MEMORANDO

MINDEPORTE 28-12-2021 15:32
Al Contestar Cite Este No.: 2021IE0010416 Fol:1 Anex:1 FA:22
ORIGEN 110-OFICINA DE CONTROL INTERNO / JAMES JILBERT LIZARAZO BARBOSA
DESTINO 100-DESPACHO DEL MINISTRO / GUILLERMO HERRERA CASTAÑO
ASUNTO INFORME FINAL AUDITORIA PROCESO "GESTIÓN DE TECNOLOGÍAS DE LA
OBS

Código Dependencia

2021IE0010416

PARA: GUILLERMO HERRERA CASTAÑO
Cargo: Ministro del Deporte

DE: 110-DESPACHO DEL MINISTRO/OFICINA DE CONTROL INTERNO

ASUNTO: Informe Final auditoria Proceso "Gestión de Tecnologías de la Información y las Comunicaciones".

Cordial Saludo señor Ministro:

De acuerdo con lo establecido en el Decreto Nacional No. 1083 de 2015 "Único Reglamentario del Sector Función Pública", modificado ´por el Decreto Nacional No. 00648 de 2017 y en el Plan Anual de Auditoria Interna año 2021, aprobado por el Comité Institucional de Coordinación de Control Interno, en sesión realizada el 6 de abril de 2021, y modificado en sesión del 20 de octubre de 2021, me permito presentar Informe Final de la auditoría interna al Proceso "Gestión de Tecnologías de la Información y las Comunicaciones" – Políticas de Seguridad - Plan Estratégico de Tecnologías de la Información y las comunicaciones - PETI, Riesgos de Corrupción, de Gestión y de Seguridad del Proceso y Plan de Seguridad y Privacidad de la Información-PSPI del Ministerio del Deporte.

Teniendo en cuenta el contenido de dicho informe y en cumplimiento de lo establecido en el Manual de Auditoría Interna SG-MN-002 y el Procedimiento de Auditoría Interna SG-PD-004 se solicita la elaboración del plan de mejoramiento, en el módulo Mejora de la Plataforma Isolucion Mejora, a más tardar a los cinco (5) días hábiles a partir del recibo del informe final, una vez formulado este, el plazo máximo para el cierre de cada hallazgo es de tres (3) meses.

Agradezco la atención al presente.

Cordialmente,

JAMES JILBERT LIZARAZO BARBOSA
Cargo Jefe Oficina de Control Interno

Anexos: Informe Final Auditoria Proceso “Gestión de Tecnologías de la Información y las Comunicaciones” en formato PDF contenido en 22 folios.

c.c. Integrantes del Comité Institucional de Coordinación de Control Interno y Grupo Interno de Trabajo TICs.

Elaboró:Josè Edgar Hernando Galarza Bogota - Profesional Contratista OCI

Revisó:
ANDRES GALVIS PINEDA
28-12-2021 15:25

1. DESCRIPCIÓN DE LA AUDITORÍA

Tipo de Informe: Final

Unidad Auditable: Proceso "Gestión de Tecnologías de Información y las Comunicaciones".

Responsable Unidad Auditable:

- Secretaria General
- Coordinador GIT TICs.

***Fecha de Apertura*:** 30/11/2021

Fecha de Cierre: 22/12/2021

Objetivo de la Auditoría:

1. Evaluar el estado de avance del Plan Estratégico de Tecnologías de la Información y las comunicaciones - PETI del Ministerio del Deporte.

2. Evaluación de la eficacia de los controles de los Riesgos de Corrupción, de Gestión y de Seguridad del Proceso "Gestión TICs" incluidos en el Mapa de Riesgos del Ministerio del Deporte.

3. Evaluar el estado de avance del Plan de Seguridad y Privacidad de la Información-PSPI del Ministerio del Deporte.

Alcance de la Auditoría: Comprende el análisis de la información reportada por el líder del Proceso Gestión TIC o gestionada por los sistemas de información del Ministerio del Deporte entre el 01-01-2021 al 30-10-2021.

Criterios de la Auditoría:

• **Decreto Nacional No. 1078 de 2015** "Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".

• **Decreto Nacional No. 1008 de 2018** "Por el cual se establecen los lineamientos generales

de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".

• **Manual de Gobierno Digital V6** diciembre de 2018

• **Manual del Modelo Integrado de Planeación y Gestión** MIPG V4 marzo 2021

• **Decreto Nacional No. 403 de 2020**, "*Por el cual se dictan normas para la correcta implementación del Acto Legislativo 04 de 2019 y el fortalecimiento del control fiscal." artículos 51. Evaluación del control interno, 61. Articulación con el control interno, Parágrafos 1 y 2; 62. Sistema de Alertas del Control Interno, 68. De la advertencia, 76. Actuación especial de fiscalización, 149 Organización del control interno, 150. Dependencia de control interno, 151 Deber de entrega de información para el ejercicio de las funciones de la unidad u oficina de control interno*.

• **Resolución 500** de marzo de 2021 del Ministerio TIC ""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"

• **Documento PETI**,

• **Política de Seguridad y Privacidad de la Información**,

• Proceso "Gestión TICS", procedimientos, formatos, riesgos, controles, entre otros.

• Indicadores, planes de acción, mapas de riesgos de Gestión y de Corrupción, procedimientos y demás documentos del Sistema Integrado de Gestión del Ministerio del Deporte (Antes Coldeportes) vigentes

• Normatividad adicional interna y/o externa asociada al proceso auditado.

Limitaciones: Sin limitaciones.

Equipo Auditor: José Edgar Hernando Galarza Bogotá – Profesional Contratista OCI

2. TÉCNICAS DE AUDITORÍA APLICADAS

a) **Indagación**: Entrevistas directas con responsables del proceso o actividad auditada o con terceros que tengan relación con las operaciones de mismo (evidencias testimoniales).

b) **Observación**: Verificación ocular de operaciones y procedimientos durante la ejecución de las actividades del proceso.

c) **Rastreo**: Seguimiento de una operación, a través de la documentación respectiva, a fin de conocer y evaluar su ejecución (evidencias analíticas).

d) **Comunicación**: Obtención de información directa y por escrito de la entidad auditada (evidencias testimoniales).

e) **Análisis**: Separación de los elementos o partes que conforman una operación, actividad, transacción o proceso, con el propósito de establecer sus propiedades y conformidad con los criterios de orden normativo y técnico (evidencias analíticas).

f) **Revisión selectiva**: Examen de las características importantes que debe cumplir una actividad, informe o documento, seleccionándose así parte de las operaciones que serán evaluadas o verificadas en la ejecución de la auditoría. (evidencias analíticas).

