MEMORANDO

Código Dependencia

MINDEPORTE 22-06-2022 13:37
Al Contestar Cite Este No.: 2022IE0006995 Fol:1 Anex:1 FA:18
ORIGEN 110 - OFICINA DE CONTROL INTERNO / JAMES JILBERT LIZARAZO BARBOSA
DESTINO 100 - DESPACHO DEL MINISTRO / GUILLERMO HERRERA CASTAÑO
ASUNTO INFORME FINAL AI PROCESO TICS
OBS

2022IE0006995

PARA: GUILLERMO HERRERA CASTAÑO
Cargo: Ministro del Deporte

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

ASUNTO: Informe Final AI proceso TICs

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 2022, aprobado por el Comité Institucional de Coordinación de Control Interno, en sesión realizada el 28 de enero 2022, me permito presentar Informe Final de la auditoría interna al Proceso "Gestión de Tecnologías de la Información y las Comunicaciones" del Ministerio del Deporte.

Teniendo en cuenta el contenido de dicho informe y en cumplimiento de lo establecido en el Manual de Auditoría Interna EI-MN-001 y el Procedimiento de Auditoría Interna EI-PD-002 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 observación y 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 de Auditoria Proceso Gestión TICs (18 Folios)

Elaboró: José Edgar Hernando Galarza Bogotá

Revisó:
ANDRES GALVIS PINEDA
22-06-2022 12:27

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*:** 11/05/2021
Fecha de Cierre: 2/06/2022

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. Evaluar del cumplimiento de la Resolución 1519 de 2020 emitida por el MINTIC en materia de Seguridad Digital, lo anterior dentro del marco del MSPI.
3. Evaluar el estado de avance de cumplimiento del Decreto 338 de marzo del 2022 emitida por el MINTIC.

Alcance de la Auditoría: Comprende el periodo entre el 01-01-2021 al 30-04-2022, con el análisis de la información reportada por el líder del Proceso Gestión TIC o gestionada por los sistemas de información del Ministerio del Deporte.

Criterios de la Auditoría:

- Decreto Nacional No. 1078 de 2015 *"Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".* Marco de Referencia de Arquitectura V2.0, MGPTI.G.GEN.01 – Documento Maestro del Modelo de Gestión de Proyectos TI.
- Decreto 338 del 8 de marzo de 2022 *"Por el cual se adiciona el Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones"*
- Resolución 1519 del 24 de agosto de 2020 *"Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos", Anexo 3. Condiciones mínimas técnicas y de Seguridad Digital"*
- Directiva Presidencial 03 de marzo de 2021,

- Directiva Presidencial 02 de febrero de 2022,
- 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.
- Ley No. 1712 de 2014 *"Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.".*
- Ley 1967 de 2019, Por la cual se transforma el Departamento Administrativo del Deporte, la Recreación, la Actividad Física y el Aprovechamiento del Tiempo Libre (Coldeportes) en el Ministerio del Deporte.
- Decreto 1670 del 12-sep-2019, Por la cual se adopta la estructura interna del Ministerio del Deporte.
- 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, 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 N° 2359 del 03-dic/2019, "Por lo cual se establecen los grupos internos de trabajo del Ministerio del Deporte y se asignan sus funciones". Artículo 3 Funciones de los grupos internos de trabajo, GIT Tecnologías de la Información y de las Comunicaciones - TICs.
- Resolución 881 del 17-mar-2015, "Por la cual se modifica y adopta el Manual Específico de Funciones y Competencias Laborales para los empleos de Coldeportes", ahora Ministerio del Deporte.
- 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.
- PETI, Políticas de Seguridad y Privacidad de la Información, Proceso "Gestión TICS", procedimientos, formatos, riesgos, controles, entre otros.
- 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) **Rastreo**: Seguimiento de una operación, a través de la documentación respectiva, a fin de conocer y evaluar su ejecución (evidencias analíticas).

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

d) **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).

e) **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

Se aplicaron las Normas Internacionales para el Ejercicio Profesional de Auditoría, como observación, consulta de reportes, cruces, verificación, comparación y análisis de las mediciones y reportes de estado de avance del PETI, implementación de los controles de seguridad digital establecidos en la Resolución 1519 de 2020 del MINTIC y las actividades de planeación para el cumplimiento del Decreto 338 de 2022 emitida por el MINTIC.

a. Cumplimiento del Decreto 338 de 2022.

El Ministerio de la Tecnologías de la Información y las Comunicaciones emitió el decreto 338 el pasado 8 de marzo de 2022, el cual establece: “Por el cual se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto único 1078 de 2015, Reglamentario del Sector de la Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones”

Se evidencia que para el cumplimiento de dicho Decreto el GIT – TIC ha adelantado las siguientes actividades:

1. El GIT – TIC realizo un análisis preliminar del Decreto 338 en el cual se plasman las consideraciones que el Ministerio debe tener cuenta para el cumplimiento del mismo, adicionalmente en se definieron las acciones a realizar en el costo plazo. Dicho Análisis se evidencia en el documento “Estrategia de Seguridad Digital del Mindeporte en cumplimiento del Decreto 338 de marzo de 2022”. Publicado en el micro sitio de seguridad digital del Mindeporte.

