Radicado 2021_IE_1826 del 31_08_2021

MEMORANDO

OCI

Bogotá.

PARA: Doctora **NIDIA ROCÍO VARGAS**
Directora

DE: **JEFE OFICINA DE CONTROL INTERNO**

ASUNTO: Inicial 2021 / Entrega informe de auditoría – Auditoría de Seguimiento MSPI

Respetada Doctora Nidia Rocío:

Dando cumplimiento a lo establecido en la Ley 87 de 1993 *"Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones"* y al Plan Anual de Auditorias 2021 del Departamento Administrativo del Servicio Civil Distrital, de manera atenta me permito remitir el informe de auditoría, según el asunto.
.

Cordialmente,

ORIGINAL FIRMADO
YOLANDA CASTRO SALCEDO
Jefe Oficina de Control Interno

Anexo: Informe 42 páginas

Copia: Jefe Oficina de Tecnología de Información y Comunicaciones

ACCIÓN	FUNCIONARIO	CARGO	FIRMA	FECHA
Proyectado por:	Luz Yadira Velosa Poveda	**Contratista**	ORIGINAL FIRMADO	31/08/2021
Revisado por:	Yolanda Castro Salcedo	**Jefe de Oficina**	ORIGINAL FIRMADO	31/08/2021
Declaramos que hemos revisado el presente documento y lo encontramos ajustado a las normas y disposiciones legales, y por lo /tanto, lo presentamos para firma de la efe de la Oficina de Control Interno del Departamento Administrativo del Servicio Civil Distrital (DASCD).				

Seleccionar tipo de Informe:

Evaluación ☐ Seguimiento ☐ Auditoría de Gestión ☒

NOMBRE DEL INFORME:
Informe de auditoría de seguimiento a las observaciones realizadas en la vigencia 2020 del Modelo de Seguridad y Privacidad en la Información – MSPI

Carrera 30 No 25 – 90,
Piso 9 Costado Oriental.
Tel: 3 68 00 38
Código Postal: 111311
www.serviciocivil.gov.co

TABLA DE CONTENIDO

1 OBJETIVO DE LA AUDITORÍA

Realizar una auditoría de seguimiento a las observaciones realizadas en la vigencia 2020 del Modelo de Seguridad y Privacidad de la Información – MSPI del DASCD dando cobertura a los siguientes aspectos:

1. Revisar el avance en la implementación MSPI.
2. Presentar desde el punto de vista técnico las debilidades, oportunidades, fortalezas y amenazas identificadas según el alcance de la auditoría y presentar las recomendaciones para implementar en la organización.
3. Emitir concepto sobre el seguimiento a las acciones formuladas en el plan de mejoramiento producto de las observaciones realizadas en la vigencia 2020 del Modelo de Seguridad y Privacidad de la Información – MSPI.

2 ALCANCE

Realizar la auditoría la auditoría interna sobre las observaciones realizadas en la auditoría ejecutada en la vigencia 2020, revisando el avance en la implementación del Modelo de Seguridad y Privacidad de la información - MSPI, en cumplimiento del Plan anual de auditorías de la OCI y el Plan Operativo Anual POA para la oficina de control interno y elaborar el informe final de la auditoría que contenga las recomendaciones para implementar en el Departamento.

3 CRITERIOS DE LA AUDITORÍA

Se aplica como referente los lineamientos emitidos por el Ministerio de las TIC mediante el Manual para la Implementación de la Política de Gobierno Digital Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2) Versión 7 Abril de 2019, los lineamientos de la Norma internacional ISO/IEC 27001:2013 y las guías del Modelo de Seguridad y Privacidad de la Información, con derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la estrategia de Gobierno en Línea.

4 EQUIPO AUDITOR

Auditor Líder: Yolanda Castro – jefe de la Oficina de Control Interno.
Auditores de apoyo: Yadira Velosa – Contratista.

5 METODOLOGÍA

La auditoría se ejecutó conforme a lo establecido por la entidad en el Procedimiento de Auditorías Internas C-CYS-PR-001 con el apoyo en algunos lineamientos y buenas prácticas del Manual para la Implementación de la Política de Gobierno Digital Versión 7 abril de 2019, las guías del Modelo de Seguridad y Privacidad de la Información MSPI.

Para efectos de la auditoría se revisan las acciones e implementaciones de los controles basadas en las recomendaciones emitidas a las observaciones relacionadas en el informe C-CYS-FM-004 INFORME_AUDITORIA_TIC_2020_V1.1_cto56: Avances en la implementación del MSPI, y las acciones planteadas en el plan de mejoramiento relacionadas con el alcance de la auditoria.

La auditoría de seguimiento no corresponde a una auditoría de cumplimiento del sistema de gestión de calidad, por lo tanto, se da reconocimiento a los instrumentos y procedimientos aplicados por la OTIC para la implementación del MSPI, sin condicionamiento de que dichos instrumentos o procedimientos sean documentos controlados del sistema de gestión.

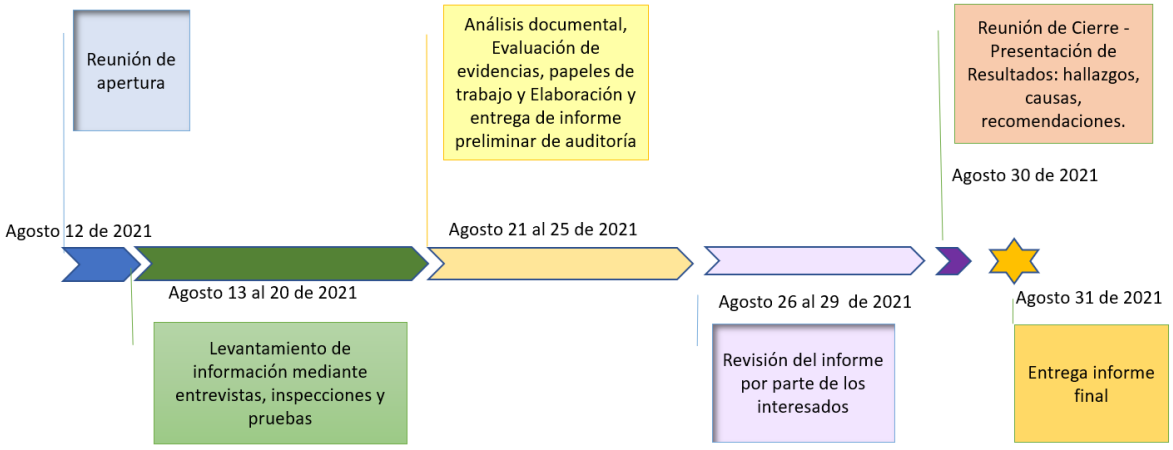
Las actividades realizadas son las siguientes:

1. Sesiones de entrevistas con los responsables de la implementación del MSPI.

2. Levantamiento de información documental como evidencia de planeación, ejecución, seguimiento y acciones de mejora.

El área que suministro la información es la Oficina de Tecnología de la Información y Comunicaciones

La auditoría fue ejecutada de acuerdo con la siguiente línea de tiempo



5.1 PRESENTACION DE RESULTADOS

Considerando que el alcance de la auditoría contempla el seguimiento a las acciones de mejoramiento en respuesta a las recomendaciones del informe de auditoría C-CYS-FM-004 INFORME_AUDITORIA_TIC_2020_V1.1_cto56, la estructura del presente informe para cada clausula y/o dominio del MSPI incluye los siguientes elementos:

- **Observaciones**: Corresponden a los aspectos positivos (fortalezas) y negativos (debilidades) identificadas para el proceso de Gestión de Tecnología de Información y las Comunicaciones. Se utiliza la siguiente nomenclatura:

  Observación Positiva.

  Observación positiva con opción de mejora.

  Observación negativa que amerita una acción de mejora.

- **Recomendaciones:** Corresponde a las oportunidades de mejora que deben ser atendidas por la OTIC en respuesta a los hallazgos negativos o debilidades identificados en el ejercicio de la auditoría y que son la fuente para determinar y priorizar las acciones de mejoramiento. Vale aclarar que los hallazgos positivos no derivan en recomendaciones. Incluye dos elementos:

  - **Seguimiento a las recomendaciones**: corresponde a los resultados el seguimiento a las acciones de mejoramiento implementadas por la OTIC en respuesta a cada una de las recomendaciones emitidas en el informe de auditoría contrato 056 de 2020 en relacionados con el avance en la implementación del MSPI.

  - **Nuevas recomendaciones**: corresponde a nuevas oportunidades de mejora identificadas en la presente auditoría y aquellas que no han sido atendidas y requieren de acciones de mejoramiento.

6 INFORME EJECUTIVO

Como resultado de las auditorías adelantadas en las vigencias anteriores se han emitido por parte de la auditoría observaciones de mejora al avance en la implementación del Modelo de Seguridad y Privacidad de la Información, revisando cada una de las cláusulas y dominios que son parte integral de la norma ISO 27001:2013 y su Anexo 27002:2013, en la cual se basa el MSPI.

En el seguimiento realizado en esta auditoria se evidencia un avance significativo en la implementación de las observaciones atrás mencionadas, que se evidencia en el cumplimiento de las recomendaciones emitidas, no solo a la implementación de MSPI, sino también a las relacionadas con la gestión de las Tecnologías de Información y las Comunicaciones, donde se

resalta el compromiso de los colaboradores de la Oficina de Tecnologías de la Información y las Comunicaciones.

La correcta implementación del modelo establece la articulación del ciclo de Planear, implementar, evaluar y mejorar como la estrategia para la construcción y mantenimiento del MSPI.

En términos generales se evidencian las siguientes mejoras en esta estrategia:

- **PLANEACION DEL MSPI**

  Su objetivo es la construcción de los instrumentos documentales y su estructuración a través de la Declaración de aplicabilidad como resultado del entendimiento del contexto de la organización y la articulación del MSPI con el Sistema de gestión de calidad.

  - Se ha mejorado la declaración de aplicabilidad.
  - Se han estructurado, socializado y publicado la política y Manual de seguridad de la información.
  - Se ha evolucionado en la construcción de los procedimientos, guías, formatos e instructivos del MSPI.
  - Se ha mejorado en el establecimiento y entendimientos de los roles y responsabilidades del MSPI.
  - Se ha optimizado el inventario de activos de información y se ha mejorado la articulación con los riesgos TIC y de seguridad.
  - Se evidencian mejoras en el tratamiento de riegos.

- **IMPLEMENTACION DEL MSPI**

  Su objetivo es la correlación entre los instrumentos documentales y las configuraciones en los activos de información, además de la gestión de la operación en articulación con los eventos y control de los riesgos.

  - Se evidencia que la OTIC ha mejorado en la implementación de los controles de seguridad en los activos de información: redes, software base, software aplicativo, archivos y recurso humano. También se han atendido de manera diligente la mayoría de las recomendaciones emitidas en las auditorías realizadas en los años 2019 y 2020.
  - De igual manera se ha mejorado la configuración de la gestión de eventos como mecanismo para el control operacional y los controles de tratamiento a los riesgos.

- **VERIFICACIÓN DEL MSPI**

  Su objetivo es contar con instrumentos implementados que permitan verificar de manera continua la efectividad de la implementación del MSPI, indicadores y auditorías regulares para la evaluación de avance y cumplimiento.

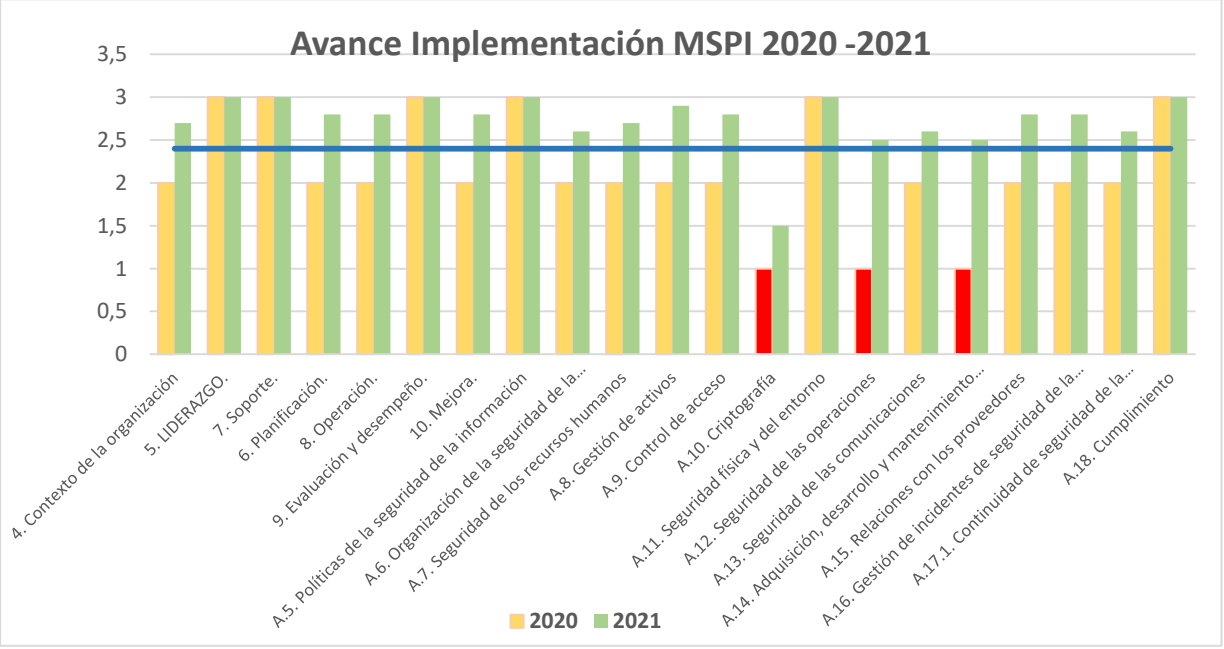
- Se ha mejorado en el uso de la gestión de eventos como mecanismo para el control operacional y los controles de tratamiento a los riesgos.
- Se han realizado pequeñas mejoras a los indicadores.
- La OCI ha aplicado regularmente las inspecciones al tratamiento de riesgos y al avance en la implementación.
- Se han realizado auditoria independientes al MSPI.