Entre otras que sean requeridas en el transcurso de la auditoría.

3. METODOLOGÍA

Para el desarrollo formal del ejercicio de verificación, se seleccionaron los controles de seguridad digital del mapa de riesgos del proceso TIC, de otra parte, se seleccionó una muestra aleatoria de los indicadores del PETI y adicionalmente se seleccionó una muestra aleatoria de los controles del Modelo de Seguridad y Privacidad de la Información que se tienen planeados implementar en la vigencia 2021.

Para la selección de la muestra de auditoria se tomó la base los controles de seguridad digital del Mapa de Riesgos de Seguridad Digital, los indicadores del PETI y los controles establecidos en el Plan de Seguridad y Privacidad de la Información.

Para los controles de Seguridad Digital se identificó un universo de dos (2) riegos para los cuales se tienen establecidos 11 controles, adicionalmente para el Tablero de Control de Indicadores del PETI se identificaron veintinueve (29) indicadores y de otra parte del Plan de Seguridad y Privacidad de la Información se identificaron cuarenta y dos (42) actividades de control a implementar mediante la definición de noventa y un (91) tareas.

Frente a lo mencionado se seleccionaron los once 11 controles correspondientes a los Riesgos de Seguridad Digital del Mapa de Riesgos del proceso de Gestión TICs, y una muestra de los indicadores del PETI y de las tareas de control del Plan de Seguridad y Privacidad de la Información 2020-2021, los cuales fueron:

Tabla No. 1: Controles Seleccionados en la Muestra del Mapa de Riesgos del Proceso Gestión TIC:

CONTROL	DESCRIPCION CONTROL	RIESGO	TIPOLOGIA
R4-C1-Con-1	Trimestralmente, el Coordinador TICS, debe Verificar que los funcionarios estén utilizando las herramientas dispuestas por la entidad para el intercambio de información, consultará a sus funcionarios las herramientas utilizadas para el intercambio de información y establecerá acuerdos sobre el uso de las mismas. En caso de identificar desviaciones en la ejecución del control, Se revisarán las sugerencias en el manejo de las herramientas y se renovarán los acuerdos en el uso de las mismas. De la ejecución de los controles se generará la siguiente evidencia: Acta de socialización	Divulgación de los datos personales que reposan en documentos y herramientas utilizadas en el proceso de gestión de TI	Seguridad Digital
R4-C1-Con-2	Semestralmente, el Coordinador TICS, debe Validar que los funcionarios no compartan información reservada para la entidad de acuerdo a las políticas definidas por la entidad, mediante la revisión del cumplimiento de las directrices establecidas en la política de protección de datos personales. En caso de identificar desviaciones en la ejecución del control, Realizara las sugerencias a que haya lugar para evitar que terceros no autorizados accedan a la información. De la ejecución de los controles se generará la siguiente evidencia: Informe de gestión	Divulgación de los datos personales que reposan en documentos y herramientas utilizadas en el proceso de gestión de TI	Seguridad Digital
R4-C2-Con-1	Trimestralmente, el Coordinador TICS, debe Validar que los funcionarios a cargo conozcan las practicas seguras, mediante la verificación de la asistencia a las actividades de formación en seguridad digital que desarrolle la entidad. En caso de identificar desviaciones en la ejecución del control, informará a los jefes o coordinadores de las dependencias la falta de asistencia de sus funcionarios a las actividades de formación. 7De la ejecución de los controles se generará la siguiente evidencia: Correó electrónico	Divulgación de los datos personales que reposan en documentos y herramientas utilizadas en el proceso de gestión de TI	Seguridad Digital
R4-C2-Con-2	Semestralmente, el Coordinador TICS, debe Validar que el sistema de detección de amenazas para el correo está actualizado y configurado de acuerdo a las necesidades de la entidad y tendencias del mercado, liderando las pruebas necesarias y los cambios requeridos a fin de hacer ajustes a las herramientas de protección de correo. En caso de identificar desviaciones en la ejecución del control, tomará las medidas correctivas que estén al alcance a fin de corregir la situación. De la ejecución de los controles se generará la siguiente evidencia: Informe del mantenimiento	Divulgación de los datos personales que reposan en documentos y herramientas utilizadas en el proceso de gestión de TI	Seguridad Digital
R4-C3-Con-1	Semestralmente, el Coordinador TICS, debe Validar que el sistema de protección perimetral y los permisos de acceso a las bases de datos se encuentren actualizados y configurados correctamente, liderará las pruebas necesarias y los cambios requeridos a fin de hacer ajustes a las herramientas de	Divulgación de los datos personales que reposan en documentos y herramientas utilizadas en el proceso de gestión de TI	Seguridad Digital