Enlace: https://coldeportes.sharepoint.com/sites/IntranetInstitucional/SitePages/Seguridad-de-la-Informaci%C3%B3n.aspx

2. El Documento "Estrategia de Seguridad Digital del Mindeporte en cumplimiento del Decreto 338 de marzo de 2022". se socializó con la Secretaria General. De la actividad anterior se dejó evidencia mediante correo electrónico del 18 de abril de 2022 remitido por el Coordinador del GIT – TIC.

3. EL GIT – TIC solicito al GIT de Comunicaciones la publicación del documento "Estrategia de Seguridad Digital del Mindeporte en cumplimiento del Decreto 338 de marzo de 2022", en el Micro sitio de Seguridad de la Información, se deja como evidencia el correo electrónico del 27 de abril de 2022 remitido por el GIT-TICs.

4. EL GIT TIC participó en el evento Colombia 4.0 organizado por el MINTIC, durante los días 5, 6 y 7 de mayo durante el cual se informó por parte de la Ministra TIC, que las Resoluciones reglamentarias del Decreto se expedirán en el corto plazo y que se encuentran en proceso de articulación con los entes reguladores. Dichas resoluciones permitirán tener precisión respecto de las actividades y recursos para el cumplimiento normativo.

5. El GIT – TICs participó en mesa de trabajo virtual organizada por el MINTIC el 7 de abril en el cual el Ministerio TIC socializó el Decreto 338, se tiene como evidencia imagen citación por grupos de Whastapp del MINTIC.

6. El GIT-TICs solicito y realizó mesa de trabajo presencial con la OCI el 20 de abril con el fin trabajar de forma articulada para el cumplimiento del Decreto 338 desde el punto de vista de la gestión y del control preventivo.

De lo anterior se observa que el Ministerio ha adelantado actividades de análisis preliminar del impacto y ha establecido un plan de trabajo para el cumplimiento normativo de forma oportuna, se recomienda que dicho plan sea presentado al Comité Institucional de Gestión y Desempeño con el fin de que sea socializado y se asegure su implementación, teniendo en cuenta que dicho cumplimiento implica la implementación de nuevas actividades, procedimiento e infraestructura para el fortalecimiento de la gestión de la Seguridad Digital del Estado Colombiano.

b. Avance del PETI

El Ministerio del Deporte cuenta con el Plan Estratégico de Tecnologías de la Información y Comunicaciones-PETI 2020-2023; para la vigencia 2022 se establecieron 15 iniciativas/proyectos, la siguiente Tabla No. 1 muestra el nombre de la iniciativa/proyecto, el área líder responsable, el porcentaje planeado para la vigencia 2022 y el avance de estas correspondiente al primer trimestre de 2022.

Tabla No. 1: Incitativas/proyecto PETI 2022

Num.	Iniciativa	Eje que apoya	Área Líder Iniciativa.	Medición Por periodo actual	Medición Trimestral Acumulada	Avance Primer Trimestre	% Avance 2022
1	Implementación de software misional	Sistemas de Información	Dirección Inspección, Vigilancia y Control.	33,33%	8,3%	8,33%	**25%**
2	Actualización plataforma tecnológica	Servicios de Tecnología	GIT TIC's	25%	6,3%	6,25%	**25%**
3	Prestar servicios de apoyo técnico para la gestión del área	Servicios de Tecnología	GIT TIC's	25%	6,3%	6,25%	**25%**
4	Cloud Computing	Estrategia TI e Innovación	*Secretaria General *GIT Comunicaciones *Dirección Posicionamiento y Liderazgo Deportivo.	33,33%	8,3%	8,33%	**25%**
5	Plataforma Colaborativa - Intranet Office 365	Servicios de Tecnología	Secretaria General	25%	6,3%	6,25%	**25%**
6	Software: "Sistema de Gestión, Control y Seguimiento Administrativo" - SISEG	Sistemas de Información		25%	6,3%	6,25%	**25%**
7	Definición e implementación de la Arquitectura empresarial.	Información		25%	3,0%	3,00%	**12%**
8	Plataforma de Ciberseguridad	Servicios de Tecnología-Información		33,33%	8,3%	8,33%	**25%**
9	Plan de entrenamiento anual de uso y apropiación de TI.	Uso y Apropiación de las TICS		25%	6,3%	6,25%	**25%**
10	Provisión de herramientas y apropiación de TIC para personas con discapacidad.	Estrategia e Innovación	GIT Servicio Integral al Ciudadano	50%	12,5%	12,50%	**25%**

Num.	Iniciativa	Eje que apoya	Área Líder Iniciativa.	Medición Por periodo actual	Medición Trimestral Acumulada	Avance Primer Trimestre	% Avance 2022
11	Aplicación Móvil	Estrategia e Innovación		50%	12,5%	12,50%	**25%**
12	Servicios de internet en las sedes del Ministerio	Servicios de Tecnología	GIT TIC's	25%	6,3%	6,25%	**25%**
13	Garantizar la Operación de los Servicios del GIT TICS	Servicios de Tecnología	GIT TIC's	25%	6,3%	6,25%	**25%**
14	Mantenimiento preventivo y correctivo de la plataforma tecnológica y otros servicios	Servicios de Tecnología		25%	6,3%	6,25%	**25%**
15	Establecer la operación del servicio de evaluación de vulnerabilidades de los aplicativos e infraestructura de la entidad	Servicios de Tecnología		33,33%	8,3%	8,33%	**25%**

Fuente: “Hoja de Ruta PETI” del GIT - TIC

De acuerdo con la información reportada por el GIT-TIC, de las 15 iniciativas/proyectos las siguientes tres (3):“Implementación de software misional”, “Cloud Computing” y Software: "Sistema de Gestión, Control y Seguimiento Administrativo – SISEG”, cuentan con cronogramas de trabajo que permitan identificar las actividades detalladas a desarrollar y los tiempos planeados de las mismas, sin embargo, se observa que en dichos cronogramas no se identifica de forma explícita el avance cuantitativo de los mismos que permita validar el avance reportado en el documento “Hoja de Ruta PETI 2022” utilizado por el GIT-TICs para el control del avance del PETI. Adicional a lo anterior se observa que los cronogramas aportados no están estandarizados y cada uno utiliza un formato particular, dificultando la evaluación de los mismos.

