ya fueron ejecutadas al 100% por la OTIC, durante el primer trimestre 2022.

  Vale la pena señalar que, al cierre de la auditoría, se obtuvo los resultados de desempeño institucional del FURAG, emitidos por el DAFP correspondientes a la vigencia 2021, logrando la Secretaria General una calificación satisfactoria en la política de gobierno digital **94,5** y en la política de seguridad digital **95,9**, cuando para la vigencia 2020 registró el 93,2 para la política de gobierno digital y del 93,9 en la política de seguridad digital. Al comparar estos resultados (vigencia 2020 y 2021) se observó un incremento o mejora de 1,39 y 2,09 respectivamente.

Como resultado de las revisiones efectuadas, en relación con entregables y/o requerimientos normativos de la implementación, basado en el Manual de Gobierno Digital y el anexo 1 del Modelo de Seguridad y Privacidad de la información, conjuntamente con el seguimiento practicado al FURAG, respaldado en la ejecución de planes de acción para cerrar las brechas del resultado arrojado para la vigencia 2020, con corte a 31 de diciembre del 2021 y para el primer trimestre del 2022, se considera conveniente que la OTIC evalué el diseño de un instrumento de control ajustado con las necesidades de la entidad que, contribuya a medir los progresos alcanzadas en la implementación de las políticas, el cual armonice los requerimientos normativos establecidos y los resultados que se obtengan del FURAG, definiendo por vigencia las actividades a desarrollar, plazos de cumplimiento, responsables y la estimación de recursos en los casos que se consideren necesarios.

Cra 8 No. 10 - 65
Código postal 111711
Tel: 381 3000
www.bogota.gov.co
Info: Línea 195

Es importante que este instrumento de control determine el horizonte de tiempo en que las políticas serán implementadas de conformidad con las necesidades y objetivos trazados por la Secretaria General, de igual manera, se determine los parámetros o criterios por los cuales se medirá periódicamente su cumplimiento. El objetivo propuesto, busca en el momento que se requiera o desee, conocer a través de este instrumento la medición del grado de avance en la implementación de las políticas con base en los progresos alcanzados de los requerimientos normativos y los planes de acción desarrollados asociados con los lineamientos establecidos por Mintic[1], así mismo se logre identificar fácilmente que actividades no se requieren ejecutar de acuerdo con restricciones de arquitectura, presupuesto y/o prioridades, entre otros.

RESULTADOS DE LA AUDITORA Y RECOMENDACIONES FORMULADAS

A continuación, se presentan los aspectos observados y las recomendaciones formuladas, con el propósito que contribuyan en la implementación de las políticas:

1. Política de Gobierno Digital

1.1. Estado Frente a Requerimientos Normativos

De conformidad con el artículo 2.2.9.1.2.2. del Decreto 1008 de 2018, la Secretaria General viene implementando la política a través del Manual de Gobierno Digital, cuyas fases se encuentran en el siguiente estado a corte de febrero de 2022, frente al desarrollo de los requerimientos y entregables por fase:

Tabla No.1 Verificación del estado de requerimientos/entregables normativos de la Política de Gobierno Digital.

Fases	Requerimientos/Entregables de las Fases	Estado de los requerimientos/entregables a la fecha de la auditoría.
1. Conocer la política.	Conocer los elementos de la política: componentes, habilitadores Transversales y propósitos.	
	Determinar las roles e instancias que ejecutan la política.	
2. Planear la política	Alinear la política de Gobierno Digital con la misión, las políticas de gestión y desempeño institucional y los procesos y servicios de la entidad.	En la etapa de planeación, los siguientes requerimientos se encuentran en **proceso de elaboración**: • Alinear la política de Gobierno Digital con la misión, las políticas de gestión y desempeño institucional y los procesos y servicios de la entidad. • Identifique la situación de la entidad frente a la implementación del Decreto 1413 de 2017 sobre servicios ciudadanos digitales y priorice o establezca un plan de acción para la implementación.
	Autodiagnóstico y Plan de Acción para cerrar la brecha del Modelo de Seguridad y Privacidad de la Información –MSPI.	
	Autodiagnóstico y Plan de Acción para cerrar la brecha del Marco de Referencia de Arquitectura Empresarial.	