- **MEJORA CONTINUA DEL MSPI**

  Su objetivo es la planeación e implementación de acciones de mejora con base en los resultados de los indicadores, herramientas de gestión de eventos, incidentes de seguridad, seguimiento a los riesgos y observaciones de auditorías.

  - Se evidencia el establecimiento de acciones en el plan de mejoramiento.
  - Se atienden en un porcentaje representativo las observaciones de mejora resultado de las auditorías internas y de evaluación independiente.

El siguiente gráfico representa el resumen de las observaciones puntuales del presente informe y permite observar el nivel de avance por cada dominio y cláusula de la norma. Con respecto al año 2020, se observa que de los 21 elementos evaluados, únicamente criptografía no ha superado una mejora significativa. Vale aclarar que los valores meta se usan como referencia grafica para recrear la mejora



7 RESULTADOS DE LA AUDITORIA

7.1 FORTALEZAS

La auditoría arrojó resultados satisfactorios en cuanto a las acciones implementadas por la OTIC en atención a las recomendaciones de mejora emitidas al avance en la implementación del MSPI en el marco del contrato 56 de 2020. Las principales fortalezas son:

- La Oficina de Tecnologías de la Información y las Comunicaciones, ha demostrado su compromiso y esfuerzo por entender y acatar las directrices del Ministerio de Tecnologías de la Información y Comunicaciones (MINTIC), a través del Manual para la Implementación de la Política de Gobierno Digital versión 7 de abril de 2019, con el propósito de "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".
- Se demuestra un gran avance en construcción de los instrumentos documentales del Sistema de Gestión de Seguridad de la Información, los que se han venido perfeccionado y complementado de forma adecuada
- La implementación de los controles definidos para el modelo de seguridad y privacidad de la información se ha realizado correctamente de acuerdo a las mejores prácticas, quedando pendiente solo algunas mejoras que se identifican en este informe.

7.2 OBSERVACIONES

7.2.1 SEGUIMIENTO A LA IMPLEMENTACION DEL MSPI

A continuación se presentan las observaciones resultado de la auditoría de seguimiento a la implementación del MSPI, basado en las recomendaciones de mejora para cada clausula y/o dominio emitidas en el informe de la vigencia 2020 e indicando en cada observación negativa la situación evidenciada, su causa y consecuencia. De igual manera, se relacionan las recomendaciones de mejora sugeridas por la auditoría con el fin de subsanar las debilidades que aún persisten, no se incluyen las identificadas como ya atendidas en el seguimiento la implementación del MSPI del informe de la vigencia 2020.

7.2.1.1 Clausula 4. Contexto de la organización

7.2.1.1.1 Observaciones 2021

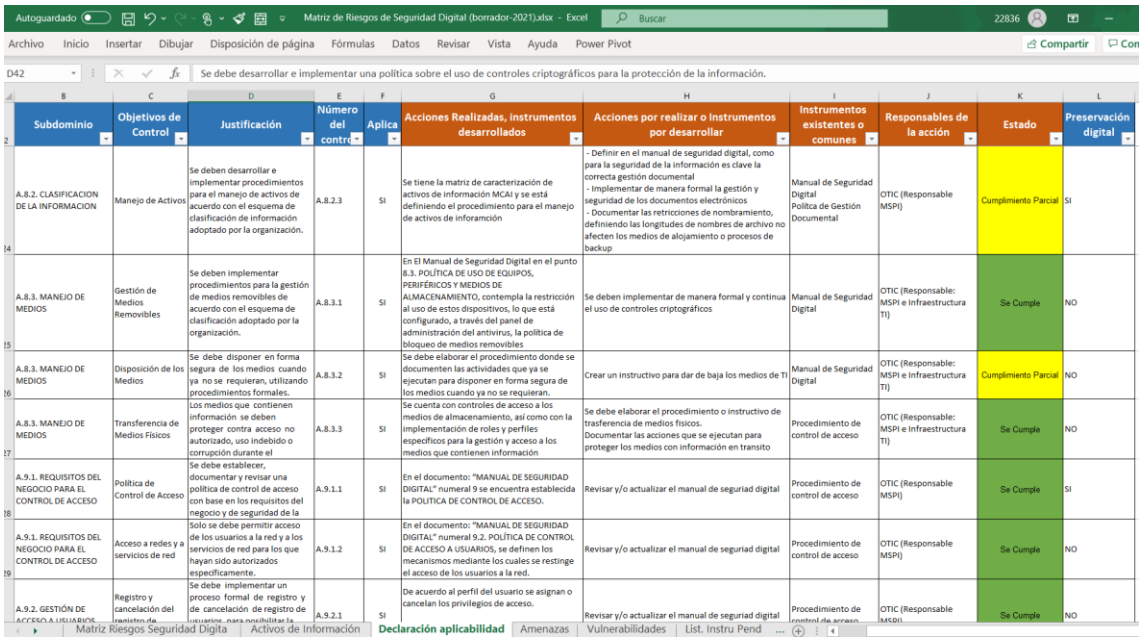
En la cláusula 4 – 'Contexto de la organización del marco de implementación MSPI' – se determina la manera en que la entidad establece la declaración de aplicabilidad y, de acuerdo con los activos y servicios que se ofrecen desde la OTIC, se especifican cuáles objetivos de control y respectivos controles se deben implementar. Además, se expone la forma en que estos últimos se van a abordar. En la revisión realizada para la vigencia 2020 se había presentado una primera versión de la

declaración de aplicabilidad ("*Declaración de Aplicabilidad", adjunto al E-SIN-FM-012 Formato Matriz de Riesgos de Seguridad Digital V2.xlsx*") y el análisis de brecha resultado del instrumento de auto diagnóstico dispuesto por MINTIC , lo que evidenciaba un avance importante.

- Se realizó una actualización de la herramienta de autodiagnóstico de MinTIC para el análisis de brecha en la implementación del MSPI, se revisaron los 114 controles en la declaración de aplicabilidad para determinar el estado de avance de cada control y determinar el listado de instrumentos pendientes. Este listado se adjuntó a la *Matriz de Riesgos de Seguridad Digital (borrador-2021)* en la hoja: *"List. Instru Pend"*, como se muestra en la siguiente imagen:

Instrumento en el que se desarrolla	Acciones por realizar o Instrumentos por desarrollar	Número del control asociado	Estado de la acción
Manual de la Estrategia de Seguridad Digital	Definir e implementar controles técnicos que permitan: - El uso de criptografía para la protección de la información institucional en dispositivos móviles - La independencia entre el uso personal e insticticional de los dispositivos móviles - Establecer roles y responsabilidades por la implementación de la política y la gestión de llaves, incluida la generación de llaves. - Establecer las condiciones de protección de contraseñas de acceso a sistemas y demás servicios que requieran autenticación. - Definir las condiciones de transmisión de información confidencial al interior de la empresa y fuera de ella. - Definir los controles criptograficos de los servicios institucionales que recopilen información de terceros. - Uso de criptografía en la mensajería instantánea institucional. - Firma digital de documentos y correos electrónicos (cuando aplique). - Definir políticas criptograficas para el resguardo de información, cuando esta información sea clasificada como confidencial o reservada. - Uso de criptografía en portátiles, celulares y medios extraíbles.	A.6.2.1, A.8.3.1 y A.10.1.2	ok
	- Documentar en el manual de seguridad digital, los controles establecidos para el trabajo en casa en el marco de la pandemia - Incluir los Controles de red para uso de equipos móviles corporativos y/o bajo la modalidad BYOD y teletrabajo.	A.6.2.2	OK
	Documentar en el manual de seguridad digital que en los documentos "A-TIC-FM-011-Acuer_confide_ contratista" y "A-TIC-FM-012-Acuer_confide_ servidores" se evidencia que después de terminada la relación labora, se obliga al funcionario a mantener la confidencialidad sobre la información del DASCD	A.7.3.1	OK
	Actualizar el manual de Seguridad Digital documentando la periodicidad y responsables de la gestión de los activos de información.	A.8.1.1	OK
	- Definir en el manual de seguridad digital, como para la seguridad de la información es clave la correcta gestión documental - Implementar de manera formal la gestión y seguridad de los documentos electrónicos - Documentar las retricciones de nombramiento, definiendo las longitudes de nombres de archivo no afecten los medios de alojamiento o procesos de backup	A.8.2.3	OK
	Definir y documentar las políticas para el cambio o reuso de equipos por distintas personas en el DASCD	A.11.2.7	Pendiente
	Actualizar el manual de Seguridad Digital con el estado y despliegue de los controles asociados en el firewall	A.12.2.1	Pendiente
	Documentar en el manual de seguridad digital la fuente y sincronización de los relojes	A.12.4.4	Pendiente
	Documentar en el Manual de Seguridad Digital, las auditorías externas que se realizan.	A.12.7.1	OK
	Actualizar y o verificar en el Manual de Seguridad Digital los siguientes temas: - Controles de red para la gestión de la seguridad en las comunicaciones - Controles de red para interconexiones mediante WLAN - Controles de red para uso de equipos móviles corporativos y/o bajo la modalidad BYOD y teletrabajo - Controles para manejo de proveedores de servicios de telecomunicaciones, redes de datos y seguridad. - Segregación de las redes organizacionales - Transferencia de información.	A.13.1.1	OK

- Se actualizó la declaración de aplicabilidad adicionando las columnas: "Acciones Realizadas, instrumentos desarrollados", "Acciones por realizar o Instrumentos por desarrollar", "Instrumentos existentes o comunes", "responsables de la acción" y "Estado", para así poder tener un control sobre la desarrollado en cada control, lo pendiente, el instrumento creado para cada control y su respectivo estado:



Subdominio	Objetivos de Control	Justificación	Número del contro	Aplica	Acciones Realizadas, instrumentos desarrollados	Acciones por realizar o Instrumentos por desarrollar	Instrumentos existentes o comunes	Responsables de la acción	Estado	Preservación digital
A.8.2. CLASIFICACION DE LA INFORMACION	Manejo de Activos	Se deben desarrollar e implementar procedimientos para el manejo de activos de acuerdo con el esquema de clasificación de información adoptado por la organización.	A.8.2.3	SI	Se tiene la matriz de caracterización de activos de información MCAI y se está definiendo el procedimiento para el manejo de activos de inforamción	- Definir en el manual de seguridad digital, como para la seguridad de la información es clave la correcta gestión documental - Implementar de manera formal la gestión y seguridad de los documentos electrónicos - Documentar las retricciones de nombramiento, definiendo las longitudes de nombres de archivo no afecten los medios de alojamiento o procesos de backup	Manual de Seguridad Digital Politca de Gestión Documental	OTIC (Responsable MSPI)	Cumplimiento Parcial	SI
A.8.3. MANEJO DE MEDIOS	Gestión de Medios Removibles	Se deben implementar procedimientos para la gestión de medios removibles de acuerdo con el esquema de clasificación adoptado por la organización.	A.8.3.1	SI	En El Manual de Seguridad Digital en el punto 8.3. POLÍTICA DE USO DE EQUIPOS, PERIFÉRICOS Y MEDIOS DE ALMACENAMIENTO, contempla la restricción al uso de estos dispositivos, lo que está configurado, a través del panel de administración del antivirus, la política de bloqueo de medios removibles	Se deben implementar de manera formal y continua el uso de controles criptográficos	Manual de Seguridad Digital	OTIC (Responsable: MSPI e Infraestructura TI)	Se Cumple	NO
A.8.3. MANEJO DE MEDIOS	Disposición de los Medios	Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	A.8.3.2	SI	Se debe elaborar el procedimiento donde se documenten las actividades que ya se ejecutan para disponer en forma segura de los medios cuando ya no se requieran.	Crear un instructivo para dar de baja los medios de TI	Manual de Seguridad Digital	OTIC (Responsable: MSPI e Infraestructura TI)	Cumplimiento Parcial	NO
A.8.3. MANEJO DE MEDIOS	Transferencia de Medios Físicos	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el	A.8.3.3	SI	Se cuenta con controles de acceso a los medios de almacenamiento, así como con la implementación de roles y perfiles específicos para la gestión y acceso a los medios que contienen información	Se debe elaborar el procedimiento o instructivo de trasferencia de medios físicos. Documentar las acciones que se ejecutan para proteger los medios con información en transito	Procedimiento de control de acceso	OTIC (Responsable: MSPI e Infraestructura TI)	Se Cumple	NO
A.9.1. REQUISITOS DEL NEGOCIO PARA EL CONTROL DE ACCESO	Política de Control de Acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la	A.9.1.1	SI	En el documento: "MANUAL DE SEGURIDAD DIGITAL" numeral 9 se encuentra establecida la POLITICA DE CONTROL DE ACCESO.	Revisar y/o actualizar el manual de seguriad digital	Procedimiento de control de acceso	OTIC (Responsable MSPI)	Se Cumple	SI
A.9.1. REQUISITOS DEL NEGOCIO PARA EL CONTROL DE ACCESO	Acceso a redes y a servicios de red	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados especificamente.	A.9.1.2	SI	En el documento: "MANUAL DE SEGURIDAD DIGITAL" numeral 9.2. POLÍTICA DE CONTROL DE ACCESO A USUARIOS, se definen los mecanismos mediante los cuales se restinge el acceso de los usuarios a la red.	Revisar y/o actualizar el manual de seguriad digital	Procedimiento de control de acceso	OTIC (Responsable MSPI)	Se Cumple	NO
A.9.2. GESTIÓN DE ACCESO A USUARIOS	Registro y cancelación del registro de	Se debe implementar un proceso formal de registro y de cancelación de registro de	A.9.2.1	SI	De acuerdo al perfil del usuario se asignan o cancelan los privilegios de acceso.	Revisar y/o actualizar el manual de seguriad digital	Procedimiento de	OTIC (Responsable MSPI)	Se Cumple	NO

- Se actualizo la política de seguridad y privacidad de la información *(E-SIN-DE-001 POLITICA_ GENERAL_DE_SEGURIDAD_Y_PRIVACIDAD_DE_LA_INFORMACION_V11)* de forma adecuada, para independizar y complementar lo relacionado con la política de tratamiento de datos personales en el nuevo documento: *"E-SIN-DE-002 POLITICA_DE_TRATAMIENTO _DE_ DATOS_PERSONALES_V1"*, en donde se establecen correctamente los lineamientos, alcance, finalidades, responsables, tratamiento y derechos de esta. Además se establecen los canales de atención y respuesta a PQRS relacionando adecuadamente el nuevo formato de reclamaciones: E-SIN-FM-007_FORMATO_RECLAMACION_DATOS_ PERSONALES_V1", documentos que se encuentran debidamente formalizados.