Adicionalmente la medición del avance cuantitativo reportado en la “Hoja de Ruta PETI” para las 12 iniciativas restantes, al no contar con cronogramas detallados y formales no se tiene evidencia razonable de la consistencia de dichas mediciones. Por lo anterior no es posible identificar si la iniciativa/proyecto presenta alguna desviación positiva o negativa con respecto a la oportunidad de su ejecución.

De otra parte, las iniciativas/proyectos no cuentan con fichas de proyectos, soportes de gestión

de alcance, gestión de tiempo, gestión de recursos, gestión de calidad y en general no se aplica una metodología de gestión de proyectos formal.

EL GIT TICs estableció fichas de indicadores para el tablero de control de seguimiento al PETI, se evidencia que dichas fichas, no se están aplicando, lo anterior genera incertidumbre respecto del avance cuantitativo del PETI. EL GIT TICs informa que dichos indicadores no se han aplicado teniendo en cuenta que están en proceso de reformulación y ajuste de los mismos.

Por lo anterior se observa debilidades en la gestión formal de proyectos del PETI, especialmente en lo que se refiere a la gestión de tiempo y la gestión de alcance, situación que incrementa la probabilidad del riesgo de incumplimiento y/o inoportunidad en la ejecución de las iniciativas/proyectos establecidos.

La gestión del tiempo, alcance, calidad entre otros son elementos de control fundamentales, en la gestión de proyectos los cuales permiten tener elementos de control para la gestión y seguimiento los mismos, lo anterior según los establecido en el Lineamiento *"7.2.2. MGPTI.LI.PLA.02 - Gestión de proyectos con componentes de TI. La Oficina de Gestión de Proyectos junto con la dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, debe liderar todas las iniciativas y proyectos de TI de la entidad, utilizando una metodología formal de gestión de proyectos que incorpore el uso de lecciones aprendidas y un esquema de gestión de cambios.",* y demás lineamientos complementarios del "MGPTI.G.GEN.01 – Documento Maestro del Modelo de Gestión de Proyectos TI" de la Política de Gobierno Digital.

c. Resolución 1519 de 2020 del MINTIC, anexo 3 Seguridad Digital

El Ministerio de la Tecnologías de la Información y las Comunicaciones emitió la Resolución 1519 el 24 de agosto de 2020, el cual establece: *"Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información, accesibilidad web, seguridad digital, y datos abiertos",* en su artículo *"6. Condiciones mínimas técnicas y de seguridad digital"* establece que *"Los sujetos obligados deberán observar las condiciones mínimas técnicas y de seguridad digital que se definen en el Anexo 3 de la presente resolución"*

Las condiciones mínimas técnicas y de Seguridad Digital del anexo 3 se muestran en la siguiente tabla No 2.

Tabla No. 2: Condiciones mínimas técnicas y de Seguridad Digital - anexo 3 de la Resolución 1519 de 2020

ITEM	REQUISITO
1	Implementar controles de seguridad durante todo el ciclo de vida del desarrollo de software.
2	Implementar o exigir controles de seguridad relacionados con el control de la autenticación, definición de roles y privilegios y separación de funciones