CONTROL	DESCRIPCION CONTROL	RIESGO	TIPOLOGIA
	protección de bases de datos. En caso de identificar desviaciones en la ejecución del control, tomará las medidas correctivas que estén al alcance a fin de corregir la situación. De la ejecución de los controles se generará la siguiente evidencia: Informe del mantenimiento		
R5-C1-Con-1	Cuatrimestralmente, el Coordinador TICS, debe Validar que el personal del grupo interno de trabajo haya cumplido con el entrenamiento en seguridad digital, consultando a sus funcionarios y contratistas sobre las actividades de formación en seguridad en las cuales han participado (estas deben ser dirigidas por el encargado de seguridad digital). En caso de identificar desviaciones en la ejecución del control, estas deben ser comunicadas al encargado de seguridad digital para tomar las medidas adecuadas. De la ejecución de los controles se generará la siguiente evidencia: Correo electrónico	Pérdida y/o modificación de la información contenida en los documentos y herramientas utilizadas en el proceso de gestión de TI	Seguridad Digital
R5-C2-Con-1	Cuatrimestralmente, el Coordinador TICS, debe Validar que se esté llevando a cabo de manera correcta el proceso de Backus de acuerdo a la Política de Seguridad Digital de la entidad y los procedimientos asociados, solicitando y verificando el reporte de los Backus realizados y verificando la correcta ejecución de los mismos. En caso de identificar desviaciones en la ejecución del control, tomará las medidas correctivas a su alcance a fin de corregir la situación. De la ejecución de los controles se generará la siguiente evidencia: Informe de la actividad	Pérdida y/o modificación de la información contenida en los documentos y herramientas utilizadas en el proceso de gestión de TI	Seguridad Digital
R5-C2-Con-2	Cuatrimestralmente, el Coordinador TICS, debe validar que se estén llevando a cabo de manera correcta los procesos de mantenimiento de infraestructura y aplicativos, mediante el seguimiento al avance del plan de mantenimiento preventivo definido al principio de cada vigencia. En caso de identificar desviaciones en la ejecución del control, tomará las medidas correctivas que estén a su alcance a fin de corregir la situación. De la ejecución de los controles se generará la siguiente evidencia: informe de la actividad	Pérdida y/o modificación de la información contenida en los documentos y herramientas utilizadas en el proceso de gestión de TI	Seguridad Digital
R5-C3-Con-1	Semestralmente, el Coordinador TICS, debe validar que los aplicativos y la infraestructura estén configurados de manera correcta ante eventuales ataques informáticos, mediante solicitud para realizar actividades de hacking ético a los diferentes aplicativos e infraestructura, estableciendo los requerimientos a evaluar y las herramientas a utilizar. En caso de identificar desviaciones en la ejecución del control, tomará las medidas correctivas que estén a su alcance a fin de corregir las vulnerabilidades encontradas en el ejercicio de hacking ético. De la ejecución de los controles se generará	Pérdida y/o modificación de la información contenida en los documentos y herramientas utilizadas en el proceso de gestión de TI	Seguridad Digital

CONTROL	DESCRIPCION CONTROL	RIESGO	TIPOLOGIA
	la siguiente evidencia: informe de vulnerabilidades y mejoras a realizar		
R5-C4-Con-1	Semestralmente, el Coordinador TICS, debe verificar los permisos de acceso de administrador a los sistemas de la entidad e identificar los funcionarios y contratistas que tienen la posibilidad de realizar modificaciones, verificando quiénes tienen acceso a los sistemas a cargo del grupo de trabajo. En caso de identificar desviaciones en la ejecución del control, tomará las medidas correctivas que estén a su alcance a fin de corregir la situación. De la ejecución de los controles se generará la siguiente evidencia: informe de la actividad	Pérdida y/o modificación de la información contenida en los documentos y herramientas utilizadas en el proceso de gestión de TI	Seguridad Digital
R5-C4-Con-2	Semestralmente, el Coordinador TICS, debe verificar que estén habilitados todos los logs y que la información disponible en los mismos permita identificar quién realiza los cambios, mediante solicitud del reporte de logs disponibles en cada sistema y la verificación de la información que se está almacenando, así como de su completitud. En caso de identificar desviaciones en la ejecución del control, tomará las medidas correctivas que estén a su alcance a fin de corregir la situación. De la ejecución de los controles se generará la siguiente evidencia: informe de la actividad	Pérdida y/o modificación de la información contenida en los documentos y herramientas utilizadas en el proceso de gestión de TI	Seguridad Digital

Fuente: Mapa de Riesgos proceso Gestión TICs.

Tabla No. 2: Indicadores Seleccionados Tablero de Control del PETI

ACTIVIDAD	ID	TIPO	INDICADOR
Estrategias 1	ESTR-01	Estratégico	Controlar el porcentaje de iniciativas planeadas, relacionadas y ejecutadas en el PETI.
Calidad 1	CALI-01	Calidad	Semestralmente ,el Coordinador TICS, debe Validar que los Medir el porcentaje de los usuarios de TI satisfechos con la calidad de TI.
Operación 3	OPER-03	Operativo	Medir el nivel de porcentaje de bienes y/o servicios de TI que se están adquiriendo en modalidad de Acuerdos Marco.
Seguridad 01	SEGU-01	Operativo	Controlar el porcentaje de incidentes significativos causados por riesgos de seguridad no identificados.
Seguridad 02	SEGU-02	Estratégico	Revisión la Política de seguridad de información por parte del comité de gestión.
Seguridad 11	SEGU-11	Gestión	Verificar que la documentación de gestión de cambios en hardware y software sean documentados.

ACTIVIDAD	ID	TIPO	INDICADOR
Seguridad 13	SEGU-13	Operativo	Validar que se están realizando las copias de seguridad según el plan de copias de seguridad.
Seguridad 18	SEGU-19	Gestión	Validar si se dio solución a los incidentes de seguridad reportados.

Fuente: PETI – Tablero de Control V- 300921.

Tabla No. 3: Controles seleccionados Plan de Implementación Seguridad y Privacidad de la Información 2020-2021

DOMINIO	ACTIVIDAD	TAREA	ID
POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	Actualización de lineamientos de riesgos	Actualización de lineamientos de riesgos	T-01
POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	Revisión Manual Políticas de Seguridad de la Información	Revisión Manual Políticas de Seguridad de la Información	T-12
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	SGSI	Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la Información	T-16
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	SGSI	Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo con la Normatividad vigente	T-17
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	SGSI	Revisar el avance de implementación del Plan de Seguridad y Privacidad en la Entidad	T-20
GESTIÓN DE ACTIVOS	Definir lineamientos para el levantamiento de activos de información	Actualización de metodología e instrumento de levantamiento de activos de información	T-32
GESTIÓN DE ACTIVOS	Socializar la guía de activos de Información	Socializar la guía de activos de Información	T-33
CONTROL DE ACCESO	Limitar el acceso a información y a instalaciones de procesamiento de información	Establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	T-42
CRIPTOGRAFÍA	Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información	Desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información	T-48
SEGURIDAD DE LAS OPERACIONES	Vulnerabilidades	Definir los lineamientos y el alcance para la realización de pruebas de vulnerabilidades	T-58
SEGURIDAD DE LAS OPERACIONES	Vulnerabilidades	Ejecución de las pruebas de vulnerabilidades y pentest de acuerdo al alcance y la metodología establecida	T-59
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida	Definir las directrices para análisis y especificaciones de requisitos de seguridad de la información en sistemas nuevos o mejoras a los existentes	T-68

Fuente: Plan de Implementación Seguridad y Privacidad de la Información 2020-2021, octubre 2020

Imagen 1: Calculo de la Muestra de indicadores y tareas de control

INGRESO DE PARÁMETROS	
Tamaño de la Población (N)	71
Error Muestral (E)	10%
Proporción de Éxito (P)	10%
Nivel de Confianza	90%
Nivel de Confianza (Z) (1)	1,645

TAMAÑO DE LA MUESTRA

Fórmula: 24

Muestra Óptima: 18

Fuente: Elaboración propia OCI.