- Se cuenta con una nueva versión en borrador manual de seguridad digital (E-SIN-MA-001 MANUAL_ SEGURIDAD_DIGITAL V2 - Borrador(2021), en la cual se han actualizado y complementado las políticas con las recomendaciones dadas por la auditoria y de acuerdo a la resolución 00500 de marzo de 2021 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, sin embargo aún no se ha formalizado.

- En la declaración de aplicabilidad solo se tienen dos controles que no aplican dentro del modelo de seguridad y privacidad de la información, el A.10.1.2 cuyo objetivo de control es la gestión de llaves de controles criptográficos y el A.18.1.5: Reglamentación de Controles Criptográficos en el subdominio: A.18.1. CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES.

En cuanto a la gestión de llaves, si bien aún no se ha definido la herramienta de criptografía que se va a implementar en la Entidad, no determina que este control no aplique, adicionalmente el objetivo principal de este control es tener un procedimiento permita resguardar y actualizar correctamente las llaves o contraseñas generadas en los procesos de encriptación de documentos o dispositivos, por lo cual debe actualizarse a que si aplica. En cuanto a la Reglamentación de Controles Criptográficos en contratos y requisitos legales la no aplicabilidad es correcta debido a él origen público de la Entidad.

7.2.1.1.2 Seguimiento a las Observaciones 2020

A continuación se relacionan las recomendaciones orientadas a complementar la declaración de aplicabilidad emitidas en el informe de la vigencia 2020 y su respectivo seguimiento:

N°	OBSERVACIÓN DE MEJORA – RECOMENDACIÓN 2020	ESTADO	SEGUIMIENTO 2021
1.	Listado de los 114 controles, y declaración de la manera en que será implementado en la entidad.	↑	Ya se adelantó en la declaración de aplicabilidad el listado de los 114 controles y la identificación de acciones para la implementación de cada control
2.	Identificación de los instrumentos del sistema de gestión que deben ser construidos para cumplir con el control.	↑	Se adiciono a la Matriz de Riesgos de Seguridad Digital (borrador-2021) en la hoja: *"List. Instru Pend"* en el cual se identificaron los instrumentos pendientes y los construidos, adicionalmente en la declaración de aplicabilidad se relacionan en la columna *"Instrumentos existentes o comunes"* .
3.	Identificación de que instrumentos preexisten en la oficina de sistemas y que deben ser ajustado atender los controles del Sistema de gestión de Seguridad de la Información (SGSI).	↑	Se tienen identificados en la Matriz de Riesgos de Seguridad Digital (borrador-2021) en la hoja: *"List. Instru Pend"* con su respectivo estado y control relacionado.
4.	Identificación de que instrumentos preexisten en el sistema de gestión integral de la entidad y que deben ser ajustados para articularse a la inclusión del SGSI.	→	Si bien se ha avanzado en la identificación de los instrumentos, aún no se encuentran ajustados para articularse con el sistema de gestión integral de la entidad o con el sistema de calidad ISO 9001, relacionando los instrumento o documentos con su respectivo prefijo.
5.	Identificación de instrumentos comunes con ISO 9001, que no existen y deben ser construidos.	→	

N°	OBSERVACIÓN DE MEJORA – RECOMENDACIÓN 2020	ESTADO	SEGUIMIENTO 2021
6.	Identificación de los actores de otras áreas que deben ser involucrados en la construcción e implementación del instrumento.		La identificación de los actores ya se encuentra correctamente relacionada en el numeral 6.2 Roles y Responsabilidades de las políticas de seguridad digital – dimensión organizacional en el documento E-SIN-MA-001 Manual_seguridad_digital v2 - borrador(2021).
7.	Identificación de las implementaciones tecnológicas que deben ser adelantadas de acuerdo con los resultados del análisis de brecha y de las auditorías de sistemas.		Las implementaciones tecnológicas se encuentran relacionadas en la declaración de aplicabilidad en las columnas "Acciones Realizadas, instrumentos desarrollados", "Acciones por realizar o Instrumentos por desarrollar" y en el listado de instrumentos pendientes.

7.2.1.1.3 Nuevas Recomendaciones

N°.	RECOMENDACIÓN
1.	Complementar, formalizar y publicar los documentos (E-SIN-MA-001 MANUAL_ SEGURIDAD_DIGITAL V2 - Borrador(2021) y *al E-SIN-FM-012 Formato Matriz de Riesgos de Seguridad Digital V2.xlsx*" que se tienen en borrador y que corresponden al mayor avance en la implementación del MSPI
2.	Actualizar a si aplica en la declaración de aplicabilidad el control A.10.1.2 para la gestión de llaves de controles criptográficos
3.	Atender las recomendaciones de la vigencia anterior que se presentan con la valoración

7.2.1.2 A.6. Organización de la seguridad de la información.

7.2.1.2.1 Observaciones 2021

- En el manual de seguridad digital se incluyeron correctamente las políticas de responsabilidad por los activos de información en la que se especifican de forma adecuada los deberes y responsabilidades de los usuarios de los activos de información.
- Se tienen definidos correctamente los niveles de autorización en la matriz de caracterización de activos de información y se incluyeron en el manual los roles y responsabilidades de las diferentes áreas de la entidad en cuanto a la protección y seguridad de los activos.
- Se agregaron correctamente las siguientes funciones de seguridad en el borrador de la resolución 277 de 2018 por la cual se crea el comité institucional de gestión y desempeño del departamento administrativo del servicio civil distrital – DASCD:

18. Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la entidad.
19. Acompañar e impulsar el desarrollo de proyectos de seguridad de la información.
20. Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos del Departamento.
21. Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.
22. Aprobar y hacer seguimiento al Plan de Seguridad y Privacidad de la Información y al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
23. Realizar revisiones periódicas al Sistema de Gestión de Seguridad de la Información - SGSI y a los diagnósticos del estado de la seguridad de la información en el DASCD, (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.
24. Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.

👉 En cuanto a las responsabilidades en seguridad de la información de terceros y contratistas, se actualizaron en el manual de seguridad digital los *requisitos de seguridad en la relación con terceros*, en donde se define el cumplimento de las políticas de seguridad de la entidad, la firma de los formatos de Acuerdo de Confidencialidad y No Divulgación de Información para Contratista Persona natural o Jurídica - SIDEAP, además de la obligación de firmar acuerdos de niveles de servicio que permitan cumplir con las políticas de seguridad de la información. Sin embargo aún no han sido formalizadas totalmente en todos los contratos. Si bien en los acuerdos de confidencialidad se hace referencia al cumplimiento de las políticas de seguridad y privacidad de la información, y de tratamiento de datos personales, aun no se incluyen en las obligaciones específicas de los contratos, ni los acuerdos de niveles de servicio relacionados con la seguridad de la información:

ALCALDÍA MAYOR DE BOGOTÁ D.C. GESTIÓN PÚBLICA	MACROPROCESO DE DIRECCIONAMIENTO INSTITUCIONAL	Código: E-SIN-FM-005
	PROCESO DE SEGURIDAD DE LA INFORMACIÓN	Versión: 3.0
	Formato Acuerdo de Confidencialidad y No Divulgación de Información – Contratista Persona natural o Jurídica - DASCD	Vigencia desde: Febrero de 2019

1.5 Conocer, adoptar y aplicar el Documento de Política General de Seguridad y Privacidad de la Información y las políticas de tratamiento de datos personales del DEPARTAMENTO ADMINISTRATIVO DEL SERVICIO CIVIL DISTRITAL, que está publicado en la página WEB de la entidad: https://www.serviciocivil.gov.co/portal/transparencia

7.2.1.2.2 Seguimiento a las recomendaciones 2020

A continuación se relacionan las emitidas en el informe de la vigencia 2020 y su respectivo seguimiento, se incluyen únicamente aquellas que no fueron atendidas.

N°	OBSERVACIÓN DE MEJORA – RECOMENDACIÓN 2020	ESTADO	SEGUIMIENTO 2021
1.	Adelantar la descripción de las responsabilidades con respecto a la implementación y mantenimiento de los controles de seguridad de los recursos de	➡	Se avanzó en la descripción de responsabilidades con respecto a la implementación y mantenimiento de los controles de seguridad de los recursos de

<table>
<tr><th>N°</th><th>OBSERVACIÓN DE MEJORA – RECOMENDACIÓN 2020</th><th>ESTADO</th><th>SEGUIMIENTO 2021</th></tr>
<tr><td></td><td>la OTIC. En el caso de los contratistas, incluir estas condiciones en las obligaciones específicas.</td><td></td><td>la OTIC en el manual de seguridad digital y en la declaración de aplicabilidad, pero aún no se ha incluido en las obligaciones específicas de los contratistas</td></tr>
<tr><td>2.</td><td>En el marco de desarrollo del dominio de Gobierno de TI de la Política de Gobierno Digital, construir e implementar una metodología de Gestión de proyectos, que incluya las siguientes condiciones de seguridad:
Si hay activos críticos involucrados en el proyecto
Si hay información o datos confidencias al que puedan acceder terceros
Riesgos de seguridad asociados al proyecto
Condiciones de propiedad intelectual
Responsabilidad por incidentes de seguridad de terceros.
En caso de proyectos de adquisición o desarrollo de sistemas de información establecer formalmente los criterios de aceptación en materia de seguridad.</td><td></td><td>Si bien, se evidencian avances en la metodología de gestión de proyectos, en la metodología de desarrollo seguro en la Entidad y en las condiciones de propiedad intelectual, además se incluyeron correctamente los criterios y condiciones de seguridad en el manual de seguridad digital en el numeral : SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS, aún no se evidencia la implementación de estos criterios en los modelos de contrato y gestión de proyectos ejecutado, debido también a que aun no se ha formalizado completamente el Manual de seguridad digital.</td></tr>
<tr><td>3.</td><td>Complementar el Manual con los directorios de contactos y grupos de interés. El siguiente es un ejemplo:
<table>
<tr><th>Descripción</th><th>Organización</th><th>Contacto</th></tr>
<tr><td>Acceso abusivo a sistemas informáticos
Violación de Datos personales
Uso de Software malicioso
Suplantación de Sitios Web
Transferencia no consentida de activos
Hurto por medios informáticos
Phishing
Ingeniería Social</td><td>Centro Cibernético Policial (CCP)</td><td>http://www.ccp.gov.co/</td></tr>
<tr><td>Respuesta a Emergencias Cibernéticas de Colombia</td><td>COLSERT – Grupo de Respuesta a Emergencias Cibernéticas en Colombia</td><td>www.colcert.gov.co/</td></tr>
</table></td><td></td><td>Se actualizaron en el manual de seguridad digital en el numeral 16 Gestión de incidentes de la seguridad de la información, los contactos con el CSIRT del gobierno y policía nacional se deben adicionar otros grupos y contactos que permitan tener mayor conocimiento del tratamiento de riesgos e incidentes de la seguridad.</td></tr>
</table>

N°	OBSERVACIÓN DE MEJORA – RECOMENDACIÓN 2020	ESTADO	SEGUIMIENTO 2021
	Atención a incidentes de seguridad informática colombiano: CSIRT-CCIT – Centro de Coordinación Seguridad Informática Colombia: https://cc-csirt.policia.gov.co Grupo de interés equipos de red: Cisco: https://community.cisco.com/t5/technology-and-support/ct-p/technology-support Grupo de interés asesoría: INCIBE: https://www.incibe.es/formulario-contacto-empresas		
4	Se recomienda limitar el uso de WhatsApp Web para dar cumplimiento a las restricciones de intercambio de información establecidas en el Manual de Seguridad Digital Incluir los Controles de red para uso de equipos móviles corporativos y/o bajo la modalidad BYOD y teletrabajo.		En el manual de seguridad digital se incluye en los numeral 9.4 la Política para uso de dispositivos móviles, y 9.1.1 Política para uso de accesos remotos a la red (teletrabajo), en donde se establecen correctamente los controles y medidas de seguridad para el uso de dispositivos móviles personales, y móviles corporativos y/o bajo la modalidad BYOD y teletrabajo. También se defines las políticas y condiciones aplicables para el intercambio de información, sin embargo falta complementar las restricciones en cuanto al uso de herramientas no aprobadas para ese intercambio, ni se referencian los controles implementados en la red para su uso.
5	Configurar en el cliente VPN y en la configuración del firewall, el bloqueo de conexiones de equipos que no cumplan con el análisis de vulnerabilidades o tengan algún problema de seguridad. En el panel de control de *Security Fabric* del firewall, se encuentra el detalle estas recomendaciones y los pasos que se deben realizar para implementarla.		Debido a la contingencia por COVID 19, aplicar el bloqueo de conexiones de equipos que no cumplan con el análisis de vulnerabilidades o tengan algún problema de seguridad, no se aplica ya que interfiere con la correcta ejecución las labores de los usuarios de la Entidad. Sin embargo la OTIC adelantó de forma adecuada un plan de acción en el cual se programan visitas a los usuarios remotos, para corregir las vulnerabilidades encontradas y así garantizar la seguridad en los accesos remotos.
6	Diseñar, documentar e implementar una política de seguridad en el dominio para las conexiones de escritorio remoto y aplicarla a los grupos de seguridad de los usuarios de las VPN.		En el Manual de seguridad digital se incluye la Política para uso de accesos remotos a la red (teletrabajo), además se implementó la política en el dominio para el control de los accesos remotos.