ITEM	REQUISITO
3	Exigir medidas de seguridad al proveedor del hosting (políticas de seguridad robustas y un nivel de madurez en seguridad optimizado).
4	Aplicar mecanismos de *hardening* para eliminar configuraciones y credenciales por defecto, además de deshabilitar métodos *HTTP* peligrosos como *put, delete, trace* y restringir en lo posible la administración remota.
5	Proteger la integridad del código, mediante: (i) la validación exhaustiva de: *inputs*, variables *post y get* (no enviar parámetros sensibles a través del método *get*), Cookies (habilitar atributos de seguridad como *Secure y HttpOnly*), y, cabeceras *HTTP*; (ii) la sanitización de los parámetros de entrada: es decir, que cuando se reciba la información de dichas variables se eliminen etiquetas, saltos de línea, espacios en blanco y otros caracteres especiales que comúnmente conforman un script, además de la restricción de formatos y tamaños de subidas de archivos; (iii) la sanitización y escape de variables en el código; (iv) verificación estándar de las Políticas de Origen de las cabeceras; y (v) la verificación y comprobación del token de CSRF (cuando aplique).
6	Ejecutar monitoreos de seguridad sobre las páginas web que contemple, entre otras, las siguientes acciones: escaneo de archivos infectados, escaneo de vulnerabilidades, análisis de patrones para detectar acciones sospechosas, verificación contra listas negras, monitoreo del tráfico para detectar ataques de denegación de servicios.
7	Exigir mecanismos de autenticación dentro de los sitios web a través de la creación de contraseñas fuertes y solicitar renovaciones periódicas de las mismas garantizando la accesibilidad de persona con discapacidad.
8	Mantener actualizado el software, *frameworks y plugins* de los sitios web.
9	Restringir el uso de *login* contra ataques de fuerza bruta, implementando, entre otros: mecanismos de *captcha* accesibles o auto detectable, y/o limitar la tasa de intentos de *login.*
10	Ocultar y restringir páginas de acceso administrativo.
11	Restringir la escritura de archivos desde la web a través de la asignación de permisos de solo lectura.
12	Crear copias de respaldo.
13	Almacenar trazas o logs de auditoría de los eventos de seguridad, logins, entre otros.
14	Garantizar conexiones seguras a través de uso de certificados, *SSL (HTTPS* para la confianza de usuarios) y cifrado en la estructura de las peticiones para portales transaccionales, para evitar la manipulación de parámetros en las peticiones. (adicional al cifrado *SSL*), También deben habilitar las cabeceras de seguridad, entre otras las siguientes: *Content-Security-Policy (CSP), X-Content-Type-Options, X-Frame-Options, X-XSS-Protection, StrictTransport-Security (HSTS), Public-Key-Pins (HPKP) Referrer-Policy, FeaturePolicy.*
15	Implementar mensajes genéricos de error, que no revelen información acerca de la tecnología usada, excepciones o parámetros que dispararon el error específico, los cuales deberán ser comprensibles por parte de las personas, incluyendo la accesibilidad para las personas con discapacidad.
16	Proteger el binario de la aplicación, a través de métodos de ofuscación que impidan realizar procedimientos de ingeniería inversa (*reversing*) para analizar la lógica de la aplicación.
17	Sanitización de parámetros de entrada mediante la eliminación de etiquetas, saltos de línea, espacios en blanco y otros caracteres especiales que comúnmente conforman un «script», además de la restricción de formatos y tamaños para subida de archivos.

ITEM	REQUISITO
18	Sanitización de caracteres especiales (secuencia de Escape de variables en el código de Programación)
19	Revisar las recomendaciones de seguridad en la guía de desarrollo seguro de aplicaciones y Servicios Web Seguros de la *Open Web Application Security Project* (OWASP).
20	Implementar en los servidores los controles necesarios (hardware o software) de protección de acceso y de ataques como Cross-site scripting, SQL injection o Denial-of-service, entre otros.
21	Incorporar validación de formularios tanto del lado del cliente como del lado del servidor.
22	Implementar monitoréos de seguridad sobre la plataforma tecnológica que hace parte del sitio web (escaneo de vulnerabilidades, escaneo de archivos infectados, análisis de patrones para detectar acciones sospechosas, verificación contra listas negras, monitoreo del tráfico para detectar ataques de denegación de servicios) y realizar las acciones de mitigación correspondientes.
23	Establecer los planes de contingencia, DRP y BCP, que permita garantizar la continuidad de la sede electrónica o del sitio web 7/24 los 365 días del año.
24	Restringir la escritura de archivos en el servidor web a través de la asignación de permisos de roles y los privilegios asociados.
25	Implementar sistemas antivirus en el servidor web, para garantizar medidas contra infecciones de malware a los archivos del mismo.
26	Controlar el escalamiento de privilegios en los Sistemas Operativos, servidor web y Bases de datos que hacen parte de la infraestructura del portal web.

Fuente: Resolución 1510 de 2020 Anexo 3

Tanto la plataforma de software como de Hardware que soporta la sede electrónica del Ministerio del Deporte cuyo dominio es www.mindeporte.gov,co están tercerizados. La plataforma de software esta implementada en una herramienta propietaria de la firma Micrositios SAS y la plataforma de Hardware se tiene contratado el servicio de AWS a través del contrato con TIGO UNE.

Por lo anterior la gran mayoría de requisitos exigidos en el anexo 3 de la Resolución 1519 de 2020, son implementados por dichos proveedores, sin embargo, caber aclarar que la responsabilidad de exigir y verificar dicha implementación es de la Entidad.

Se observa que el contrato CPS-734-2022 subscrito con el proveedor Micrositios SAS cuyo objeto es "MANTENIMIENTO, ACTUALIZACIÓN Y DESARROLLO DEL PORTAL DEL MINISTERIO Y SUBSITIOS"., en su cláusula 6- Obligaciones a cago del Contratista en el numeral 4 de la obligaciones específicas establece: *"Seguir en el trabajo de Incorporación dentro del portal y sus subsitios como compromiso del año 2022 las directrices de accesibilidad (limitación ciegos en trabajo conjunto con el INCI) como ya se mencionó con base en la resolución 1519 de 2020, en la ley 2052 de 2020-Articulo 30 y en la Norma Técnica NTC 5854 de Mintic, con el propósito de llegar a nivel AAA con puntos de verificación de prioridad 1,2,3 de las "pautas de accesibilidad para contenidos web*". , sin embargo, no se tiene establecido contractualmente la obligación especifica de la implementación de las condiciones mínimas técnicas y de seguridad digital establecidos en el anexo 3 de dicha Resolución.

Se evidencia que 3 de las 26 condiciones mínimas técnicas y de seguridad digital no aplican para la sede electrónica del ministerio, teniendo en cuenta que: la sede electrónica no tiene implementados tramites y/o servicios en línea que requieran login, la plataforma tecnológica no lo requiere y la sede electrónica no implementa formularios.