Realizada la selección del universo de auditoría, paso seguido se solicitó, mediante el memorando **2021IE0008363** del 18 de noviembre de 2021, al coordinador del GIT de TICs, la información de evidencias de aplicación de los controles establecidos, así como también de la evaluación de los indicadores. En respuesta a lo anterior, las personas que fungieron como enlaces de la unidad auditada reportaron la información mediante carpeta compartida en la plataforma SharePoint.

Adicionalmente se realizaron tres (3) reuniones virtuales con los enlaces del GIT Tics con el objetivo de identificar y precisar la información requerida por el Equipo Auditor. En cada una de las reuniones se organizaron los temas de acuerdo con los objetivos de la Auditoria. En dichas reuniones se establecieron como fecha límite de entrega de la información el 9 de diciembre de 2021.

Así pues, la labor de verificación de eficacia de los controles inició con el análisis de la documentación de los registros establecidos en el diseño de los controles.

Por lo mencionado, se identificaron en la muestra de auditoria documentos tales como:

1. Evidencias de la aplicación de los controles a los Riesgos de Seguridad Digital del proceso de Gestión TICs, tales como los registros establecidos en el mapa de riesgos del proceso auditado.
2. Evidencias de la implementación de los controles del Modelo de Seguridad y Privacidad de la Información-MPSI.
3. Evidencias del avance de los indicadores del Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETI proyectado para el Ministerio del Deporte, mediante documentación del tablero de Control de Seguimiento del mismo.

En lo relacionado con el tema de socialización de la Política de Gobierno Digital, se validó el micrositio de seguridad de la información con que cuenta el Ministerio al igual que las actividades de capacitación realizadas por el GIT TICs en materia de Seguridad de la Información a los funcionarios de la Entidad.

Adicionalmente se identificó y valido las actividades de apropiación de la Política de Gobierno Digital realizadas por el Ministerio TIC en las que ha participado el Ministerio del Deporte.

4. RIESGOS CUBIERTOS EN LA AUDITORÍA

En el desarrollo de la auditoria se evaluaron los controles asociados a los siguientes riesgos del proceso, los cuales fueron identificados en el mapa de riesgos respectivo:

RIESGOS SEGURIDAD DIGITAL 2021:

a) Divulgación de los datos personales que reposan en documentos y herramientas utilizadas en el proceso de Gestión de las Tecnologías de la Información y las Comunicaciones.

b) Pérdida y/o modificación de la información contenida en los documentos y herramientas utilizadas en el proceso de Gestión TICs.

Los resultados de la realización de las pruebas de recorrido, a los controles que en la práctica son ejercidos para la mitigación de los riesgos, evidencia que se presentan debilidades de completitud respecto a la documentación formal establecida en la columna “Evidencia de la Ejecución de la Actividad de control”, lo anterior teniendo en cuenta que las evidencias aportadas por el Auditado no corresponden estrictamente a las establecidas en el Mapa de Riesgos, se procederá a elevar la respectiva observación en el acápite pertinente.

Con respecto a los indicadores del PETI se observan debilidades en la elaboración de las fichas de estos, lo cual se detalla en las observaciones correspondientes.

En lo que corresponde al Plan de Implementación de Seguridad de la Información, se observa que el Ministerio ha tenido avances en la implementación de los controles de acuerdo con el Cronograma, sin embargo, la actividad de aprobación del documento de “Política de Seguridad de la Información” por parte del “Comité Institucional de Gestión y Desempeño” a la fecha de este informe se encuentra pendiente.

INDICADORES DEL PLAN ESTRATÉGICO DE TECNOLOGIAS DE LA INFORMACION-PETI

En el desarrollo de la auditoria se evaluó una muestra de indicadores del tablero de control del PETI, realizadas las verificaciones documentales se observan debilidades en la elaboración de las fichas de estos, lo cual se detalla en las observaciones correspondientes.

De otra parte, se evidencia que de los dieciséis (16) proyectos del PETI planeados para iniciar su ejecución en las vigencias 2020 y 2021, el 94% han tenido avances, sin embargo, uno de ellos el Proyecto "Definición e implementación de la Arquitectura Empresarial", previsto para su ejecución durante la vigencia 2020 - 2023, a la fecha de corte del presente informe no ha tenido avance.

PLAN DE IMPLMENTACION SEGURIDAD DE LA INFORMACIÓN 2020-2021

En el desarrollo de la Auditoria se evaluó una muestra de los controles del Plan y se observa que el Ministerio ha tenido avances en la implementación de los controles de acuerdo con el Cronograma, sin embargo, la Actividad de aprobación del Documento de Políticas de Seguridad de la Información por parte del Comité de Gestión y Desempeño a la fecha de este informe se encuentra pendiente.

5. FORTALEZAS

- En cuanto a la implementación del Sistema de Seguridad y Privacidad de la Información el cual es uno de los pilares de la Política de Gobierno Digital, el Ministerio ha implementado un micro sitio en la Intranet para socializar los temas relacionados con el tema, dicha herramienta permite a los funcionarios y contratistas de la Entidad contar con información relevante y coadyuva a la apropiación de dicho sistema.
- El Ministerio del Deporte ha participado en los eventos organizados por el Ministerio TIC para apoyar a las entidades públicas en la apropiación e implementación de la Política de Gobierno Digital, cabe destacar que el Ministerio ha obtenido el primer puesto en el evento denominado Máxima Velocidad, dicho reconocimiento ha permitido avanzar en la implementación de la Política, al igual que tener al Ministerio del Deporte como referencia en la aplicación de buenas prácticas en la implementación de la Política.
- El Ministerio del Deporte cuenta con un equipo de funcionarios especializado en tema de Seguridad de la Información para apoyar la implementación del Modelo de Seguridad y Privacidad de la Información.