7.2.1.2.3 Nuevas Recomendaciones

N°.	RECOMENDACION
1.	Incluir en las obligaciones específicas de los contratos las condiciones de seguridad y la obligación de firmar acuerdos de niveles de servicio que permitan cumplir con las políticas de seguridad de la información.
2.	Atender las recomendaciones de la vigencia anterior que se presentan con la valoración

7.2.1.3 Clausula 7 Soporte. - A.7. Seguridad de los recursos humanos.

7.2.1.3.1 Observaciones 2021

- En el Manual de seguridad digital y la Política General de la Seguridad y Privacidad de la información se tienen correctamente definidas las Política de seguridad de la información orientadas al talento humano, en donde se establece que los Servidores Públicos, Contratistas, Proveedores y Partes Interesadas, deben dan cumplimiento a las políticas, normas y procedimientos de seguridad de la información y sus respectivas responsabilidades, así como su asistencia y participación de las actividades de capacitación y sensibilización programadas en temas de seguridad digital. También se tiene correctamente definidas las políticas en el proceso de vinculación, de ejercicio del empleo o ejecución del contrato, de terminación o cambio del empleo, terminación del contrato y de licencias o vacaciones.
- Se crearon y actualizaron los acuerdos de confidencialidad que deben diligenciar y firmar todos los servidores públicos y contratistas que ingresen al DASCD, en donde se incluye el cumplimiento y conocimiento de las políticas de seguridad

7.2.1.3.2 Seguimiento a las recomendaciones 2018, 2019

A continuación se relacionan las observaciones emitidas en el informe de la vigencia 2020 y su respectivo seguimiento, se incluyen únicamente aquellas fueron identificadas como no atendidas.

N°	OBSERVACIÓN DE MEJORA – RECOMENDACIÓN 2020	ESTADO	SEGUIMIENTO 2021
1.	Se recomienda incluir la entrega del manual y su aceptación formal en los procesos de inducción y reinducción del 5. Plan Estratégico de Talento Humano 2020.		Si bien se avanzó en la correcta definición y especificación de las políticas, y se han socializado con el área de talento humano, aún no se evidencia la inclusión de aceptación formal del manual de seguridad digital.

N°	OBSERVACIÓN DE MEJORA – RECOMENDACIÓN 2020	ESTADO	SEGUIMIENTO 2021
2.	Incluir el cumplimiento del Manual de manera complementaria a la Política de seguridad, en la obligación de los contratistas		Se crearon y actualizaron los acuerdos de confidencialidad que deben diligenciar y firmar todos los servidores públicos y contratistas que ingresen al DASCD. Las obligaciones generales de los contratistas incluyen el cumplimiento de las Políticas de Seguridad
3.	Incluir las temáticas de seguridad de la información en el Plan Estratégico de Talento Humano.		Se ha avanzado en la socialización con el área del Talento Humano las temáticas de seguridad relacionadas en el manual y política general de seguridad y privacidad de la información, sin embargo aun no se han formalizado en el plan estratégico, debido a que el manual de seguridad digital tampoco se ha formalizado.
4.	Incluir en el Manual las referencias a la cesión de derechos para desarrolladores de software.		En el numeral 8 Políticas de Gestión de Activos de Información del manual de seguridad digital, se incluyó el texto: *"El DASCD es el dueño de la propiedad intelectual, los avances tecnológicos e intelectuales desarrollados por los funcionarios y los contratistas, derivados del cumplimiento de sus funciones, de las obligaciones y/o tareas asignadas."*, dando cumplimento a esta recomendación

7.2.1.3.3 Nuevas Recomendaciones

N°.	RECOMENDACION
1.	Formalizar el manual de Seguridad digital para que se adopten todas las políticas definidas para la seguridad de los recursos humanos y se incluyan formalmente en el Plan Estratégico de Talento Humano.
2.	Atender las recomendaciones de la vigencia anterior que se presentan con la valoración

7.2.1.4 Clausula 6. Planificación y 8. Operación

7.2.1.4.1 Observaciones 2021

Se actualizó la caracterización de activos y su respectiva tipificación para relacionar los tipos de activos en la Matriz de Riesgos de Seguridad Digital (borrador-2021), en el inventario de activos de información se agregó la columna *Riesgos Asociados al tipo de activo,* en la cual se relaciona el activo con sus posibles riesgos, además de incluir de forma adecuada, un hipervínculo al tipo de activo en la matriz de riesgos y uno en el tipo de riesgo para el inventario de activos.

👉 En cuanto a la tipificación de activos en la matriz de riesgos y a la caracterización de los mismos se evidencia que se encuentran tipificados de forma muy general, y por ende los riesgos y controles relacionados con el tipo de activo no se aplican correctamente, como el caso de los sistemas de información propios de la Entidad que se tipifican como: "Software", si bien los riesgos asociados a los sistemas de información coinciden en algunos casos con el software base (Sistemas operativos, Office, etc.), existen otros riesgos inherentes a los sistemas de información que no se están abordando en la matriz actual. Otro caso es la tipificación: *hardware* en la cual se incluyen equipos de usuarios, servidores, impresoras, escáneres, dispositivos biométricos y memorias, en la cual se evidencia que los riesgos inherentes a los servidores, que son diferentes a los de equipos de usuarios y/o periféricos no tengan el tratamiento y control adecuado.

👎 En la columna *Descripción del control existente* de la matriz de riesgos se esta registrando la justificación de la declaración de aplicabilidad para el control, mas no el control que se tiene implementado para tratar el riesgo, lo cual impide determinar cuál es el control implementado.

👍 Se está realizando de forma adecuada el seguimiento a la matriz de riesgos, de acuerdo con lo establecido en el Procedimiento Gestión de Riesgos de Seguridad Digital V1 y registrando correctamente los avances en la implementación de los controles en las columnas*: acciones realizadas, primera , segunda y tercera línea de defensa*, en donde se describe correctamente cada acción implementada y los pendientes para cada riesgo.

👍 El avance a las observaciones de mejora emitidas por la auditoría en el informe de la vigencia 2020 para los 25 riesgos a los cuales se ha diligenciado el *autocontrol del proceso - la primera línea de defensa* se encuentran registradas en el archivo: Primer_Seguimiento_Riesgos_de_ Seguridad_Digital_V2.xls con su respectivo seguimiento para el periodo 1 en las columnas "*Seguimiento OAP - segunda línea de defensa"* y *"Seguimiento control interno - tercera línea de defensa"*

7.2.1.4.2 Seguimiento a las recomendaciones 2020

A continuación se relacionan las recomendaciones emitidas en el informe de la vigencia anterior. Se incluyen aquellas que no fueron subsanadas en el avance de la implementación del MSPI del mismo, el seguimiento a las recomendaciones para el plan de continuidad y estrategias de copias de seguridad se emiten en el numeral 7.2.1.15 de este informe.

N°	OBSERVACIÓN DE MEJORA – RECOMENDACIÓN 2020	ESTADO	SEGUIMIENTO 2021
1.	Deben atenderse las mejoras al diseño de los controles, técnicas de		Se ha avanzado de forma adecuada en la ejecución de las acciones recomendadas para

N°	OBSERVACIÓN DE MEJORA – RECOMENDACIÓN 2020	ESTADO	SEGUIMIENTO 2021
	seguimiento y evidencias presentadas en cada caso, tomando como guía las observaciones del numeral 7.2.1.4.1 del informe para la vigencia 2020.		la implementación y verificación de los 25 controles en la matriz de Riesgos con autocontrol del proceso definido, registradas en el formato Primer_Seguimiento_Riesgos _de_Seguridad_Digital_V2. No se avanzado en la identificación detallada de los controles específicos que aplican para cada riesgo. No se modificó el procedimiento de gestión de riesgos para incluir las actualizaciones por demanda que se generen por cambios en la plataforma tecnológica y que impacten el inventario de activos de información, la matriz de riesgos y/o los controles definidos para cada riesgo.
2.	Contemplar análisis de causas y acciones a tomar frente a la “Verificación de la implementación y funcionamiento de los controles de seguridad de la información” en el procedimiento de gestión de riesgos.		Aun no se ha modificado el procedimiento para incluir esta recomendación en el flujo de este.
3.	En la matriz de riesgos, ajustar el planteamiento de los riesgos para identificar su relación con los activos de información		Ya se actualizó la matriz de riesgos con la relación de tipos de activos de información.
4.	Al momento de establecer los controles, identificar aquellos que para su verificación requieren inspección de configuración en las herramientas de administración y gestión de la plataforma tecnológica y/o pruebas de efectividad.		Se adicionaron las columnas necesarias para la valoración del control (Diseño), Valoración del control (ejecución), Análisis y evaluación de los controles, de análisis y evaluación de los controles y solidez del control, en donde se puede complementar de forma adecuada la recomendación dada
5.	Continuar la identificación de riesgos y asociación con los controles de MSPI dando cobertura a los demás objetivos de control de la norma.		En la Matriz de Riesgos de Seguridad Digital (borrador-2021) se evidencia el avance en la identificación de riesgos en donde están incluidos todos los objetivos de control de la norma, si bien aún no están diligenciados completamente, esta recomendación implica un proceso continuo que es parte del avance en el nivel de madurez del modelo del MSPI.

7.2.1.4.3 Nuevas Recomendaciones

N°.	RECOMENDACIÓN
1.	En la matriz de riesgos, ajustar la descripción del control existente, identificando de forma detallada el control, no la justificación de su implementación para poder verificar de forma adecuada su efectividad y cumplimiento.
2.	Atender las recomendaciones de la vigencia anterior que se presentan con la valoración

7.2.1.5 Clausula 9. Evaluación y desempeño – Clausula 10 Mejora.

7.2.1.5.1 Observaciones 2021

- La Oficina de Control interno ha cumplido con su rol de verificación establecido en el Manual de Seguridad Digital, con la ejecución anual de la auditoría que incluye el seguimiento al MSPI. Los resultados son socializados debidamente con la Dirección.
- Se cuenta con 5 indicadores relacionados con la seguridad de la información: Implementación de controles de seguridad de la información, Implementación de controles de acceso físico y lógico, Incidentes de seguridad de la información gestionados, Indicador de seguimiento a riesgos de TI y Cobertura de las actividades de sensibilización y/o concientización en Seguridad de la Información. En la hoja de vida de cada indicador se registra correctamente su respectivo análisis y conclusiones de los resultados, por parte de la oficina de planeación.

7.2.1.5.2 Seguimiento a las recomendaciones 2020

A continuación se relacionan las observaciones emitidas en el informe de la vigencia 2020 y su respectivo seguimiento, se incluyen únicamente aquellas fueron identificadas como no atendidas.

N°	OBSERVACIÓN DE MEJORA – RECOMENDACIÓN 2020	ESTADO	SEGUIMIENTO 2021
1.	Continuar la construcción de los indicadores del MSPI de manera alineada con los objetivos de control, algunos ejemplos son: ✓ Hacer escaneo de red y determinar el número de equipos con software no autorizado sobre el total de equipos en dominio.		Se cuenta con 5 indicadores relacionados con la seguridad de la información, sin embargo se reitera la recomendación de construcción y diseño de indicadores alineados a los objetivos de control del MSPI que aún no se han contemplado.