La información aportada para cada uno de los requisitos de seguridad digital, permite evidenciar que se tienen avances en la implementación de dichos controles por parte de los proveedores del servicio de hosting y soporte y mantenimiento de la plataforma que soporta la sede electrónica, el detalle técnico de dicha implementación no se describe en el presente informe teniendo en cuenta que dicha información es sensible y puede ser utilizada para realizar ataques de tipo informático.

Se recomienda que se realice la verificación por parte de los supervisores de dicho contrato de la implementación de las condiciones mínimas técnicas y de seguridad digital y se deje evidencia de la misma, de otra parte, teniendo en cuenta la dinámica tecnológica y evolución de la sede electrónica es necesario realizar la revisión y actualización de la implementación de algunos de las condiciones técnicas mínimas y de seguridad digital de forma periódica.

4. RIESGOS CUBIERTOS EN LA AUDITORÍA

Se evidencia que el Mapa de Riesgos del proceso Gestión TIC se actualizo para la vigencia 2022, el nuevo mapa de riesgos se publicó en la plataforma Isolucion con el seguimiento por parte del proceso a corte del primer cuatrimestre (enlace isolución: https://sig.mindeporte.gov.co/Isolucion/Administracion/frmFrameSet.aspx?Ruta=fi9CYW5jb0Nvbm9jaW1pZW50bzRDb2xkZXBvcnRlcy8wLzA3MmI1Njg1ZjRjZDRhNDU5NzAzNTUwMmIyZTI2N2ZlLzA3MmI1Njg1ZjRjZDRhNDU5NzAzNTUwMmIyZTI2N2ZlLmFzcA==&debug=yes).

La siguiente tabla No. 3 relaciona los riesgos de gestión y seguridad de información con sus respectivos controles:

Tabla No. 3: Riesgos y Controles Mapa de Riesgos del Proceso Gestión TICs

CONTROL	DESCRIPCIÓN CONTROL	RIESGO	TIPOLOGÍA	EVIDENCIA DE APLICACIÓN
R2-Con-1	Cada vez que se requiera, el Coordinador TICS, debe verificar la correcta funcionalidad y disponibilidad de equipos de centro de cómputo, mediante los mantenimientos preventivos a los equipos. En caso de identificar desviaciones en la ejecución del control, Se debe realizar mantenimiento correctivo de equipos de centro de cómputo con registro en el formato GT-FR-011 Bitácora registro servidores. De la ejecución de los controles se generará la siguiente evidencia: Informe del mantenimiento.	Posibilidad de afectación económica y reputacional por perdida de información e indisponibilidad de canales y servicios. (Correo, servidores, aplicaciones etc), debido a fallas en la plataforma tecnológica.	Gestión	A la fecha no se ha generado el informe de mantenimientos preventivos a los equipos.

R2-Con-2	Anualmente, el Coordinador TICS, debe Verificar la vida útil de los equipos tecnológicos, Mediante el análisis del estado del inventario de los equipos tecnológicos. En caso de identificar desviaciones en la ejecución del control, se debe determinar si se adquiere o repotencia el equipo que haya superado su vida útil. De la ejecución de los controles se generará la siguiente evidencia: Documento de inventario analizado.			Se evidencia la aplicación del Control dejando como evidencia un inventario de equipos analizado, sin embargo, no se observa la información que registre la vida útil de los equipos.
R2-Con-3	Mensualmente, el Coordinador TICS o el supervisor del contrato asignado, debe revisar el cumplimiento de los ANS en la atención de casos por parte de: Mesa de Ayuda, Conectividad, Nube Pública, GESDOC, SARA, Portal Web, revisando que las solicitudes se hayan atendido dentro de los tiempos acordados. En caso de identificar desviaciones en la ejecución del control, se analizan las inconformidades e incumplimientos y se informan al proveedor del contrato y se toman las medidas correspondientes a cada caso. De la ejecución de los controles se generará la siguiente evidencia: Informe del proveedor.			No se evidencia que se haya aplicado el control con frecuencia mensual con información que permita identificar el cumplimiento de los ANS para el servicio de mesa de ayuda, Conectividad, Nube Pública, GesDOC, SARA, Portal Web
R2-Con-4	Trimestralmente, el Coordinador TICS o el supervisor del contrato asignado, solicitará al encargado de infraestructura el detalle de servicio de los canales de comunicación hacia internet y MPLS entre sedes, mediante reporte de la plataforma Entuity, para revisar el cumplimiento de los ANS acordados en el contrato de servicios. En caso de identificar desviaciones en la ejecución del control, se procederá inmediatamente a abrir un ticket con el proveedor para la resolución de la incidencia. De la ejecución de los controles se generará la siguiente evidencia: Reporte ANS, Ancho de Banda por canal contratado. El presente control es transversal a los Riesgos de gestión y/o de Seguridad de la información.			Se evidencia la aplicación y se deja como registro del reporte de ANS correspondiente. .
R3-Con-1	Cada vez que se requiera el Coordinador TICS o su delegado, mediante controles automáticos de la plataforma de ciberseguridad de la entidad (Antispam en la Nube, SIEM, UTM, Consola Antivirus-DLP) monitorea la contención efectiva de los ataques internos y externos con el fin de prevenir la extracción de información y datos personales. En caso de identificar desviaciones en la ejecución del control, se procederá manualmente a realizar contención del ataque. Se generará la siguiente evidencia: Reportes de actividades de la plataforma de ciberseguridad de la entidad (Antispam en la Nube, SIEM, UTM, Consola Antivirus-DLP).	Posibilidad de pérdida de confidencialidad de los datos personales contenidos en las plataformas tecnológicas de la entidad, que sean susceptibles de ser utilizados, comercializados o modificados por terceros .	Seguridad de la Información	Se evidencia la aplicación del control motivado por la jornada electoral del 13 de marzo de 2022, dejando como evidencia: Informe PMU Cibernético, informe de actividades de las plataformas: SOPHOS AntiSpam, FireWall Av 68, FireWall CAR, SIEM, Sistema de Detección de Ataques-DOS.
R3-Con-2	Cada vez que se requiera el Coordinador TICS o su delegado, reportará los incidentes de Seguridad de la Información en la Bitácora de Incidentes clasificándolo de acuerdo a la incidencia presentada, con el fin de intervenir y solucionar cada caso en específico. En caso de identificar desviaciones en la ejecución del control, se solicitará al primer respondiente del incidente que de manera extemporánea lo documente al líder de Seguridad de la Información. Se generará la siguiente evidencia: Bitácora de incidentes.		Seguridad de la Información y	Se evidencia la aplicación del Control dejando como evidencia la Bitácora de Incidentes 2022, donde se puede observar que no se presentaron eventos ni incidentes en el periodo.