6. RESUMEN DE HALLAZGOS Y OBSERVACIONES

Código	Título
H – GT – 01 – 2021	*EVIDENCIAS DE REGISTROS DE LA APLICACIÓN DE LOS CONTROLES DE LOS RIESGOS DE SEGURIDAD DIGITAL*
H – GT – 02 – 2021	*AVANCE DEL PROYECTO "Definición e implementación de la Arquitectura empresarial." DEL PETI*

Código	Título
O – GT – 01 – 2021	*MEDICION DEL INDICADOR Seguridad-11 "Verificar que la documentación de gestión de cambios en hardware y software sean documentados."*
O – GT – 02 – 2021	*INDICADOR DEL PETI SEGU-13 "Validar que se están realizando las copias de seguridad según el plan de copias de seguridad.*
O – GT – 03 – 2021	*DOMINIO RELACION CON PROVEEDORES DEL PLAN DE IMPLEMENTACION DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.*
O – GT – 04 – 2021	*DOCUMENTO GT-MN-006 "Manual de Operación de la Política de Backus y Restauración" EN ISOLUCION.*

7. DESCRIPCIÓN DE LOS HALLAZGOS Y OBSERVACIONES

HALLAZGOS:

H – GT– 01 – 2021 – EVIDENCIAS DE REGISTRO DE LA APLICACIÓN DE LOS CONTROLES DE LOS RIESGOS DE SEGURIDAD DIGITAL

Condición:

En el 63,63% de los controles de los riesgos de Seguridad Digital evaluados en el procedimiento auditor, se evidencia que se presentan debilidades de completitud respecto a la documentación formal establecida en la columna "Evidencia de la Ejecución de la Actividad de control" del Mapa de Riesgos del Proceso Gestión TICs, lo anterior teniendo en cuenta que las evidencias aportadas por el Auditado no corresponden estrictamente a las establecidas en dicho Mapa de Riesgos. (ver anexo No. 1).

Criterios:

El Mapa de Riesgos del Proceso Gestión TICs establece en la columna "Evidencia de la Ejecución de la Actividad de control", los documentos que soportan la aplicación del control, de acuerdo con lo definido en la "Guía para la administración del riesgo y el diseño de controles en entidades públicas" V5, sin embargo al no contar con las evidencias definidas formalmente, los beneficios de la gestión del riesgo establecidos en dicho manual como son: Apoyo a la toma de decisiones, Garantizar la operación normal de la organización, Minimizar la probabilidad e impacto de los riesgos, Mejoramiento en la calidad de procesos y sus servidores (calidad va de la mano con riesgos), Fortalecimiento de la cultura de control de la organización, Incrementar la capacidad de la entidad para

alcanzar sus objetivos, dotar a la entidad de herramientas y controles para hacer una administración más eficaz y eficiente, se pueden ver afectados.

El procedimiento GO-PD-011- ADMINISTRACION DE RIESGOS tiene como objetivo: "*Administrar los riesgos de gestión, corrupción y seguridad de la información del Ministerio del Deporte, mediante la identificación, valoración, monitoreo y seguimiento de riesgos, de acuerdo con los lineamientos establecidos en la política de administración del riesgo del Ministerio del Deporte", en sus actividades 9- Efectuar el monitoreo y reporte de los controles de riesgos 10- Verificar los resultados del monitoreo de riesgos, se definen las acciones de monitoreo de los riegos*.

Posible Causa identificada por la Oficina de Control Interno:

- Posibles debilidades de verificación de la aplicación y elaboración de la traza documental de los controles, por parte de los responsables
- Posible desactualización del Mapa de Riesgos del proceso Gestión TICs.
- Posible debilidad en la aplicación de los controles por parte de las diferentes líneas de defensa.

Descripción del Riesgo:

Incumplimiento normativo en materia de gestión de los Riesgo del proceso.

Lo evidenciado en la auditoria se relaciona con el Riesgo Estratégico, incluido en el mapa de Riesgo del Proceso Gestión Organizacional, denominado:

"*Incumplir los lineamientos del Modelo Integrado de Planeación y Gestión*"

Del cual se evidencia posible materialización de la causa No 1

"Debilidad en el seguimiento a la implementación de MIPG"

Así mismo, se evidencia debilidad en la ejecución del Control:

"Cada vez que se requiera, el Profesional asignado de la Oficina Asesora de Planeación, debe verificar el cumplimiento de las actividades programadas, a través del seguimiento a las actividades del Plan de Trabajo para la Implementación del Modelo Integrado de Planeación y Gestión. En caso de identificar desviaciones en la ejecución del control, se debe enviar las observaciones vía correo electrónico al líder de política institucional de gestión y desempeño con copia al enlace encargado del reporte de las actividades por proceso. De la ejecución de los controles se generará la siguiente evidencia: Correos electrónicos".

Lo Anterior, se sustenta al evidenciar posible falta de seguimiento por parte de la primera y segunda línea de defensa en el cumplimiento de los lineamientos normativos para la Gestión del Riesgo.

Efectos:

- Posibles materializaciones de los riesgos que son mitigados con los controles establecidos.
- Posible ineficacia en la ejecución del control
- Posibles procesos disciplinarios por incumplimiento de la normatividad.
- Posibles hallazgos por parte de la Contraloría General de la Republica.

Derecho a la Réplica:

Mediante comunicación 2021IE0010312 del 27 de diciembre de 2021, el Grupo Interno de Trabajo TICs informó que no presenta réplica al informe preliminar.

Por lo anterior el Hallazgo se mantiene en las mismas condiciones establecidas en el Informe Preliminar.

Recomendaciones

- Se recomienda actualizar lo relacionado con los registros de evidencia de ejecución de los controles del Mapa de Riegos en lo que respeta a los Riesgos de Seguridad Digital.
- Se recomienda elaborar y gestionar los registros de evidencias de aplicación de los controles de acuerdo con lo establecido en el Mapa de Riesgos
- Se recomienda fortalecer las actividades de verificación de la documentación de las evidencias de la ejecución de los controles establecidas en el Mapa de Riesgos del Proceso Gestión TICs.

H – GT - 02 – 2021 – AVANCE DEL PROYECTO "Definición e implementación de la Arquitectura empresarial." DEL PETI

Condición:

El proyecto "Definición e implementación de la Arquitectura empresarial." definido en el PETI para desarrollar en las vigencias 2020 a 2021, no ha presentado avances en la vigencia 2020, a la fecha de corte del presente informe. (ver anexo No. 2).

***Criterios**:*

El "Manual de la Política de Gobierno Digital" y sus guías complementarias las cuales son parte integral de los establecido en el Decreto Nacional No. 1008 de 2018 "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el

capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones", define en su numeral 1.5 Elementos de la Política, el elemento transversal Arquitectura como uno de los tres habilitadores de la Política de Gobierno Digital.