[1] https://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7652.html

Cra 8 No. 10 - 65
Código postal 111711
Tel: 381 3000
www.bogota.gov.co
Info: Línea 195

Fases	Requerimientos/Entregables de las Fases	Estado de los requerimientos/entregables a la fecha de la auditoría.
	Identifique la situación de la entidad frente a la implementación del Decreto 1413 de 2017 sobre servicios ciudadanos digitales y priorice o establezca un plan de acción para la implementación.	Este requerimiento **no se ha elaborado al corte:** • Autodiagnóstico y Plan de Acción para cerrar la brecha del Marco de Referencia de Arquitectura Empresarial.
3. Ejecutar la política. Una vez la entidad cuente con los siguientes documentos, debe desarrollarlos y aplicar los lineamientos que corresponden a los componentes TIC para el Estado y TIC para la Sociedad.	PETI y su grado de cumplimiento. Plan de seguridad y privacidad de la información. Plan de acción para la implementación de Servicios Ciudadanos Digitales	En la etapa de ejecución, el requerimiento anexo se encuentra en **proceso de elaboración**: • Plan de acción para la implementación de Servicios Ciudadanos Digitales: *Los requisitos asociados a carpeta ciudadana y servicio de autenticación electrónica no aplican para la Secretaria General. En el caso del servicio de interoperabilidad la entidad cuenta con este servicio, no obstante, aún se encuentra en proceso de adopción del Marco de Interoperabilidad emitido por MinTIC.*
4. Medir la política.	Definir indicadores de seguimiento para medir y evaluar el avance del Plan de seguridad y privacidad de la información, el Plan Estratégico de Tecnología -PETI y la implementación de servicios ciudadanos digitales. Realizar el autodiagnóstico General de la Política de Gobierno Digital. Realizar el autodiagnóstico específico en materia de seguridad y privacidad de la información. Hacer el reporte oficial de la implementación de la política de Gobierno Digital a través del FURAG.	En la etapa de medición el siguiente requerimiento descrito se encuentra en **proceso de elaboración**: • Realizar el autodiagnóstico General de la Política de Gobierno Digital en la fase de medición. En la etapa de medición, el requerimiento relacionado **no se ha elaborado a febrero del 2022:** • Definir indicadores de seguimiento para medir y evaluar el avance del Plan de seguridad y privacidad de la información y la implementación de servicios ciudadanos digitales.

Fuente: Información consolidada por la OCI, con base en el Manual de Gobierno Digital y la información suministrada por la OTIC.

Como resultado de la auditoría, a corte de febrero del 2022 se identificó que existe un total de 13 entregables o requerimientos, el 54% (7/13) se ejecutaron, el 31% (4/13) se encuentra en proceso de ejecución y el 15% (2/13) está pendiente de elaboración por parte de la OTIC. Se recomienda a la Oficina de la OTIC, priorizar el desarrollo de los entregables: Autodiagnóstico y Plan de Acción para cerrar la brecha del Marco de Referencia de Arquitectura Empresarial y el Plan de acción para la implementación de Servicios Ciudadanos Digitales.

Durante la etapa de comunicación de resultados del informe preliminar, la OTIC mediante el memorando 3-2022-15162 de fecha 23 de mayo del 2022 manifestó: "… *si bien en el informe indican que se lleva un cumplimiento por las actividades desarrolladas, se hace imperioso contar con la discriminación de las actividades a nivel de cada elemento transversal y cada propósito definido, para conocer cuáles son los puntos débiles detectados por la auditoría realizada*".