N°	OBSERVACIÓN DE MEJORA – RECOMENDACIÓN 2020	ESTADO	SEGUIMIENTO 2021
	✓ Indicador de cumplimiento en derechos de autor. ✓ Indicador de número de copias restauradas exitosas sobre el total de la muestra.		
2.	Diseñar los indicadores para contar con herramientas para el tratamiento de riesgos y facilitar la toma de acciones correctivas, usando en lo posible fuentes automáticas, para generar carga operativa adicional. (Mejoras al indicador de seguimiento a riesgos de TI).		Se presenta avance en cuanto a la mejora y diseño del indicador de tratamiento de riesgos, en cuanto al desarrollarlo de los indicadores basados en la clasificación del riesgo desde la consola del antivirus y de controles en la declaración de aplicabilidad. Se recomienda complementarlos con la clasificación de cumplimiento desde la consola del nuevo Firewall que esta en proceso de adquisición.
3.	**Recomendaciones de mejora al indicador Cobertura de las actividades de sensibilización y/o capacitación en Seguridad de la Información**: el indicador puede ser mejorado con respecto a: De acuerdo con el documento "*HV INDICADORES SEG-INF abr_2020.xlsx*", el indicador se calcula como la (*Sumatoria de Funcionarios y Contratistas cubiertos por las actividades de sensibilización en seguridad de la información en el trimestre) / (total de funcionarios y Contratistas durante el trimestre * Número de actividades realizadas en el trimestre),* lo cual resulta confuso, ya que el denominador se refiere al número de asistencias esperadas, y el denominador a número de personas El indicador mide asistencia mas no apropiación del conocimiento, lo cual es relevante para que las políticas de seguridad sean entendidas y		De acuerdo a lo registrado en la hoja de vida del indicador, la formulación continua igual y por tanto aún no se cuenta con un indicador que mida la apropiación de conocimiento de las políticas de seguridad.

N°	OBSERVACIÓN DE MEJORA – RECOMENDACIÓN 2020	ESTADO	SEGUIMIENTO 2021
	aplicadas por todos los usuarios de servicios tecnológicos		

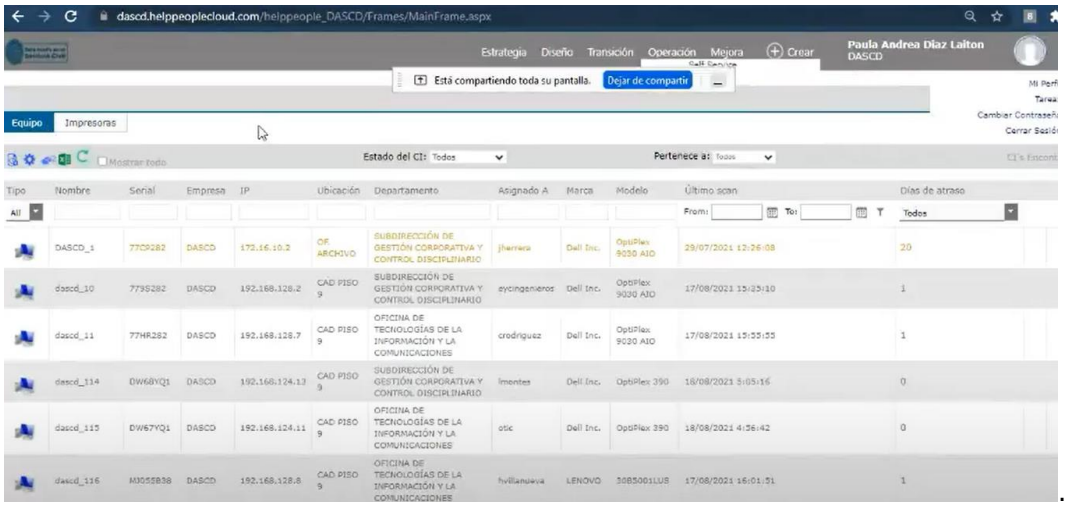
7.2.1.5.3 Nuevas Recomendaciones

N°.	RECOMENDACION
1.	Atender las recomendaciones de la vigencia anterior que se presentan con la valoración

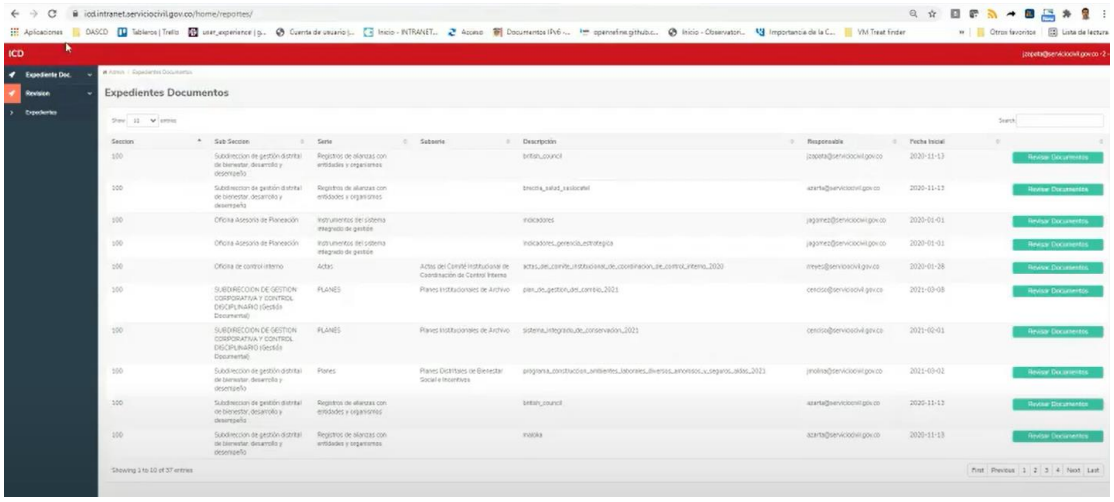
7.2.1.6 A.8. Gestión de activos.

7.2.1.6.1 Observaciones 2021

- Se aprobó mediante acta la Matriz de Caracterización de Activos de Información – 2020 – MCAI, en donde se incluyen todas las consideraciones necesarias para la identificación del activo, sus responsables, esquema de publicación, índice de información clasificada y reservada, aspectos de seguridad de la información, backups, migración IPv6, criticidad en la operación y servicios, clasificación documental, y además consolida con todos los elementos de ley necesarios. También se encuentra correctamente publicada en la pagina web de la Entidad.
- Se actualizó y complementó el Manual de seguridad digital con las Políticas de Gestión de Activos de Información con las observaciones realizadas por la auditoria en los informes de vigencias anteriores, definiendo de forma adecuada las políticas de responsabilidad por los activos de información, de clasificación y manejo de la información, de uso de equipos, periféricos, medios de almacenamiento, y de formatos de almacenamiento.
- Se están realizando de forma adecuada, jornadas para la actualización y mantenimiento de la matriz de caracterización con las dependencias de la Entidad para garantizar el control, validación y mejoras sobre la misma.
- En la matriz de caracterización se incluye un diccionario. en el cual se especifica y define el manejo cada uno de los datos que conforman la matriz, lo que asegura que cualquier actualización o cambio sea controlado y validado por medio de listas de valores y de acuerdo con las normas.
- En cuanto a la articulación del inventario de activos con el inventario de hardware y software , ya se implementó en la herramienta de HelpPeople , el escaneo automático sobre la plataforma tecnológica de la entidad y se le hace el respectivo seguimiento para correcto funcionamiento, sin embargo no se ha definido un procedimiento o herramienta para el cruce de los resultados del escaneo con la Matriz de Caracterización de Activos de Información. Se está evaluando la adquisición o desarrollo de una herramienta que permita automatizar la gestión de la matriz y sus respectivas actualizaciones para evitar los trabajos manuales:



- Con la implementación total del escaneo de hardware y software desde la herramienta de HelpPeople se está controlando de forma adecuada el licenciamiento y uso de software en los equipos de la Entidad
- Se creó el *Instructivo para la gestión de los repositorios oficiales de información y la denominación de los documentos electrónicos* cuyo objetivo es: "Definir los mecanismos que permitan almacenar adecuadamente la producción documental electrónica con fines archivísticos de manera separada del resto de la producción documental electrónica, y así de esta manera, poder controlar procesos de clasificación, valoración y disposición final de manera técnica, aportando a la preservación digital a largo plazo, de la documentación con cualidades patrimoniales, históricas y técnicas producida en la entidad", asegurando que se almacene y clasifique de forma adecuada todos los documentos que producen los usuarios, de esta forma se evitan problemas en las copias de seguridad, y en la organización y búsqueda de la misma.
- Se desarrolló e implementó una herramienta para la organización de los expedientes electrónicos y del inventario de control documental, en la cual permite crear los expedientes, su clasificación, codificación, prefijos de tabla de retención y mantener la traza de los documentos cumpliendo así con todas las recomendaciones emitidas en cuanto clasificación, etiquetado y alojamiento de la información:



Se creó una nueva unidad de almacenamiento compartido organizada por áreas, con los permisos de usuario por grupos en el directorio activo correctamente configurados y articulada con los etiquetados de información de la herramienta de inventario de control documental garantizando el correcto almacenamiento y control de acceso a la información.

7.2.1.6.2 Seguimiento a las recomendaciones 2020

A continuación se relacionan las observaciones emitidas en el informe de la vigencia 2020 y su respectivo seguimiento, se incluyen únicamente aquellas fueron identificadas como no atendidas.

N°	OBSERVACIÓN DE MEJORA – RECOMENDACIÓN 2020	ESTADO	SEGUIMIENTO 2021
1.	Continuar con la ejecución de las acciones de los planes establecidos. En las políticas de etiquetado, contemplar que las longitudes de nombres de archivo no afecten los medios de alojamiento o procesos de backup. En el caso de activos TIC incluir las siguientes definiciones de etiquetado: • Trazabilidad, etiquetado y alojamiento de los requerimientos y documentos asociados al ciclo de fábrica		Se ha dado cumplimiento a estas recomendaciones con la actualización en el Manual de la Seguridad digital para incluir las políticas adecuadas. Con la implementación y puesta en marcha de la herramienta de inventario de control documental y expediente electrónico, se obliga de forma adecuada el cumplimento del etiquetado, adicionalmente del control de longitudes de nombre de archivos para evitar fallos en las copias de seguridad.

N°	OBSERVACIÓN DE MEJORA – RECOMENDACIÓN 2020	ESTADO	SEGUIMIENTO 2021
	• Etiquetado de versiones de fuentes en desarrollo • Etiquetado de sintaxis en la creación de cuentas de usuario en servicios tecnológicos • Trazabilidad, etiquetado y alojamiento de los registros de los formatos del MSPI. • Etiquetado de medios de almacenamiento (si aplica)		
2.	Involucrar las políticas de backup de archivos, correo electrónico, limpieza de accesos directos y entrega a paz y salvo de activos de información frente a retiros.		Se definieron las políticas en el manual de Seguridad digital, además de incluir en la Matriz de Caracterización de Activos de Información – 2020 lo recomendado para los backups de los activos de información.
3.	Está pendiente finalizar la depuración de los activos de hardware y software a partir de los registros en HelpPeople		Ya se tiene configurada y funcionando correctamente la herramienta de inventarios de hardware y software automatizados por escaneos, si bien se realiza el seguimiento de forma adecuada, aún falta articularla con la Matriz de Caracterización de Activos de Información, ya se está en proceso la evaluación de requerimientos para adquirir una herramienta que permita automatizar la depuración y articulación de los dos inventarios.
4.	En el marco del dominio A10 establecer mecanismos de encriptación sobre medios removibles autorizados. Desarrollar los procedimientos faltantes.		En cuanto a los mecanismos de encriptación de medios removibles autorizados, si bien se incluye la política en el Manual de Seguridad digital aun no se ha establecido el mecanismo o herramienta a utilizar. En cuanto a los procedimientos e instructivos pendientes ya se tiene identificados en el listado de instrumentos pendientes incluido en la Matriz de Riesgos de Seguridad.

7.2.1.6.3 Nuevas Recomendaciones

N°.	RECOMENDACION
1.	Atender las recomendaciones de la vigencia anterior que se presentan con la valoración

7.2.1.7 A.9. Control de acceso.

7.2.1.7.1 Observaciones 2021

👍 Las políticas de control de acceso se encuentran correctamente definidas en el manual de Seguridad de la Información, el control de acceso se continúa gestionado de forma adecuada de acuerdo con lo establecido en el E-SIN-PR-002 Procedimiento de control de acceso V1, la matriz de gestión de accesos "E-SIN-FM-03 tabla de control de acceso a los servicios tecnológicos - 2020.xlsx" y el instrumento "E-SIN-FM-02 solicitud y respuesta de acceso a usuarios - 2020.xlsx".

👍 Se creó el formato A-TIC-FM-007 MONITOREO_PLATAFORMA_TI_V4 en donde se registra correctamente todo el seguimiento a las alertas de los tableros de control, la gestión de accesos a elementos de la infraestructura y a las acciones realizadas para el mejoramiento de la plataforma.

👉 Si bien se lleva de forma adecuada la asignación y traza de permisos y roles de usuario para los accesos a los servicios tecnológicos de la entidad por medio de la tabla de control de acceso a los servicios tecnológicos – 2020, aun no se tiene definido un procedimiento de verificación de la configuración de estos permisos en los diferentes sistemas de información, para validar lo definido en la tabla con lo implementado en cada servicio tecnológico.