El PETI 2020-2023 estableció en su numeral 8.1 HOJA DE RUTA el conjunto de proyectos a desarrollar en las diferentes vigencias y estableció el proyecto "Definición e implementación de la Arquitectura empresarial", de otra parte, en el numeral 1.6 ANALISIS FINANCIERO definió una partida presupuestal para la vigencia 2021.

Posible causa identificada por la oficina de control interno:

- Posible debilidad en gestión para contar con un equipo técnico que apoye la función de Arquitectura Empresarial.
- Posible falta de presupuesto para financiar el proyecto.
- Posibles debilidades en la Planeación de los proyectos incluidos en el PETI del Ministerio del Deporte.

Descripción del Riesgo:

El presente hallazgo se relaciona con el riesgo del proceso Gestión TICs denominado

"*Adquisición de bienes y servicios informáticos desarticulados con las necesidades de la entidad*",

Del cual se evidencia posible materialización de la causa No.3

"*Falta de priorización de los proyectos de TI que requieren las dependencias*"

De igual forma, la Oficina de control Interno propone se incluya la siguiente causa No. 4:

"Planear proyectos sin la debida financiación que asegure la ejecución de estos".

Así mismo, se evidencia debilidad en la ejecución del Control:

"*Anualmente el Coordinador de TICs debe revisar la viabilidad y prioridad de todas las necesidades del proyecto de TI identificados durante el año, analizando su complejidad, compatibilidad, componentes, prioridad y tiempos de implementación. En caso de identificar desviaciones en la ejecución del control, es decir, proyectos inviables, se emite el respectivo concepto sobre el proyecto de TI solicitado. De la ejecución de los controles se generará la siguiente evidencia: Proyectos de TI viables y priorizados identificados para la Entidad o memorando, email u oficio de devolución al área solicitante*"

Lo Anterior, se sustenta al evidenciar posible falta de seguimiento por parte de la primera línea de defensa en el cumplimiento de los Planes establecidos para TI ya que pasadas 2

vigencias no se ha iniciado la ejecución del proyecto “Definición e implementación de la Arquitectura empresaria” referenciado en el PETI.

Efectos:

- Posible pérdida de oportunidad en la generación de capacidades tecnológicas de la Entidad.
- Posible incumplimiento con los establecido en la Política de Gobierno Digital de MIPG
- Posible incumplimiento de la meta del 100% del Plan de Acción 2021, establecida en el indicador “Porcentaje de implementación del PETI”
- Posibles hallazgos administrativos por parte de la Contraloría General de la Republica.

Derecho a la Réplica:

Mediante comunicación 2021IE0010312 del 27 de diciembre de 2021, el Grupo Interno de Trabajo TICs informó que no presenta réplica al informe preliminar.

Por lo anterior el Hallazgo se mantiene en las mismas condiciones establecidas en el Informe Preliminar.

Recomendaciones:

- Se recomienda, se realice la revisión y su respectiva actualización al menos con frecuencia anual del PETI, lo anterior con el fin de ajustarlo a las dinámicas estratégicas, normativas, tecnológicas y presupuestales, lo anterior con el objetivo de contar con un plan actualizado y articulado a las necesidades de la entidad.
- Se recomienda establecer un control en las políticas de Gestión TICs, que asegure la revisión y actualización del PETI con la frecuencia adecuada y el cual deba ser aprobado por el Comité Institucional de Gestión y Desempeño.
- Se recomienda fortalecer las actividades de seguimiento y monitoreo de la implementación de MIPG, en lo que respecta a la Política de Gobierno y Seguridad Digital

***OBSERVACIONES*:**

***O – GT – 01 – 2021* – MEDICION DEL INDICADOR DEL PETI Seguridad-11 “Verificar que la documentación de gestión de cambios en hardware y software sean documentados.”**

Se evidencia debilidad en la documentación de soporte de la actividad de verificación y medición del indicador, lo anterior teniendo en cuenta que con la evidencia aportada nos es posible identificar la totalidad de los cambios realizados y cuántos de estos fueron debidamente documentados durante cada semestre de 2021. Adicionalmente, no se cuenta con la traza documental de la medición del primer semestre.

Derecho a la Réplica:

Mediante comunicación 2021IE0010312 del 27 de diciembre de 2021, el Grupo Interno de Trabajo TICs informó que no presenta réplica al informe preliminar.

Por lo anterior la presente Observación se mantiene en las mismas condiciones establecidas en el Informe Preliminar.

Recomendaciones:

- Se recomienda evaluar y documentar el indicador de acuerdo con lo establecido en la ficha del mismo.
- Se recomienda que la información soporte de la medición del indicador sea gestionada y documentada de forma que permita su adecuada organización y preservación.
- Se recomienda establecer controles procedimentales para la gestión de cambios de la plataforma TIC de acuerdo con las mejores prácticas.

.

***O – GT – 02 – 2021* – INDICADOR DEL PETI SEGU-13"Validar que se están realizando las copias de seguridad según el plan de copias de seguridad.**

Se evidencia debilidades en la documentación soporte de la medición del indicador "**Validar que se están realizando las copias de seguridad según el plan de copias de seguridad",** lo anterior teniendo en cuenta que no se cuenta con los registros documentales de la validación mediante la medición cuatrimestral de acuerdo con lo establecido en la respectiva ficha del indicador.

Derecho a la Réplica:

Mediante comunicación 2021IE0010312 del 27 de diciembre de 2021, el Grupo Interno de Trabajo TICs informó que no presenta réplica al informe preliminar.

Por lo anterior la presente Observación se mantiene en las mismas condiciones establecidas en el Informe Preliminar.

Recomendaciones:

- Se recomienda evaluar y documentar el indicador de acuerdo con lo establecido en la ficha del mismo.
- Se recomienda que la información soporte de la medición del indicador sea gestionada y documentada de forma que permita su adecuada organización y preservación.

O – GT – 03 – 2021 – DOMINIO RELACION CON PROVEEDORES DEL PLAN DE IMPLEMENTACION DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.

Se evidencia que en el documento "POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION" no se describe de forma explícita y concreta los requisitos de seguridad de los proveedores de la Entidad", lo anterior de acuerdo con lo establecido en el Plan de Seguridad de la Información en la Actividad de Control "Seguridad de la información en las relaciones con los proveedores" y las tareas T74-"Detallar en la política de seguridad de la información como se asegura la protección de los activos de la entidad que sean accesibles para los proveedores" y T75- "Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores"

Derecho a la Réplica:

Mediante comunicación 2021IE0010312 del 27 de diciembre de 2021, el Grupo Interno de Trabajo TICs informó que no presenta réplica al informe preliminar.