Al respecto, recomendamos que en virtud del principio de autocontrol se sugiere como líderes de la implementación de las políticas se desarrollen los análisis periódicos respectivos, para determinar las debilidades en el desarrollo de las actividades ejecutadas, basados en su conocimiento técnico y como experticia en la materia. Por nuestra parte, tendremos en cuenta dicha apreciación para próximos procesos de auditoría en la medida que las circunstancias técnicas nos lo permitan.

Cra 8 No. 10 - 65
Código postal 111711
Tel: 381 3000
www.bogota.gov.co
Info: Línea 195

De igual manera la OTIC, indicó que en la Fase No.4. correspondiente a Medir la política, que se encuentra detallada en la última sección el cuadro anterior, sobre el requerimiento que figura con el estado de no elaborado relacionado con: "Definir indicadores de seguimiento para medir y evaluar el avance del Plan de seguridad y privacidad de la información y la implementación de servicios ciudadanos digitales", manifestó: "…*los indicadores actuales son los que nos brinda el instrumento de medición del MSPI que brinda y da el MINTIC"*.

Sobre el particular, reiteramos que los indicadores a los cuales se hace referencia corresponden al Manual para la Implementación de la Política de Gobierno Digital, son los indicadores propuestos en el numeral 4.1. Seguimiento y Evaluación por parte de la Entidad que miden el avance del Plan de Seguridad y privacidad de la información y la implementación de Servicios Ciudadanos Digitales basado en aspectos sugeridos por MinTIC tales como; Ahorro en términos de tiempos y recursos - Disminución de costos - Nivel de satisfacción de usuarios internos y externos, es de precisar que dichos indicadores se calculan en la fase final de medición.

1.2 Resultado FURAG 2020 y plan de acción 2021 de la Política de Gobierno Digital.

Como resultado del diligenciamiento del cuestionario FURAG correspondiente a la vigencia 2020 y de la herramienta de autodiagnóstico, la entidad a través de la Oficina de Tecnología de la Información y las Comunicaciones, implementó un plan de acción el cual se ejecutó durante la vigencia 2021. El plan consta para la política de Gobierno Digital de 39 actividades de las cuales, a 31 de diciembre del 2021, se cumplieron 33 actividades, es decir el 85% de lo programado, quedando las siguientes actividades pendientes de culminación, las cuales fueron reprogramadas en el Plan MIPG 2022: actividad No. 48 (con avance del 29%), actividad No. 50 (con avance del 91,21%), actividad No. 71 (avance del 60%), actividad No. 72 (avance del 60%), actividad No. 73 (sin avance), y la actividad No. 86 (avance del 95%).

Para la vigencia 2022 en el Plan de MIPG para cerrar la brecha frente al FURAG correspondiente a la vigencia 2020, se incluyeron 16 actividades programadas, las cuales para el primer trimestre (enero-marzo), presentan un cumplimiento del 100% frente a lo programado.

2. Política de Seguridad Digital

2.1. Estado de requerimientos normativos

En cumplimiento del CONPES 3854 del 2016 y la Resolución 500 del 2021 emitida por Ministerio de Tecnología de la Información y las Comunicaciones, la entidad ha adoptado la Política de Seguridad Digital.

Cra 8 No. 10 - 65
Código postal 111711
Tel: 381 3000
www.bogota.gov.co
Info: Línea 195

A continuación, se describe el detalle de las fases y el cumplimiento de los entregables/requerimientos normativos para identificar el avance de la implementación de la política:

Tabla No. 2 Verificación del estado de requerimientos/entregables normativos de la Política de Seguridad Digital.