7.2.1.7.2 Seguimiento a las recomendaciones 2020

N°	OBSERVACIÓN DE MEJORA – RECOMENDACIÓN 2020	ESTADO	SEGUIMIENTO 2021
1.	Se configuraron correctamente las VLAN´s de las áreas funcionales y no permite realizar escaneos a los segmentos diferentes al asignado, con excepción del segmento de servidores que aún continúa expuesto.	⬆	Se ha dado cumplimiento a estas recomendaciones con la actualización de la configuración en el firewall del segmento de servidores, dejando únicamente el servicio de carpetas compartidas que debe ser visible desde todos los segmentos.
2.	Si bien se han restringido la ejecución de algunos archivos ejecutables con algunas listas negras y tanto el firewall como el antivirus tiene controles sobre tipos de descargas consideradas como peligrosas, el auditor aun pudo realizar algunas descargas y ejecutar aplicaciones portables.	⬆	Se está realizando de forma adecuada el seguimiento y control de presencia de software considerado peligros desde las consolas del antivirus, firewall y desde la herramienta del HelpPeople, para eliminar cualquier software no permitido. Se continúa actualizando las listas negras el Firewall y el antivirus para impedir la ejecución de software peligroso
3.	En los tableros de control e informes del firewall se evidencias alertas y recomendaciones que no se han		Se evidencia el seguimiento a las alertas que se presentan tanto en la consola del Firewall como la del antivirus. En cuanto a las alertas del

N°	OBSERVACIÓN DE MEJORA – RECOMENDACIÓN 2020	ESTADO	SEGUIMIENTO 2021
	ejecutado, no existe un registro formal de las acciones correctivas realizadas basadas en las alertas del Firewall.	↑	antivirus se realizan correctamente las acciones para mantener el nivel de seguridad de la plataforma.
4.	Aun no se ha implementado la solución para el control de usuarios administradores locales, el auditor encontró expuesta la contraseña de este usuario en la red, y logro tener acceso a varios equipos con ella, además de evadir los controles de seguridad implementados en la plataforma.	↑	Ya se implementaron las recomendaciones dadas en cuanto a las contraseñas de administrador local y se realiza seguimiento y control de su respectivo cambio en todos los equipos.
5.	Restringir por medio de directivas del dominio que, en las estaciones de trabajo, los usuarios pueden ingresar al editor de registro de Windows, a la ejecución de comandos (CMD) y al PowerShell. Estas ejecuciones pueden ser aprovechadas por atacantes para cambiar configuraciones y desactivar protecciones	↑	Se crearon y actualizaron las políticas en el dominio para acatar con esta recomendación
6.	El administrador de la base de datos informó que se está realizando el cambio de contraseña cada 3 meses, sin embargo, no se ha implementado un formato para evidenciarlo, ni existe un procedimiento documentado del mismo.	→	Si bien se está cumpliendo el cambio, aún no se ha implementado el formato que lo evidencie.
7.	Se recomienda dejar un único usuario administrador que debería ser el DBA en la instancia de producción de SQL de la base de datos SIDEAP. Adicionalmente realizar una revisión de los usuarios con rol de SUPER USUARIO en el aplicativo de SIDEAP, y eliminar los que no son necesarios.	↑	Ya se realizó una depuración de usuarios administradores en la base de datos y en los roles de Sideap, la contraseña de administrador de las bases de datos se comparte con el DBA y administrador de la infraestructura.
8.	En los hallazgos del informe anterior se muestra la evidencia de archivos con clave de administrador local, y de los usuarios *ext_gopher y antivirus_interlan* expuestas y sin protección adecuada.	↑	Se ha dado cumplimiento a esta recomendación en la depuración y nuevo esquema de las carpetas compartidas.
9.	Crear un procedimiento en el cual se garantice la atención y remediación de las alertas emitidas por las	↑	Esta recomendación se encuentra atendida y se está realizando correctamente el registro de acciones de remediación y tratamiento de

N°	OBSERVACIÓN DE MEJORA – RECOMENDACIÓN 2020	ESTADO	SEGUIMIENTO 2021
	herramientas de monitoreo existentes en la entidad (Firewall, Antivirus, Hosting, ETB.), se debe implementar un formato de registro de estas evidencias y de las acciones, que permita realizar un análisis cuantitativo de ocurrencia y orígenes de esta.		alertas en el formato A-TIC-FM-007 MONITOREO_PLATAFORMA_TI_V4.
10.	Activar y configurar los filtros para la prevención de perdida de datos (DLP) en el firewall de acuerdo con lo especificado en el marco del proyecto SIC - Sistema Integrado de Conservación del Plan de Acción de Trasformación Digital. También se deben configurar filtros adicionales para afinar la prevención de intrusos en el firewall, ya que solo tiene la protección por defecto.		Esta recomendación no se ha implementado aun, debido a que se va a realizar un cambio del Firewall y se espera configurar en el firewall adquirido con las características nuevas que ofrezca el dispositivo.

7.2.1.7.3 Nuevas Recomendaciones

N°.	RECOMENDACION
1.	Atender las recomendaciones de la vigencia anterior que se presentan con la valoración

7.2.1.8 A.10. Criptografía.

7.2.1.8.1 Observaciones 2021

En el manual de Seguridad Digital de la Entidad se agregó en el numeral 10, la Política de Controles Criptográficos en donde se establece la protección de activos de información clasificada mediante el uso de herramientas criptográficas. También se define de forma adecuada el uso de conexiones cifradas en cuanto a las claves de acceso, correos electrónicos, mensajería, intercambio de información y el uso de herramienta de cifrado en dispositivos móviles y medios de almacenamiento extraíbles.

Se clasificó correctamente la confidencialidad de los documentos en la Matriz de Caracterización de Activos de Información, sin embargo aun no se ha definido la herramienta que se usara como control criptográfico para estos.

7.2.1.8.2 Seguimiento a las recomendaciones 2020

N°	OBSERVACIÓN DE MEJORA – RECOMENDACIÓN 2020	ESTADO	SEGUIMIENTO 2021
1.	Se deben identificar los requisitos e implementar controles criptográficos en los siguientes casos: ✓ Protección de contraseñas de acceso a sistemas y demás servicios que requieran autenticación. ✓ Transmisión de información confidencial al interior de la empresa y fuera de ella. ✓ Transmisión de información de voz a través de los medios de comunicación. ✓ Servicios institucionales que recopilen información de terceros. ✓ Uso de correo electrónico institucional, vía web. ✓ Mensajería instantánea institucional. ✓ Firma digital de documentos y correos electrónicos (cuando aplique). ✓ Para el resguardo de información, cuando esta información sea clasificada como confidencial o reservada. ✓ Portátiles, celulares y medios extraíbles		Si bien se definió la política de controles criptográficos en el Manual de Seguridad de la Información, aún no se han implementado.

7.2.1.8.3 Nuevas Recomendaciones

N°.	RECOMENDACION
1.	Seleccionar o adquirir una herramienta criptográfica para implementarla en los activos de información clasificados como confidenciales
2.	Atender la recomendación de la vigencia anterior que se presenta con la valoración

7.2.1.9 A.11. Seguridad física y del entorno.

7.2.1.9.1 Observaciones 2021

Se continúa aplicando adecuadamente los controles de seguridad definidos para este dominio, se adicionaron adecuadamente las correcciones al contrato se de mantenimiento.

7.2.1.9.2 Seguimiento a las recomendaciones 2020

N°	OBSERVACIÓN DE MEJORA – RECOMENDACIÓN 2020	ESTADO	SEGUIMIENTO 2021
1.	Incluir en las Especificaciones Técnicas del contrato de mantenimiento: • Proteger la información confidencial que se utilice para el ejercicio de sus labores. El auditor encontró en un archivo desprotegido en carpetas compartidas la clave de administrador local de los PC´s. • Certificar que todo el software para la ejecución del objeto contratado está debidamente licenciado. El auditor encontró evidencia de uso de software en versiones de evaluación (Hard Disk Sentinel). • Hacer uso o almacenar en los activos de la entidad programas potencialmente peligrosos. El auditor encontró programas para violar el licenciamiento de productos Microsoft. • Pese a que la OTIC elaboró un instructivo de mantenimiento preventivo acatando las recomendaciones de la auditoría en materia de seguridad de la información, se observa que el Anexo técnico en D. Especificaciones Técnicas Mínimas - 1. Mantenimiento Preventivo Bienes Informáticos 1.2. Equipos de Cómputo, no hace referencia a dicho instructivo, ni incluye el mantenimiento preventivo de seguridad.		Se ha dado cumplimiento con esta recomendación con la modificación y seguimiento al contrato de mantenimiento.

7.2.1.9.3 Nuevas Recomendaciones

N°.	RECOMENDACION
1.	Los controles implementados en este dominio son los adecuados, debe mantenerse el seguimiento y revisión al funcionamiento de estos

7.2.1.10 A.12. Seguridad de las operaciones.

7.2.1.10.1 Observaciones 2021

- Los controles implementados para este dominio se encuentran correctamente implementados de acuerdo con las evidencias presentadas y el cumplimiento de las recomendaciones emitidas en los informes de vigencias anteriores y, los pendientes en la implementación están concentrados en la falta de procedimientos documentados e instructivos de los mismos.

- Se actualizó el formato de monitoreo de la plataforma en donde se esta registrando de forma adecuada todas las acciones realizadas para garantizar la correcta operación de la misma, además se detalla el evento, la solución, categoría, incidencia y servicio como insumo para la toma de decisiones en el ciclo de mejoramiento continuo, sin embargo esta formato al no ser automatizado, implica una alta carga operativa en su registro y análisis de causa e incidencias, por lo cual se debería evaluar la adquisición o desarrollo de una herramienta que permita analizar las incidencias y soluciones de forma ágil y oportuna :

ALCALDÍA MAYOR DE BOGOTÁ D.C.	MACROPROCESO DE APOYO: APOYO A LA GESTIÓN	Código: A-TIC-FM-007
	PROCESO GESTIÓN DE LAS TIC	Versión: 4.0
	FORMATO: MONITOREO PLATAFORMA TI (ADMINISTRACIÓN PLATAFORMA TECNOLÓGICA)	Vigencia: Marzo de 2021

Funcionario:	[redacted]	CC - 7965589 Profesional Especializado 222-21	Vigencia: 2021

DETALLE DEL MONITOREO DE LOS COMPONENTES PLATAFORMA TI

día	mes	año						
09	03	2021	Fecha	09/03/2021	Consecutivo	1	Incidencia	Seguimiento - control
			Categoría	Dispositivos_físicos			Servicio	Servidores
			Detalle Evento			Detalle Solución		
			Ingresar servidores fisicos y realizar exportación de máquinas virtuales			Se ingresa a cada uno de los servidores fisicos se crea la carpeta BK-HYPER-V, se programa inciio de exportación de máquinas virtuales.		
10	03	2021	Fecha	10/03/2021	Consecutivo	1	Incidencia	Actualización - Ajustes
			Categoría	Hosting			Servicio	Servidor Aplicaciones
			Detalle Evento			Detalle Solución		
			SOL13903 - permisos de acceso servidores Buenos días, brindar permisos de acceso a los servidores del SIDEAP, para l[redacted]res de Hosting, para efectuar los ajustes solicitados de acuerdo a las contratista JENNY GALINDO. APLICACIONES (lectura / escritura) acceso para despliegues BASE DATOS (lectura / escritura) respuesta a solicitudes			ACCIONES REALIZADAS instrucciones recibidas. GERARDO GUTIERREZ -Servidor de aplicaciones se adiciona el usuario -Servidor de base de datos se adiciona el usuario [redacted] dascd_jgalindo JEISSON PINEDA -Favor crear permisos en la Base de datos usuario VPN dascd_jgalindo / usuario BD jgalindo		
10	03	2021	Fecha	10/03/2021	Consecutivo	2	Incidencia	Seguimiento - control
			Categoría	Dispositivos_físicos			Servicio	Servidores
			Detalle Evento			Detalle Solución		
			El día 9-03-2021, se frealizo backup de las máquinas virtules que actualmnete estan en funcionamianto. Se requiere verificación de la culminación del backup			Se ingreso a los diferentes servidores fisicos y se verifico en el panel de hyper-v, que terminara el proceso de exportación de las máquinas virtuales. Todos culminaros satisfactoriamnete		

7.2.1.10.2 Seguimiento a las recomendaciones 2020

N°	OBSERVACIÓN DE MEJORA – RECOMENDACIÓN 2020	ESTADO	SEGUIMIENTO 2021
1.	Analizar en detalle el alcance de este dominio en el MSPI, toda vez que corresponde a uno de los más grandes y con mayor relación con el Dominio de Servicios Tecnológicos. La siguiente es una lista de posibles instrumentos que deben ser articulados e implementados en la plataforma tecnológica, entendiendo que debe cumplirse en las operaciones con el ciclo PHVA • Procedimientos de seguridad en el uso de equipos personales (BYOD) • Procedimiento de registro y seguimiento de eventos de Sistemas de información y Comunicaciones • Procedimiento de gestión de cambios y adquisiciones • Procedimiento de gestión de ambientes • Plan de gestión de capacidad • Bitácoras de monitoreo de capacidad y desempeño • RFC de solicitud de cambios (base para HelpPeople) • Bitácora de Creación de ambiente_ • Políticas de_ respaldo de la información • Políticas de seguridad de operaciones • Modelo de Servicio • Procedimientos de registro, monitoreo y medición de capacidad y desempeño • Plan de copias de respaldo • Registro de restauración de copias de respaldo • Novedades restauración de backups • Matriz de Adquisiciones y terceros • Catalogo y Especificaciones técnicas de capacidad por servicio • Inventario de logs organizacionales		Se presenta avance en los siguientes instrumentos: • A-TIC-FM-007 MONITOREO_PLATAFORMA_TI_V4. • A-TIC-GI-001 Guía de implementación y despliegue de conexiones VPN V1. • A-TIC-GI-002 GUIA_DE_PLAN_DE_GENERACION_COPIAS_DE_SEGURIDAD_DASCD_V1 • A-TIC-GI-003 GUIA_APAGADO_SEGURO_SERVIDORES_V2. • A-TIC-IN-004 INSTRUCTIVO_CAMBIO_CONTRASEÑA_V1. • A-TIC-PR-005 CONSTRUCCION_Y_MANTENIMIENTO_DE_SOFTWARE_DYD_V6. • E-SIN-IN-001 INSTRUCTIVO_GESTIÓN_REPOSITORIOS_OFICIALES_INFORMACIÓN_DDELEC V2. • Ver2-A-TIC-PR-007 PROCEDIMIENTO DE GESTIÓN DE CAMBIOS. • E-SIN-PR-003 Procedimiento de Gestión de Incidentes V1. • E-SIN-FM-008 FORMATO DE REGISTRO Y CONTROL DE INCIDENTES V1 • ARQUITECTURA SIDEAP. • Formato casos de prueba. • Formato Checklist Pruebas funcionales • Formato de requerimientos. • Formato despliegue producción. • Formato viabilidad de requerimientos.docx • Protocolo de restauración de BD. • Protocolo de soporte a peticiones. • PLAN_RECUPERACION_DESATRES_TI_V6. Que evidencian un alto avance en esta recomendación y en su implementación ya que estos documentos han sido generados de acuerdo con lo ya implementado.