R3-Con-3	Semestralmente el delegado del GIT- TICs para la ciberseguridad con el experto de infraestructura, deben realizar seguimiento en el sistema de protección perimetral y los permisos de acceso a las bases de datos se encuentren actualizados y configurados correctamente. En caso de identificar desviaciones en la ejecución del control, el Coordinador del GIT- TICs dará la instrucción de generar el mantenimiento inmediatamente. Se generará la siguiente evidencia: Informe del mantenimiento de las Bases de Datos.		Seguridad de la Información	Para el periodo no se requirió aplicación del control
R3-Con-4	Cada vez que se requiera el Coordinador TICS o su delegado, realizará capacitaciones y/o socializaciones a todos los colaboradores de la entidad en las buenas prácticas de manejo de información digital y en el cumplimiento de las normas internas relacionadas para mantenerlo actualizados y sensibilizados. En caso de identificar desviaciones en la ejecución del control, se programarán de manera prioritaria estas capacitaciones y/o socializaciones. Se generará la siguiente evidencia: NOTIC´s, listados de asistencia y divulgación de información mediante el Micrositio Seguridad de la Información.		Seguridad de la Información	Se evidencia la aplicación del Control dejando como evidencia la elaboración del informativo NOTICS para los meses de febrero, marzo abril
R4-Con-1	Cada vez que se requiera el Coordinador TICS o su delegado, asegurará todas las comunicaciones externas a través de protocolos que permitan mantener la integridad de los datos en su tránsito, a través de VPN (Virtual Private Network o Red Privada Virtual) y SSL (Secure Sockets Layer o Seguridad de la Capa de Transporte). En caso de identificar desviaciones en la ejecución del control, se debe cerrar cualquier posibilidad de comunicación no segura identificada y se debe registrar en la bitácora como un incidente de Seguridad de la Información para darle el tratamiento y remediación correspondiente. Se generará la siguiente evidencia: Bitácora de Incidentes de Seguridad de la Información.	Posibilidad de modificaciones no autorizadas a los datos contenidos en las plataformas tecnológicas de la entidad afectando la integridad de los mismos.	Seguridad de la Información	Se evidencia la aplicación del Control dejando como evidencia la Bitácora de Incidentes 2022, donde se puede observar que no se presentaron eventos ni incidentes en el periodo.
R4-Con-2	Cuatrimestralmente, el Coordinador Cada vez que se requiera el Coordinador TICS o su delegado, realizará seguimiento a los procesos de mantenimiento de infraestructura y aplicativos. En caso de identificar desviaciones en la ejecución del control, El Coordinador TICs solicitará realizar el mantenimiento de manera inmediata. Se generará la siguiente evidencia: Formato cronograma mantenimiento preventivo (código Isolución: GT-FR-010) y Formato mantenimiento preventivo y correctivo (código Isolución: GT-FR-003).		Seguridad de la Información	No se evidencia la aplicación del control mediante la elaboración de los Formatos GT-FR-010 y GT-Fr-003... Se aporta un informe estadística de casos el cual no es consistente con lo establecido en el control como evidencia de aplicación del control
R4-Con-3	Cada vez que se requiera el Coordinador TICS o su delegado, realizará solicitud a los líderes Técnicos, Funcionales, Proveedores o al que se requiera para ejecutar las actividades de Hacking Ético y pruebas de vulnerabilidad a los sistemas de información susceptibles de realizarse. En caso de identificar desviaciones en la ejecución del control, el Coordinador TICs solicitará realizar la actividad inmediatamente. Se generará la siguiente evidencia: Informe de Análisis y recomendaciones para mitigación del riesgo.		Seguridad de la Información	Se evidencia la aplicación del control mediante la elaboración de informe de análisis y recomendaciones del sistema SISEG, en el cual se identificaron algunas vulnerabilidades