Fase	Entregable	Estado de los requerimientos/entregables a la fecha de la auditoría.
1.Diagnóstico	• Herramienta Autodiagnóstico MSPI. • Alcance MSPI: Identificar qué información (generada o utilizada en los procesos de la Entidad) será protegida mediante la adopción del MSPI. • Acto administrativo con las funciones de seguridad y privacidad de la información. • Política de seguridad y privacidad de la información. • Declaración de aplicabilidad, aceptada y aprobadas en el comité de gestión institucional para el Año 2021.	En la etapa de diagnóstico se encuentra **<u>en proceso de elaboración</u>** el siguiente requerimiento: • La estrategia de seguridad digital, de acuerdo con la Resolución número 00500 de marzo 10 de 2021 emanada de MinTic*: En el plan de trabajo de la SGSI para la vigencia 2022 en la actividad No. 2 está programado la actualización de los documentos del Sistema con base en la estrategia.*
2. Planificación	• Contexto de la entidad. • Partes interesadas. • Evidencia en el acto administrativo que soporta la conformación del comité de gestión y desempeño o quien haga sus veces, señalando las funciones de seguridad y privacidad de la información. • Acto administrativo con la adopción de la Política de seguridad y privacidad de la información. • Roles y responsabilidades. • *Modelo de Seguridad y Privacidad de la Información -MSPI (Implementación de las fases).* • Incluir dentro de los proyectos de inversión de la Entidad aquellas actividades relacionadas con la adopción de MSPI de acuerdo con el alcance establecido. • Procedimiento de inventario y clasificación de la información. • Documento metodológico de inventario y clasificación de la información. • Procedimiento y metodología de gestión de riesgos institucional incluyendo el capítulo de seguridad y privacidad de la información aprobado por el comité de coordinación de control interno. *Guía de gestión de riesgos de seguridad de la información.* • Plan de tratamiento de riesgos, aprobado por los dueños de los riesgos y el comité institucional de gestión y desempeño (Decreto 612 de 2018 Publicación antes de 31 de enero de cada vigencia). • *Matriz de riesgos de Seguridad Digital y plan de acción: En la matriz se deben definir controles considerando aspectos tales como la estructura, tamaño, canales de atención, volumen transaccional, número de usuarios, evaluación del riesgo y servicios prestados por la entidad.* • *Realizar un análisis de riesgo para determinar la pertinencia de contratar o implementar el servicio de un equipo especializado para atender incidentes de seguridad digital. El análisis debe identificar las características del proveedor, herramientas, servicios y privacidad de la información, entre otros.* • *Procedimiento de gestión de incidentes de seguridad digital: Realizar el tratamiento, investigación y gestión de los incidentes*	En la etapa de planificación se encuentran **<u>en proceso de elaboración</u>** los siguientes entregables: • *Matriz de riesgos de Seguridad Digital y plan de acción: En la matriz se deben definir controles considerando aspectos tales como la estructura, tamaño, canales de atención, volumen transaccional, número de usuarios, evaluación del riesgo y servicios prestados por la entidad.* En la etapa de planificación se encuentran **<u>en proceso de actualización</u>** los siguientes entregables: • Procedimiento de inventario y clasificación de la información. • Documento metodológico de inventario y clasificación de la información. • Procedimiento y metodología de gestión de riesgos institucional incluyendo el capítulo de seguridad y privacidad de la información aprobado por el comité de coordinación de control interno. *Guía de gestión de riesgos de seguridad de la información.* En la etapa de planificación, **<u>no se han elaborado</u>** los siguientes entregables: • Realizar un análisis de riesgo para determinar la pertinencia de contratar o implementar el servicio de un equipo especializado para atender incidentes de seguridad digital. El análisis debe identificar las características del proveedor, herramientas, servicios y privacidad de la información, entre otros. • Procedimiento para la retención y destrucción final de la información digital. • Formato de Reporte y Reporte ante el CSIRT (Equipo de Respuesta a Incidentes de Seguridad Digital) de Gobierno, los incidentes catalogados como Muy Grave, Grave, Menos Grave y Menor presentados en la entidad.