N°	OBSERVACIÓN DE MEJORA – RECOMENDACIÓN 2020	ESTADO	SEGUIMIENTO 2021
	Instructivos de: administración de directorio activo. configuración de dispositivos firewall. configuración de dispositivos switchs. configuración de dispositivos router. configuración de dispositivos Access point. configuración de dispositivos teléfonos IP. gestión de bases de datos. alistamiento de equipos PC. alistamiento de servidores físicos y virtualizados administración de carpetas compartidas. administración de servicio VOIP.		En el Listado de Instrumentos pendientes incluido en la Matriz de Riesgos de Seguridad se tiene correctamente identificados los procedimientos, formatos e instructivos que han falta por documentar.

7.2.1.10.3 Nuevas Recomendaciones

N°.	RECOMENDACION
1.	Adelantar la construcción de los instrumentos faltantes identificados en el Listado de Instrumentos pendientes incluido en la Matriz de Riesgos de Seguridad

7.2.1.11 A.13. Seguridad de las comunicaciones.

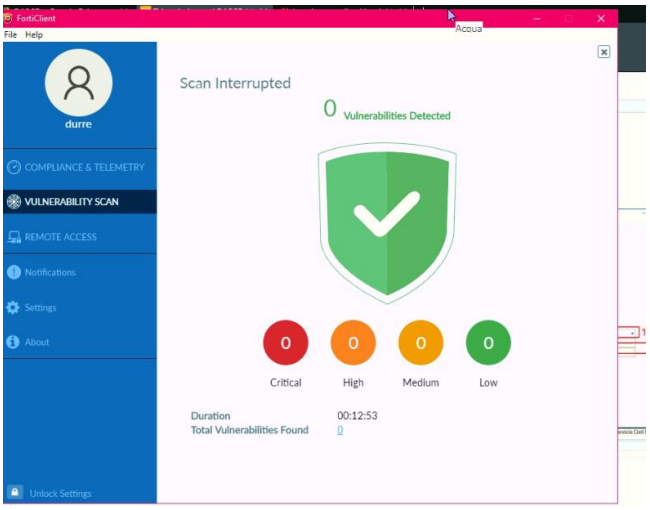
7.2.1.11.1 Observaciones 2021

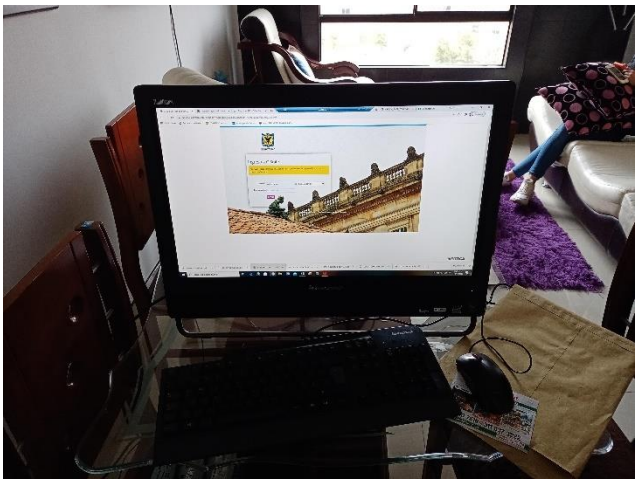
- Se actualizaron las configuraciones del firewall para implementar las recomendaciones de seguridad emitidas en el informe de la vigencia 2020, sin embargo debido a la obsolescencia programada identificada en el firewall actual se adelantó el proceso de selección, evaluación ya adquisición de un nuevo firewall.

- Se ha avanzado en la configuración de permisos en el firewall por grupos en el directorio activo y se adelantó la configuración de ipV6 en el firewall de manera que todas las reglas definidas para ipV4 se migren adecuadamente a esta configuración.

- Se realizó una validación de todas las reglas y se desactivaron las que ya no se necesitan como parte de la depuración para preparan la migración al nuevo firewall y simplificar la implantación en el mismo.

- En cuanto a los conexiones remotas y VPN´s se realizo la validación de vulnerabilidades en los equipos remotos mediante visitas programadas a los usuarios, además se actualizaron las políticas del dominio para el control de conexiones por escritorio remoto:





- Se segmento de forma adecuada en el firewall el segmento de red de los servidores principales para evitar posibles descubrimientos o accesos no autorizados y se configuro el segmento para el servidor de carpetas compartidas de tal manera que no permita identificar DNS o direcciones ip que puedan utilizarse para un ataque a los otros segmentos de red.

7.2.1.11.2 Seguimiento a las recomendaciones 2020

N°	OBSERVACIÓN DE MEJORA – RECOMENDACIÓN 2020	ESTADO	SEGUIMIENTO 2021
1.	Aplicar la misma configuración de la VLAN's de áreas funcionales, al segmento de servidores que aún permanece expuesto a escaneos desde otros segmentos, aquellos servicios que deban ser visibles desde los otros segmentos deben configurase sin comprometer todo el segmento, en especial los servidores de dominio y de bases de datos.	↑	Ya se encuentra atendida esta recomendación de acuerdo con la inspección de la configuración del firewall.
2.	Configurar en el cliente VPN y en la configuración del firewall, el bloqueo de conexiones de equipos que no cumplan con el análisis de vulnerabilidades o tengan algún problema de seguridad. En	↑	Se bien no se habilito el bloqueo de conexiones de equipos que no cumplan con el análisis de vulnerabilidades o tengan algún problema de seguridad, se realizo una campaña para la validación en los

N°	OBSERVACIÓN DE MEJORA – RECOMENDACIÓN 2020	ESTADO	SEGUIMIENTO 2021
	el panel de control de *Security Fabric* del firewall, se encuentra el detalle estas recomendaciones y los pasos que se deben realizar para implementarla.		equipos de usuarios dando cumplimiento a esta recomendación
3.	Continuar la construcción del dominio incorporado los siguientes elementos documentales de política: • Controles de red para la gestión de la seguridad en las comunicaciones • Controles de red para interconexiones mediante WLAN • Controles de red para uso de equipos móviles corporativos y/o bajo la modalidad BYOD y teletrabajo • Controles para manejo de proveedores de servicios de telecomunicaciones, redes de datos y seguridad. • Segregación de las redes organizacionales • Transferencia de información.		Si bien se ha avanzado en la documentación de algunos controles en este dominio aún no se ha avanzado en la construcción de los enunciados en esta recomendación. Sin embargo se tienen identificados en el Listado de Instrumentos pendientes incluido en la Matriz de Riesgos de Seguridad.
4.	Activar y configurar los filtros para la prevención de perdida de datos (DLP) en el firewall de acuerdo con lo especificado en el marco del proyecto SIC - Sistema Integrado de Conservación del Plan de Acción de Trasformación Digital. También se deben configurar filtros adicionales para afinar la prevención de intrusos en el firewall, ya que solo tiene la protección por defecto		Se tiene planificado activarlo en la implementación del nuevo Firewall

7.2.1.11.3 Nuevas Recomendaciones

N°.	RECOMENDACION
1.	Adelantar la construcción de los instrumentos faltantes identificados en el Listado de Instrumentos pendientes incluido en la Matriz de Riesgos de Seguridad para este dominio
2.	Atender la recomendación de la vigencia anterior que se presenta con la valoración

7.2.1.12 A.14. Adquisición, desarrollo y mantenimiento de sistemas.

7.2.1.12.1 Observaciones 2021

👍 En este dominio se evidencia un gran avance en la implementación controles de acuerdo con las recomendaciones emitidas por la auditoría en informes anteriores, ya que se adoptado e implementado correctamente todos los lineamientos de metodología de desarrollo ágil basado en Scrum.

👉 Se han definido de forma adecuada los estándares de desarrollo para código limpio, procedimiento de gestión de códigos y se está siguiendo correctamente el procedimiento de gestión de cambios, sin embargo aun no se han formalizado.

👍 Se cuenta con la Herramienta Taiga para el control de la metodología de desarrollo adoptada, en donde se gestiona adecuadamente los requerimientos, historias de usuarios, planeación, gestión de capacidad, tiempos de desarrollo y sus desviaciones.

7.2.1.12.2 Seguimiento a las recomendaciones 2020

N°	OBSERVACIÓN DE MEJORA – RECOMENDACIÓN 2020	ESTADO	SEGUIMIENTO 2021
1.	Documentar, formalizar, implementar y divulgar los procedimientos de gestión de cambios y gestión de la capacidad de la plataforma tecnológica en el marco de la implementación del MSPI especialmente para los controles: 12.1.2 Gestión de cambios. 12.1.3 Gestión de capacidades...	➡	Se creó el instrumento: Informe pruebas de carga y rendimiento como parte de la gestión de capacidad sin embargo, aun no cuenta con un procedimiento formal. Se actualizó el procedimiento de gestión de cambios (Ver2-A-TIC-PR-007 PROCEDIMIENTO DE GESTIÓN DE CAMBIOS) en el cual se incluye el control de cambios en los sistemas, la revisión y seguimiento del cambio referenciando adecuadamente el Plan de Reversión (roll-back) previamente estipulado en Requerimiento de Cambio. Se incluye en el procedimiento de cambios: en las políticas operacionales la definición: "Todo cambio debe contar con la evaluación de su impacto, la urgencia, el costo, los beneficios para el servicio y de riesgos, para su programación y aprobación. La evaluación de riesgos contempla los riesgos
2.	En el marco del proyecto de implementación MSPI adelantar el procedimiento de gestión de cambios en concordancia con los controles ISO 27001. 14.2.2 Procedimientos de control de cambios en los sistemas. 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema productivo. 14.2.4 Restricciones a los cambios en los paquetes de software. Incluir la valoración de la pertinencia de los cambios para el negocio: regulatorio, de	⬆	

N°	OBSERVACIÓN DE MEJORA – RECOMENDACIÓN 2020	ESTADO	SEGUIMIENTO 2021
	valor misional, de valor no misional o de apoyo a la operación.		financieros, técnicos, de seguridad de la información y del negocio, los cuales deberán ser evaluados en el comité de cambios. la valoración de riesgo de seguridad de la información" , dando cumplimiento a las recomendaciones emitidas.
3.	En el marco del dominio 14 del MSPI crear las políticas y procedimientos y actualización de formatos para la Adquisición y Desarrollo de software aplicativo en tres escenarios: • Adquisición de software comercial. • Desarrollo de software por encargo a terceros. • Desarrollo de software interno Crear los procedimientos de cambios a sistemas de información que incluyan el análisis de viabilidad técnica.		En cuanto al Desarrollo de software interno se ha avanzado en la actualización de políticas y se cuenta con la documentación adecuada sin embargo aún no se ha formalizado como parte de la documentación del dominio. En procedimientos asociados a la adquisición y de desarrollo por encargo aún no se presenta avance.

7.2.1.12.1 Nuevas Recomendaciones

N°.	RECOMENDACION
1.	Atender la recomendación de la vigencia anterior que se presenta con la valoración

7.2.1.13 A.15. Relaciones con los proveedores.

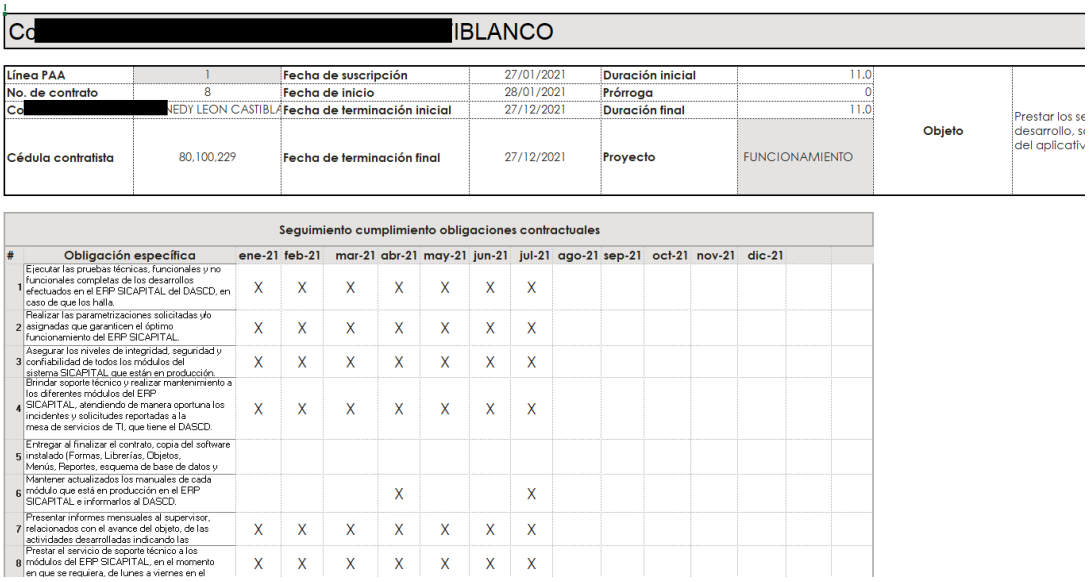
7.2.1.13.1 Observaciones 2021

Se incluyó la póliza de transferencia de conocimiento en los contratos con servicios profesionales, técnicos y con terceros en la cual se especifica la duración, horarios y temáticas de estas capacitaciones.