R4-Con-4	Anualmente el Coordinador TICS o su delegado, durante el primer trimestre se realizará solicitud de la matriz de roles y perfiles de los usuarios de la entidad, a la mesa de ayuda o al experto en infraestructura para verificación de cumplimiento en los permisos de acceso de acuerdo a la Política General de Seguridad de la Información. En caso de identificar desviaciones en la ejecución del control, el Coordinador TICs solicitará el bloqueo, desactivación o eliminación inmediata del usuario, rol o perfil que no deba estar activo y se registrará en la Bitácora de Incidentes de Seguridad de la Información. Se generará la siguiente evidencia: Matriz general de roles y perfiles y Bitácora de Incidentes de Seguridad de la Información.		Seguridad de la Información	Se evidencia la aplicación del control mediante la elaboración de la matriz general de roles y perfiles con corte a enero de 2022 y la Bitácora de Incidentes de Seguridad de la Información

Fuente: Isolucion- Listado Temático GT-DI-019 Mapa de Riesgos GT Primer Monitoreo 2022

5. FORTALEZAS

1. Se evidencia que el Ministerio del Deporte con el Liderazgo de El GIT TIC's de la Secretaría General, implementaron para las jornadas electorales del 2022 la estrategia de establecer un Puesto de Mando Unificado - PMU, cuyo objetivo es el de mitigar los riesgos de indisponibilidad, integridad y confidencialidad de la información.

Dicho PMU estableció los siguientes controles:

- Focalizar el riesgo a las plataformas que presentan mayor resiliencia ante ataques.
- Monitoreo permanente de toda la actividad cibernética asociada a la entidad desde el 25 de mayo hasta el día 30 inclusive.
- Tener copias de seguridad que permitan un restablecimiento del estado del arte de la semana previa.
- Mantener comunicación permanente con COLCET, CSIRT y Cibercomando conjunto para detección rápida y mitigación de incidentes.
- Mantener la operación de todas las plataformas de atención como muestra de madurez tecnológica de la Entidad.
- Mantener informados a Despacho del Ministro y Secretaria General en todo momento de las novedades que se presenten en la materia.

Se destaca como fortaleza del proceso Gestión TICs la implementación de dicho PMU, como elemento de control preventivo ý correctivo que fortalece la gestión de la Seguridad Digital y por lo tanto de la Política de Gobierno Digital.

2. El GIT-TIC definió de forma oportuna la estrategia para de cumplimiento del Decreto 338 de marzo de 2022, la cual fue documentada. La estrategia definida derivó de un análisis para determinar las consideraciones y acciones a desarrollar en el corto plazo.

6. RESUMEN DE HALLAZGOS Y OBSERVACIONES

Código	Título	Observación
H – GT – 01 – 2022	H – GT– 01 – 2022 : GESTIÒN FORMAL DE LOS PROYECTOS DE TI DEL PETI	Se Mantiene
O – GT – 02 - 2022	O – GT – 02- 2022: CUMPLIMIENTO DE LA RESOLUCION 1519 DE 2020 DEL MINTIC	Se Mantiene

7. DESCRIPCIÓN DE LOS HALLAZGOS Y OBSERVACIONES

HALLAZGOS:

H – GT– 01 – 2022 – *GESTIÓN FORMAL DE PROYECTOS DE TI DEL PETI*

Condición:

El 100% de las iniciativas/proyectos establecidos para el 2022 no cuentan con documentación formal que evidencie la aplicación de una metodología formal de gestión de proyectos. Lo anterior se evidencia en lo siguiente:

- No se cuenta con fichas de proyectos formales donde se establezca el objetivo y alcance de los mismos
- Tres de las iniciativas/proyectos cuentan con cronogramas, sin embargo, dichos cronogramas no son estándar y no están evaluados al corte abril 2022,
- La medición cuantitativa de avance del documento “Hoja de Ruta PETI” no es consistente con las fichas de indicadores establecidas,
- No se cuenta con evidencias de gestión de alcance, gestión de tiempo, gestión de calidad, gestión de riesgos de la cada iniciativa/proyecto establecidos en el PETI.
- El procedimiento GT-PD-017 PROYECTOS ESPECIALES DE TECNOLOGIA dentro de su alcance y actividades no contempla actividades para la gestión formal de proyectos.

Criterios:

Elemento Transversal Arquitectura de la Política de Gobierno Digital que establece el MGPTI.G.GEN.01 – Documento Maestro del Modelo de Gestión de Proyectos TI del Marco de Referencia de Arquitectura TI v2. Que indica en el lineamiento *“7.2.2. MGPTI.LI.PLA.02 - Gestión de proyectos con componentes de TI. La Oficina de Gestión de Proyectos junto con la dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, debe liderar todas las iniciativas y proyectos de TI de la entidad, utilizando una metodología formal de gestión de proyectos que incorpore el uso de lecciones aprendidas y un esquema de gestión de cambios.”*

Posible Causa identificada por la Oficina de Control Interno:

- Posibles debilidades en la implementación de la Política de Gobierno Digital
- Posibles debilidades en la planeación y seguimiento de los proyectos del PETI.
- Posibles debilidades en la aplicación del mapa de control y fichas de indicadores de los proyectos de TI establecidos por el proceso de Gestión TICs.