Cra 8 No. 10 - 65
Código postal 111711
Tel: 381 3000
www.bogota.gov.co
Info: Línea 195

Fase	Entregable	Estado de los requerimientos/entregables a la fecha de la auditoría.
	de seguridad digital que se presente en relación con los activos de información de cada proceso. *_Bitácora de incidentes* *_Formato de Reporte y Reporte ante el CSIRT (Equipo de Respuesta a Incidentes de Seguridad Digital) de Gobierno, los incidentes catalogados como Muy Grave, Grave, Menos Grave y Menor presentados en la entidad.* *_Plan de Mejoramiento de Incidentes: Identificación de causa raíz, definición de actividades y gestión hasta su cumplimiento.* *_Para la gestión de incidentes incluir en la estrategia de seguridad digital las actividades a realizar en las etapas de prevención; protección y detección; respuesta y comunicación; recuperación y aprendizaje.* • *Procedimiento para la retención y destrucción final de la información digital.* • *Proceso/Procedimiento de ciclo de vida del desarrollo del software: Integrar la seguridad digital, dentro del ciclo de vida del desarrollo del software para todos los sistemas de información, aplicaciones web y móviles.* • Plan de cambio, cultura, apropiación, capacitación y sensibilización de Seguridad y Privacidad de la Información y seguridad digital. Este se puede incluir en el Plan Institucional de Capacitaciones - PIC. *El Plan debe incluir actualizaciones sobre las nuevas amenazas cibernéticas.* • Plan de comunicaciones del modelo de seguridad y privacidad de la información.	
3. Operación:	• Plan de implementación de controles de seguridad y privacidad de la información que contenga como mínimo: controles, actividades, fechas, responsable de implementación y presupuesto. Implementar los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación. Determinar e implementar controles para mitigar los riesgos que pudieran afectar la seguridad digital y física de acuerdo con el resultado del análisis y evaluación de riesgos y cumplir con las siguientes características y responsabilidades *_Reportar los resultados del análisis de riesgos y gestión de incidentes al comité institucional de gestión y desempeño o quien haga sus veces.* *_Asesorar a la dirección de la entidad sobre seguridad de la información y seguridad digital, para que pueda hacer seguimiento y tomar las decisiones adecuadas en esta materia.* • Evidencia de la implementación de los controles de seguridad y privacidad de la información.	En la etapa de operación a febrero del 2022, **no se han elaborado** los siguientes entregables: • Plan de implementación de controles de seguridad y privacidad de la información que contenga como mínimo: controles, actividades, fechas, responsable de implementación y presupuesto. Implementar los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación. Determinar e implementar controles para mitigar los riesgos que pudieran afectar la seguridad digital y física de acuerdo con el resultado del análisis y evaluación de riesgos y cumplir con las siguientes características y responsabilidades: _Reportar los resultados del análisis de riesgos y gestión de incidentes al comité institucional de gestión y desempeño o quien haga sus veces. _Asesorar a la dirección de la entidad sobre seguridad de la información y seguridad digital, para que pueda hacer seguimiento y tomar las decisiones adecuadas en esta materia. • Evidencia de la implementación de los controles de seguridad y privacidad de la información.
4. Evaluación de desempeño: Determinar el	• Hoja de vida de indicadores, los cuales deben incluirse en el tablero de control del plan de acción, tal como lo ordena el	En la etapa de evaluación se encuentran **en proceso de elaboración** los siguientes entregables:

Cra 8 No. 10 - 65
Código postal 111711
Tel: 381 3000
www.bogota.gov.co
Info: Línea 195