Se incluyó en las obligaciones del contrato el diligenciamiento y uso de los procedimientos de seguridad y formatos de la OTIC, y se incluyen en los anexos técnicos las consideraciones de seguridad alineadas con las políticas de la entidad.

En cuanto al contrato de mantenimiento si bien se incluyeron en el anexo técnico las condiciones de seguridad, sin embargo aún no se especificó dentro de las obligaciones del contrato, obligaciones para el uso de software legal en la ejecución de este y/o utilización de archivos inseguros con contraseñas, necesarias para evitar las fugas de seguridad que se detectaron.

Se diseño e implemento el uso del formato *OTIC Seguimiento contratos*, en el cual se registra de forma adecuada el seguimiento a las obligaciones específicas de todos los contratos periódicamente:



Co[redacted]IBLANCO

Línea PAA	1	Fecha de suscripción	27/01/2021	Duración inicial	11.0		
No. de contrato	8	Fecha de inicio	28/01/2021	Prórroga	0		
Co[redacted]	NEDY LEON CASTIBLA	Fecha de terminación inicial	27/12/2021	Duración final	11.0		
Cédula contratista	80.100.229	Fecha de terminación final	27/12/2021	Proyecto	FUNCIONAMIENTO	Objeto	Prestar los se desarrollo, s del aplicativ

Seguimiento cumplimiento obligaciones contractuales

#	Obligación específica	ene-21	feb-21	mar-21	abr-21	may-21	jun-21	jul-21	ago-21	sep-21	oct-21	nov-21	dic-21
1	Ejecutar las pruebas técnicas, funcionales y no funcionales completas de los desarrollos efectuados en el ERP SICAPITAL del DASCD, en caso de que los halla.	X	X	X	X	X	X	X					
2	Realizar las parametrizaciones solicitadas y/o asignadas que garanticen el óptimo funcionamiento del ERP SICAPITAL.	X	X	X	X	X	X	X					
3	Asegurar los niveles de integridad, seguridad y confiabilidad de todos los módulos del sistema SICAPITAL que están en producción.	X	X	X	X	X	X	X					
4	Brindar soporte técnico y realizar mantenimiento a los diferentes módulos del ERP SICAPITAL, atendiendo de manera oportuna los incidentes y solicitudes reportadas a la mesa de servicios de TI, que tiene el DASCD.	X	X	X	X	X	X	X					
5	Entregar al finalizar el contrato, copia del software instalado (Formas, Librerías, Objetos, Menús, Reportes, esquema de base de datos y												
6	Mantener actualizados los manuales de cada módulo que está en producción en el ERP SICAPITAL e informarlos al DASCD.				X			X					
7	Presentar informes mensuales al supervisor, relacionados con el avance del objeto, de las actividades desarrolladas indicando las	X	X	X	X	X	X	X					
8	Prestar el servicio de soporte técnico a los módulos del ERP SICAPITAL, en el momento en que se requiera, de lunes a viernes en el	X	X	X	X	X	X	X					

7.2.1.13.2 Seguimiento a las recomendaciones 2020

N°	OBSERVACIÓN DE MEJORA – RECOMENDACIÓN 2020	ESTADO	SEGUIMIENTO 2021
1.	En los contratos no se incluyen condiciones de seguridad en la ejecución del contrato , ni en los desarrollos, ni se especifican los acuerdos de niveles de servicio -ANS	↑	En los nuevos contratos se están incluyendo los acuerdos de niveles de servicio y condiciones de seguridad. En cuanto a las condiciones de seguridad de contratos de desarrollo se especificaron el borrador de la política de desarrollo seguro y en el Manual de seguridad.
	Fortalecer el desarrollo del dominio construyendo un documento de política que incluya por lo menos los siguientes elementos: • Instrumentos ya existentes del proceso de contratación que puedan requerir algún ajuste. • Gestión de cambios en relación con terceros • Matriz de ANS por terceros y políticas de ANS	→	En el Manual de la Seguridad Digital se definieron y actualizaron las políticas de gestión de terceros en donde se han definido los lineamientos para la relación con terceros. Se han construido 4 modelos de acuerdos de confidencialidad para incluir en los contratos las condiciones de seguridad y políticas de propiedad intelectual

N°	OBSERVACIÓN DE MEJORA – RECOMENDACIÓN 2020	ESTADO	SEGUIMIENTO 2021
	• Políticas de accesos temporales a servicios TIC • Gestión de riesgos y requisitos de continuidad extensivos a proveedores • Acuerdos de confidencialidad • Políticas de propiedad intelectual • Criterios de aceptación de productos y servicios Matrices de evaluaciones de requisitos como insumo para estudios previos: funcionales, técnicos, económicos, de relación con el tercero: soporte y garantía y reputacionales.		• Aún no se cuenta con los siguientes instrumentos: Gestión de cambios en relación con terceros • Matriz de ANS por terceros y políticas de ANS • Gestión de riesgos y requisitos de continuidad extensivos a proveedores • Criterios de aceptación de productos y servicios. Ni las matrices de evaluación de requisitos.

7.2.1.13.1 Nuevas Recomendaciones

N°.	RECOMENDACION
1.	Atender la recomendación de la vigencia anterior que se presenta con la valoración

7.2.1.14 A.16. Gestión de incidentes de seguridad de la información.

7.2.1.14.1 Observaciones 2021

Se cuenta con el instrumento E-SIN-PR-003 Procedimiento de Gestión de Incidentes V1. En el cual se detalla el tratamiento , clasificación, contención del incidente y su flujo hasta la remediación del mismo.

Los incidentes de seguridad se están registrando adecuadamente en la herramienta de HelpPeople, en donde se permite realizar el seguimiento de este y se registran lecciones aprendidas, correctivos a tomar y se utiliza como base de conocimiento.

En el formato: *E-SIN-FM-008 FORMATO DE REGISTRO Y CONTROL DE INCIDENTES V1* se registran los responsables, la descripción del incidente, acciones correctivas y de contención, lecciones aprendidas y posibles vulnerabilidades. Sin embargo, al estar registrándose también los incidentes en la herramienta de HelpPeople, se incurre en un doble trabajo, por lo cual debería evaluarse el uso de esta última herramienta para que esta genere dicho formato automáticamente como un reporte.

7.2.1.14.2 Seguimiento a las recomendaciones 2020

N°	OBSERVACIÓN DE MEJORA – RECOMENDACIÓN 2020	ESTADO	SEGUIMIENTO 2021
1.	Ajustar los instrumentos del dominio para que contemple: - Un incidente de seguridad también puede ser de tipo “ético” para lo cual debe disponerse un canal de comunicación confidencial y establecer el protocolo a seguir para su análisis y acciones. - Establecer el funcionario responsable del monitoreo de manera independiente y a que herramientas debe tener acceso para hacer este monitoreo. - Recursos para la gestión de incidentes de seguridad de la información. - Establecer niveles de impacto para evaluar un incidente de seguridad y establecer su prioridad de atención con base en riesgos y criticidad de los activos de información. - Técnicas para utilizar para la recopilación de evidencia para propósitos de acciones legales y disciplinarias. - Herramienta de registro y consulta de acciones correctivas y lecciones aprendidas.		Si bien se esta utilizando la herramienta de HelpPeople para el registro y consulta de acciones correctivas y lecciones aprendidas, aun no se han ajustado los instrumentos con todos los puntos emitidos en esta recomendación. Ya se actualizó en el procedimiento de gestión de incidentes para determinar el canal de comunicación para el manejo de los incidentes de seguridad cuando son de tipo “ético”, en el Manual de Seguridad Digital que en el caso en el que se necesite o desee hacer un reporte anónimo, se cuenta con las herramientas https:// www.serviciocivil.gov.co/portal/form/ventanilla_virtual y https ://sdqs.bogota.gov.co/, los cuales permiten radicar solicitudes o peticiones de forma anónima y cargue de adjuntos. La información que se suministré mediante estos mecanismos es recibida inicialmente por el área funcional de correspondencia y es tratada de forma confidencial de acuerdo con el acuerdo de confidencialidad y no divulgación de información que debe firmar cada integrante de este equipo de trabajo.

7.2.1.14.1 Nuevas Recomendaciones

N°.	RECOMENDACION
1.	Atender la recomendación de la vigencia anterior que se presenta con la valoración
2.	Implementar el formato de registro y control de incidentes como un reporte de la herramienta de HelpPeople para unificar el registro de los incidentes de seguridad.

7.2.1.15 A.17.1. Continuidad de seguridad de la información.

7.2.1.15.1 Observaciones 2021

Se cuenta con el instrumento : PLAN_RECUPERACION_DESATRES_TI_V6 correctamente actualizado con las recomendaciones dadas por la auditoría en los informes anteriores, en donde

se detalla la estrategia de continuidad de la Entidad y que está debidamente estructurado como un manual para la construcción del Plan de recuperación de desastres y de continuidad del negocio, y tiene algunos avances con respecto al análisis BIA y la identificación de actores.

- Se creó la guía A-TIC-GI-002 GUIA_DE_PLAN_DE_GENERACION_COPIAS_DE SEGURIDAD_DASCD_V1 en la cual se describe de forma adecuada el esquema de copias de seguridad contemplado por el DASCD incluye Servicios, Aplicaciones, Bases de datos y Documentos de uso.

7.2.1.15.2 Seguimiento a las recomendaciones 2020

N°	OBSERVACIÓN DE MEJORA – RECOMENDACIÓN 2020	ESTADO	SEGUIMIENTO 2021
1.	Incluir e implementar dentro del plan de copias de seguridad los respaldo a configuraciones de elementos activos de red, de servidores físicos y configuraciones de motores de bases de datos.	→	Si bien se encuentran implementadas y se ejecutan copias de seguridad sobro los elementos de red no se incluyeron en la en la guía del plan de generación de copias de seguridad.
2.	Adelantar las pruebas integrales al Plan de Continuidad y documentar los protocolos y resultados, contemplar los lineamientos de ISO 27002:2013 en el control 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	→	Si bien el plan se probo debido a dos contingencias presentadas en el periodo, en la cuales se demostró la efectividad de este y se documentaron los resultados, Es importante tener un plan de pruebas periódicas con diferentes escenarios.
3.	Continuar la identificación de riesgos y asociación con los controles de MSPI dando cobertura a los demás objetivos de control de la norma.	→	Se evidencian mejoras en la identificación de riesgos, aunque todavía no se relacionan claramente con los activos críticos, ni se han abordado todos los dominios de MSPI.
4.	Documentar todo el plan y programación de copias de seguridad de la entidad, en un único formato que permita identificar rápidamente tiempos, ubicaciones, responsables y medios de todos los respaldos y estrategias utilizadas en el proceso.	↑	Se adelantó la creación de la A-TIC-GI-002 GUIA_DE_PLAN_DE_GENERACION_COPIAS_DE SEGURIDAD_DASCD_V1 para atender esta recomendación, sin embargo se debe complementar con un formato que permita identificar rápidamente la disposición final de todas las copias de seguridad de la información respaldada y de esta forma disminuir los tiempos de recuperación.

7.2.1.15.1 Nuevas Recomendaciones

N°.	RECOMENDACION
1.	Atender las recomendaciones de la vigencia anterior que se presentan con la valoración →

8 CONCLUSIONES

La presente auditoría evidencia que la OTIC ha adelantado un proceso de análisis e implementación de las recomendaciones emitidas en el informe de auditoría del Contrato 56 de 2021. Como resultado, se da cumplimiento a los lineamientos emitidos por MINTIC en el Manual de Gobierno digital del año 2019 y se logra la implementación del Modelo de Seguridad y Privacidad de la información, en la medida en que la OTIC ha asignado a un recurso dedicado a dicha implementación.

Es posible evidenciar grandes avances en el proceso de implementación del MSPI. A la fecha de esta auditoría se ha cubierto gran parte de la construcción de los instrumentos definidos en los lineamientos emitidos por MINTIC para tal implementación. Así mismo, se ha evolucionado en la construcción e implementación de los controles tecnológicos que abarcan todos los dominios del modelo. Sin embargo, queda por perfeccionar los mecanismos para medir técnicamente la efectividad de los controles y la toma de acciones correctivas, de acuerdo con las recomendaciones presentadas en este informe. Así mismo, resulta necesario implementar el modelo de mejora continua para culminar con la implementación del MSPI.

ORIGINAL FIRMADO

YOLANDA CASTRO SALCEDO
Jefe Oficina de Control Interno

EQUIPO AUDITOR		
NOMBRES	**CARGO**	**FIRMA**
YADIRA VELOSA POVEDA	CONTRATISTA	ORIGINAL FIRMADO