Por lo anterior la presente Observación se mantiene en las mismas condiciones establecidas en el Informe Preliminar.

Recomendaciones

- Se recomienda actualizar el documento de "POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION" para establecer concretamente los requisitos de seguridad de la información que deben cumplir los proveedores de la entidad.
- Se recomienda que en los contratos con proveedores se establezca dentro de sus obligaciones, de forma explícita y concreta los requisitos de Seguridad de la Información que deben cumplir los proveedores, lo anterior basado en lo que se establezca en la "Política General de Seguridad de Información" del Ministerio del Deporte", con respecto a los proveedores.

O – GT – 04 – 2021 – DOCUMENTO GT-MN-006 "Manual de Operación de la Política de Backus y Restauración" EN ISOLUCION.

Se evidencia que el documento GT-MN-006 "Manual de Operación de la Política de Backus y Restauración de Información", con fecha de aprobación de del 30 de abril de 2020, perteneciente al Proceso Gestión TICs, se encuentra desactualizado. Sin embargo, el GIT TICs inicio el proceso de aprobación de la Actualización del documento el pasado 4 de octubre ante la Oficina Asesora de Planeación.

Derecho a la Réplica:

Mediante comunicación 2021IE0010312 del 27 de diciembre de 2021, el Grupo Interno de Trabajo TICs informó que no presenta réplica al informe preliminar.

Por lo anterior la presente Observación se mantiene en las mismas condiciones establecidas en el Informe Preliminar.

Recomendaciones

- Se recomienda fortalecer la gestión ante la Oficina Asesora de Planeación con el fin de asegurar que el trámite de actualización de los elementos del Sistema de Gestión, se oficialice de forma oportuna.
- Se recomienda a la OAP fortalecer la gestión con el fin de asegurar la respuesta oportuna a las solicitudes de actualización de los elementos del Sistema de Gestión por parte del Proceso Gestión TICs.

8. *HALLAZGOS Y OBSERVACIONES REPETITIVOS:*

En la presente evaluación realizada no se identificaron hallazgos u observaciones de carácter repetitivo.

9. *DESCRIPCIÓN DE LOS BENEFICIOS DE AUDITORÍA:*

En el presente ejercicio auditor, no se presentó el beneficio de auditoría.

Conclusiones:

- El proceso Gestión TICs cuenta con un plan de implementación de la Política de Seguridad Digital, el cual durante la vigencia 2021 se ha venido implementando apoyado en un equipo de trabajo especializado en el tema., adicionalmente el

Ministerio ha logrado una posición de liderazgo frente a las entidades públicas en materia de Seguridad Digital, mediante la activa participación en las actividades de la oferta institucional del Ministerio TIC.

- Lo anterior ha permitido lograr avances importantes en la implementación de la Política de Seguridad Digital, la cual es uno de los tres pilares de la Política de Gobierno Digital.
- En cuanto al elemento transversal Arquitectura de la Política de Gobierno Digital, durante la vigencia 2021 el Ministerio no logro avances.
- El proceso Gestión TICs presento debilidades en la elaboración formal de la documentación que da soporte a la medición de los indicadores del PETI de acuerdo con las fichas de estos, dicha debilidad, no permite tener información precisa para el seguimiento e identificación de desviaciones de la gestión.

10. RECOMENDACIONES GENERALES:

- Teniendo en cuenta que el Ministerio cuenta con un Plan de Seguridad de la Información, se recomienda asegurar la sostenibilidad del Sistema de Gestión de Seguridad de la Información, lo cual permita seguir avanzando en la implementación de los controles y en la sostenibilidad de los controles implementados.
- Se recomienda identificar la causa raíz por la cual el proyecto de Arquitectura Empresarial no logro avanzar en la vigencia 2021, lo anterior con el fin tomar las decisiones adecuadas y de asegurar que dicho proyecto se priorice y se cumplan con los objetivos establecidos**.**
- Se recomienda fortalecer la gestión para asegurar que la traza documental de los indicadores del Plan Estratégico de Tecnologías de la Información-PETI, se realice de acuerdo con lo establecido en las fichas correspondientes.
- Se recomienda fortalecer la gestión para asegurar que las evidencias de aplicación de los controles este acorde con lo definido en el Mapa de Riesgos del proceso.

(Memorando remisorio firmado por)

JAMES LIZARAZO BARBOSA
Jefe Oficina de Control Interno

Elaboró: José Edgar Hernando Galarza Bogota – Profesional Contratista OCI
Revisó Andrés Galvis Pineda – Profesional Especializado OCI

ANEXOS

Anexo No. 1

Definición del Control	Evidencia de la Ejecución de la Actividad de Control	DESCRIPCION DE LA EVIDENCIA DOCUMENTAL
Trimestralmente, el Coordinador TICS, debe Verificar que los funcionarios estén utilizando las herramientas dispuestas por la entidad para el intercambio de información, consultará a sus funcionarios las herramientas utilizadas para el intercambio de información y establecerá acuerdos sobre el uso de las mismas. En caso de identificar desviaciones en la ejecución del control, Se revisarán las sugerencias en el manejo de las herramientas y se renovarán los acuerdos en el uso de las mismas. De la ejecución de los controles se generará la siguiente evidencia: Acta de socialización.	Acta de socialización	No se evidencia la elaboración del "Acta de Socialización" trimestral, establecida en el Mapa de Riesgos del Proceso Gestión TICs. Como evidencia el GIT TIC reporta un informe semanal que describe estadísticamente el uso por parte de los funcionarios de la Entidad de las herramientas tecnológicas dispuesta para los mismos.
Semestralmente, el Coordinador TICS, debe Validar que los funcionarios no compartan información reservada para la entidad de acuerdo a las políticas definidas por la entidad, mediante la revisión del cumplimiento de las directrices establecidas en la política de protección de datos personales. En caso de identificar desviaciones en la ejecución del control, Realizara las sugerencias a que haya lugar para evitar que terceros no autorizados accedan a la información. De la ejecución de los controles se generará la siguiente evidencia: Informe de gestión	Informe de gestión	No se evidencia la elaboración del "Informe de Gestión" semestral, establecido en el Mapa de Riesgos del Proceso Gestión TICs. Como evidencia el GIT TIC reporta un información del inventario de activos de información, políticas de clasificación de la información