Fase	Entregable	Estado de los requerimientos/entregables a la fecha de la auditoría.
sistema y forma de evaluación de la adopción del modelo.	decreto 612 de 2018. *Definición y cálculo de indicadores de seguridad de la información y seguridad digital.* • Informe con la evaluación y medición de la efectividad de la implementación de los controles definidos en el plan de tratamiento de riesgos. • *Resultados/ Informes de las auditorías internas con aspectos técnicos de seguridad digital: auditorías de seguridad de la información al menos una vez al año, que contemplen aspectos técnicos de la seguridad digital como análisis de vulnerabilidades a sistemas de información críticos, entre otros.* • No conformidades de las auditorías internas. • Plan de auditorías que evidencia la programación de las auditorias de seguridad y privacidad de la información, este plan debe estar aprobado por el Comité de Coordinación de Control Interno. • Revisión a la implementación • Acta y documento de Revisión por la Dirección. • Compromisos de la Revisión por la Dirección. • *Acto Administrativo de aprobación de la Estrategia, que incluya la definición de roles y responsabilidades.* • *Determinar los recursos técnicos, humanos y administrativos de seguridad de la información y seguridad digital, necesarios para la entidad. Dichos recursos deben manejarse de manera diferenciada a los de operaciones y tecnología de la información.*	• Resultados/ Informes de las auditorías internas con aspectos técnicos de seguridad digital: auditorías de seguridad de la información al menos una vez al año, que contemplen aspectos técnicos de la seguridad digital como análisis de vulnerabilidades a sistemas de información críticos, entre otros. • Acto Administrativo de aprobación de la Estrategia, que incluya la definición de roles y responsabilidades En la etapa de evaluación, **no se han elaborado** los siguientes entregables: • Informe con la evaluación y medición de la efectividad de la implementación de los controles definidos en el plan de tratamiento de riesgos. • No conformidades de las auditorías internas. • Plan de auditorías que evidencia la programación de las auditorias de seguridad y privacidad de la información, este plan debe estar aprobado por el Comité de Coordinación de Control Interno. • Revisión a la implementación • Acta y documento de Revisión por la Dirección. • Compromisos de la Revisión por la Dirección.
5. Mejoramiento Continuo:	• Plan anual de mejora del MSPI.	En la etapa de mejoramiento a febrero del 2022, **no se ha elaborado** el siguiente entregable: • Plan anual de mejora del MSPI.

Fuente: Modelo de Seguridad y Privacidad Anexo 1 febrero del 2021/Resolución 500 del 2021 emitidos por Ministerio de Tecnología de la Información y las Comunicaciones.

Producto de la auditoría efectuada a los requerimientos y entregables normativos consignados en el anexo 1 Modelo de Seguridad y Privacidad de la Información, Versión 4 de fecha 22 de febrero del 2021 emitido por MinTic, durante la auditoría, se identificó que existe un total 36 entregables, de los cuales el 45% (16) están finalizados y actualizados, el 8% (3) se encuentran en proceso de actualización, 11% (4) están en proceso de elaboración y el 36% (13) no se han elaborado.

2.2. Resultado FURAG 2020 y Plan de Acción ejecutado en 2021 de la Política de Seguridad Digital.

En desarrollo de la Política de Seguridad Digital, una vez identificadas las brechas como resultado del cuestionario de FURAG 2020 y de la herramienta de autodiagnóstico, se establecieron 8 actividades a implementar durante la vigencia 2021, de las cuales, se cumplieron 7 actividades, quedando pendiente de ejecución la actividad correspondiente a realizar ejercicios simulados de Ingeniería social al personal de la entidad, que estaba programada para el mes de noviembre de 2021. Es de anotar que, esta actividad será desarrollada en el plan programado para su ejecución durante toda la vigencia 2022.

Cra 8 No. 10 - 65
Código postal 111711
Tel: 381 3000
www.bogota.gov.co
Info: Línea 195

En el Plan MIPG 2022, en la política de seguridad digital se programaron 4 actividades, que para el primer trimestre de 2022 (enero-marzo) presentaron una ejecución del 100% frente a lo programado.

Recomendación General:

Como resultado de las revisiones efectuadas sobre la implementación de las políticas de Gobierno Digital y Seguridad Digital de la Secretaria General , en relación con entregables y/o requerimientos normativos de la implementación, basado en el Manual de Gobierno Digital y el anexo 1 del Modelo de Seguridad y Privacidad de la información, conjuntamente con el seguimiento practicado al FURAG, respaldado en la ejecución de planes de acción para cerrar las brechas del resultado arrojado para la vigencia 2020, con corte a 31 de diciembre del 2021 y para el primer trimestre del 2022, se considera conveniente que la OTIC evalué el diseño de un instrumento de control ajustado con las necesidades de la entidad que, contribuya a medir los progresos alcanzadas en la implementación de las políticas, el cual armonice los requerimientos normativos establecidos y los resultados que se obtengan del FURAG, definiendo por vigencia las actividades a desarrollar, plazos de cumplimiento, responsables y la estimación de recursos en los casos que se consideren necesarios.

Es importante que, este instrumento de control determine el horizonte de tiempo en que las políticas serán implementadas de conformidad con las necesidades y objetivos trazados por la Secretaria General, de igual manera, se determine los parámetros o criterios por los cuales se medirá periódicamente su cumplimiento.

El objetivo propuesto, busca en el momento que se requiera o desee, conocer a través de este instrumento la medición del grado de avance en la implementación de las políticas con base en los progresos alcanzados de los requerimientos normativos y los planes de acción desarrollados asociados con los lineamientos establecidos por MinTIC, así mismo se logre identificar fácilmente que actividades no se requieren ejecutar de acuerdo con restricciones de arquitectura, presupuesto y/o prioridades, entre otros.

Al respecto, la Oficina de Tecnologías de la Información y las Comunicaciones- OTIC mediante el memorando 3-20202-15162 de fecha 23 de mayo del 2022 manifestó: *“considera conveniente que se revalúe por parte de la auditoría la recomendación de "...crear otro instrumento de medición..." debido a que consideramos que es una carga adicional para el trabajo que desarrolla la OTIC, más aún cuando esta medición actualmente se hace con base en las directrices dadas por el Ministerio TIC…”.*

Cra 8 No. 10 - 65
Código postal 111711
Tel: 381 3000
www.bogota.gov.co
Info: Línea 195

Así las cosas, retiramos por considerar importante contar con una herramienta integral de medición de estas políticas, la recomendación que formulamos de evaluar o estudiarla, tiene como único propósito fortalecer y conocer a ciencia cierta los progresos logrados a lo largo del tiempo previsto de su implantación, por tanto, es discrecional si la OTIC en sus consideraciones la adopta o no.

Ahora bien, en tal sentido nuestro planteamiento de la recomendación se fundamenta en parte en el lineamiento dado por MinTIC, que se encuentra en la página web: https://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7652.html, la cual señala que para desarrollar la política de Gobierno Digital, se debe consultar y aplicar lo establecido en los siguientes documentos: Manual de implementación de la política de gobierno digital y Decreto No. 1499 de 2017 - Modelo Integrado de Planeación y gestión. La OTIC en la actualidad tiene un instrumento de medición basado en el MIPG (FURAG), por ello, se invitó a armonizar dicho instrumento con base en los requerimientos normativos establecidos en el Manual de implementación de la política de gobierno digital y el anexo 1 del Modelo de Seguridad y Privacidad de la información,

Criterios de clasificación de conceptos derivados de la auditoría.

Tipo de observación	Descripción
Observación	Incumplimiento de normas o procedimientos internos que pueden materializar un riesgo.
Oportunidad de mejora	Sin implicar un incumplimiento normativo o de procedimientos internos, es susceptible de mejora el proceso.

Elaborador por: Linda Reales Magdaniel – Profesional Especializado OCI
Revisado y aprobado por: Jorge Eliecer Gómez Quintero – Jefe Oficina de Control Interno

Cra 8 No. 10 - 65
Código postal 111711
Tel: 381 3000
www.bogota.gov.co
Info: Línea 195