Semestralmente, el Coordinador TICS, debe Validar que el sistema de detección de amenazas para el correo está actualizado y configurado de acuerdo a las necesidades de la entidad y tendencias del mercado, liderando las pruebas necesarias y los cambios requeridos a fin de hacer ajustes a las herramientas de protección de correo. En caso de identificar desviaciones en la ejecución del control, tomará las medidas correctivas que estén al alcance a fin de corregir la situación. De la ejecución de los controles se generará la siguiente evidencia: Informe del mantenimiento	Informe del mantenimiento	No se evidencia la elaboración del "Informe de Mantenimiento" semestral establecido en el Mapa de Riesgos del Proceso Gestión TICs. Como evidencia el GIT TIC reporta tres(3) Actas de Soporte del proveedor SoftSecurity ante un incidente del producto McAfee ePO 5.10 de la entidad realizados al final del mes de octubre y durante el mes de noviembre.
Semestralmente, el Coordinador TICS, debe verificar los permisos de acceso de administrador a los sistemas de la entidad e identificar los funcionarios y contratistas que tienen la posibilidad de realizar modificaciones, verificando quiénes tienen acceso a los sistemas a cargo del grupo de trabajo. En caso de identificar desviaciones en la ejecución del control, tomará las medidas correctivas que estén a su alcance a fin de corregir la situación. De la ejecución de los controles se generará la siguiente evidencia: informe de la actividad	informe de la actividad	No se evidencia la elaboración del "Informe de Actividad" semestral establecido en el Mapa de Riesgos del Proceso Gestión TICs. Como evidencia el GIT TIC reporta el documento "SISTEMAS DE INFORMACION DEL MINISTERIO - CONTROL DE ACCESO" el cual contiene la relación de Sistemas de información y servidores con usuario administrador, sin embargo, dicho documento no relaciona otros tipo de recursos como equipos de red, software utilitario, antivirus entre otros con que cuenta la entidad y por lo tanto el control no se realiza sobre la totalidad de los recursos TIC.

Anexo No. 2.

PETI-MINDEPORTE 2020-2023 V1 25-08-2020.pdf - Adobe Acrobat Reader DC (32-bit)

Archivo Edición Ver Firmar Ventana Ayuda

Inicio Herramientas 1. Lista de chequ... 2. Declaración Ju... Plan de Segurida... POLÍTICA GENER... PETI-MINDEPOR...

25 / 45 125%

6. Análisis financiero

Anualmente, la coordinación del GIT-TIC's realiza un ejercicio de proyección de requerimientos teniendo en cuenta: los proyectos ejecutados en la vigencia correspondiente, el estado de la infraestructura tecnológica, la lista de proyectos de tecnología solicitados por las dependencias, y las necesidades en cuanto a adquisiciones y proyectos detectados internamente por la dependencia. Con base en los gastos de la vigencia y en lo estipulado en el Plan Anual de Adquisiciones se realizó una proyección del presupuesto de tecnología estimado para las vigencias del PETI:

Proyectos			Presupuesto	2020 $ 4,203 M	2021 $ 4,800 M	2022 $ 5,520 M	2023 $ 5,930 M
Iniciativas de transformación	Área Líder	ID	Nombre de proyecto	E F M A M J J A S O N D	E F M A M J J A S O N D	E F M A M J J A S O N D	E F M A M J J A S O N D
	DIRECCIÓN INSPECCIÓN, VIGILANCIA Y CONTROL.	IT-001	Implementación de software misional.		$ 200 M		
	DIRECCIÓN RECURSOS Y HERRAMIENTAS.	IT-002	Robótica y drones				
		IT-003	infraestuctura tecnologica para la certificación de laboratorio control dopaje.	$ 537 M			
		IT-004	Implementación de software misional.			$ 300 M	
	DIRECCION POSICIONAMIENTO Y LIDERAZGO	IT-005	Cloud Computing				
		IT-006	Desarrollo de software misional.				$ 300 M
	Secretaria General	IT-007	Software administrativo - SISEG				
		IT-008	Plataforma Colaborativa - Intranet Office 365				
		IT-009	Cloud Computing				
		IT-010	BlockChain				$ 200 M
		IT-011	Definición e Implementación de Arquitectura empresarial		$ 20 M		
		IT-012	Plataforma de Ciberseguridad		$ 200 M		
		IT-013	Plan de entrenamiento anual de uso y apropiacion de TI.		$ 10 M		

Bases PEI	Plan Estratégico Institucional												TERCER TRIMESTRE 2021	
Lineas del PEI - Mindeporte	Estrategia	Objetivo estrategia	Iniciativa	Eje que apoya	Área Lider Iniciativa.	Estado	Medicion	Medición Trimestral Acumulada	Avance por Trimestre				% Avance 2021	Comentarios	Año (per total)
							Por periodo actual		Primer	Segundo	Tercer	Cuarto			
			Definición e implementación de la Arquitectura empresarial.	Información		En proceso	25%	0,0%					0%	https://coldeportes.sharepoint.com/sites/gittics/Documentos%20compartidos/Forms/AllItems.aspx?RootFolder=%2Fsites%2Fgittics%2FDocumentos%20compartidos%2FARQUIT	2020-2
			Plataforma de Ciberseguridad	Servicios de Tecnologia-		En proceso	33,33%	33,3%	8,33%	8,33%	16,67%		100%	Se montaron mejoras en s	2021-2
			Plan de entrenamiento anual de uso y apropiacion de TI.	Uso y Apropiación de las TICS		En proceso	25%	18,8%	6,25%	6,25%	6,25%		75%	establecio el plan de capacitaciones anuales. Julio y Septiembre: Se inicio la propuesta del plan de uso y apropiación	2020-2
			Provisión de herramientas y apropiación de TIC para personas con discapacidad.	Estrategia e Innovación	GIT Servicio Integral al Ciudadano	En proceso	50%	37,5%	12,50%	12,50%	12,50%		75%	Requerimientos para el portal del Ministerio, enfocado a personas	2021- 2
			Aplicación Móvil	Estrategia e Innovación		En proceso	50%	37,5%	12,50%	12,50%	12,50%		75%	Se programó la adquisiciones en el PAA Julio- sept= Se esta en conversaciones con el proveddor para	2021-2