Descripción del Riesgo:

Lo evidenciado en la auditoria se relaciona con el Riesgo No. 3 de gestión *"Posibilidad de afectación reputacional por la falta de implementación del MIPG debido a la falta de seguimiento y mantenimiento del mismo."*, incluido en el mapa de Riesgo del proceso "Direccionamiento Estratégico y Aprendizaje Organizacional"; Del cual se evidencia posible materialización de la causa inmediata *"Falta de Implementación de MIPG"* o la causa Raíz *"Falta de seguimiento y mantenimiento del mismo. "*

Así mismo, se evidencia debilidad en la ejecución del Control No. 2 del Riesgo No 3:

> *"Cada vez que se requiera, el Profesional designado del GIT de Planeación y Gestión, debe realizar seguimiento a las actividades programadas, a través del seguimiento 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 notificar al responsable de la actividad el incumplimiento del tiempo del desarrollo de la actividad. De la ejecución de los controles se generará la siguiente evidencia: Seguimiento Plan de Trabajo".*

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 incumplimiento normativo
- 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.
- Posible afectación en la gestión y desempeño de la Entidad
- Posible afectación a la imagen de la Entidad

Réplica recibida del responsable de la unidad auditable:

Una vez cumplido el plazo para la presentación de la Réplica, el proceso Gestión de Tecnologías de la Información y las Comunicaciones no se pronunció al respecto con relación al presente Hallazgo.

Respuesta de la Oficina de Control Interno:

Debido a que el proceso "Gestión de Tecnologías de la Información y las Comunicaciones" no presentó réplica que desvirtuara lo evidenciado en el procedimiento de auditoría, el presente Hallazgo se mantiene en las mismas condiciones descritas en el Informe preliminar.

Recomendaciones Específicas.

- Se recomienda fortalecer la gestión de proyectos de TI de acuerdo con la normatividad vigente.
- Se recomienda definir, formalizar e implementar y una metodología de gestión de proyectos formal que contemple al menos la gestión de tiempo, la gestión de alcance, la gestión de la calidad, y la gestión de riesgos.
- Se recomienda revisar, actualizar y aplicar los indicadores del tablero de control del PETI.
- Se recomienda revisar, actualizar y lograr aprobación del PETI en el Comité Institucional de Gestión y desempeño, a la vez que presentar informe de avance al mismo de forma periódica.

OBSERVACION:

O – GT – 02- 2022: CUMPLIMIENTO DE LA RESOLUCION 1519 DE 2020 DEL MINTIC

Se evidencia que el Ministerio del Deporte no cuenta con registro documental en la que se haya definido el alcance a desarrollar para cada una de las condiciones técnicas mínimas y de seguridad digital de acuerdo con las particularidades de la plataforma tecnológica de la entidad que soporta la sede electrónica, en cumplimiento del Anexo 3 de la Resolución 1519 de 2020 del MINTIC.

Lo anterior genera incertidumbre respecto del nivel de cumplimiento normativo ya que el contrato de soporte y mantenimiento para la página web de la entidad no especifica de forma explícita la obligación del proveedor de implementar las condiciones mínimas técnicas y de seguridad digital establecidas en el Anexo 3 de dicha resolución.

Réplica recibida del responsable de la unidad auditable:

Una vez cumplido el plazo para la presentación de la Réplica, el proceso Gestión de Tecnologías de la Información y las Comunicaciones no se pronunció al respecto con relación a la presente Observación.

Respuesta de la Oficina de Control Interno:

Debdo a que el proceso “Gestión de Tecnologías de la Información y las Comunicaciones” no presentó réplica que desvirtuara lo evidenciado en el procedimiento de auditoría, la presente Observación se mantiene en las mismas condiciones descritas en el Informe preliminar.

Recomendaciones Específicas.

- Se recomienda definir y documentar el alcance específico para el cumplimiento de las condiciones mínimas técnicas de Seguridad Digital del anexo 3 de la Resolución 1519 de 2020 del MINTIC, de acuerdo con las particularidades especificas técnicas y de gestión de la plataforma que soporta la sede electrónica y demás aplicaciones web del Ministerio.
- Se recomienda establecer la brecha de implementación de las condiciones mínimas técnicas de Segundad Digital para la sede electrónica y demás aplicaciones web que soportan la gestión de información del ministerio.
- Se recomienda realizar un cronograma de implementación de las condiciones mínimas técnicas de seguridad digital para la sede electrónica y demás aplicaciones web que soportan la gestión de información del ministerio. Lo anterior teniendo en cuenta lo definido en los puntos precedentes.

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 la presente evaluación realizada no se identificaron Beneficios de Auditoria.

10. RECOMENDACIONES GENERALES:

- Atendiendo que el Ministerio cuenta con un Plan General para el Cumplimiento del Decreto 338 de 2022 del MINTIC, se recomienda su presentación y aprobación ante el Comité Institucional de Gestión y Desempeño, lo anterior teniendo en cuenta su impacto y compromiso de recursos que se requieren.

- Se recomienda establecer la brecha y plan de acción para la implementación las condiciones mínimas técnicas de Seguridad Digital para la sede electrónica y demás aplicaciones web que usa el Ministerio.

- Se recomienda revisar, actualizar el PETI y aplicar una metodología formal para la gestión de proyectos del mismo, lo anterior permitirá fortalecer la gestión y seguimiento e identificar desviaciones en la ejecución de los proyectos establecidos.

- 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.

CONCLUSIONES

- El proceso Gestión TICs cuenta con un plan general para el cumplimiento del Decreto 338 de marzo de 2022 del MINTIC. Sin embargo, es importante que dicho plan sea socializado y aprobado por el Comité Institucional de Gestión y Desempeño.

- EL Misterio del Deporte presenta debilidades en la definición, implementación y aplicación de una metodología de gestión de proyectos de TI formal, de acuerdo con lo establecido en la Política de Gobierno Digital.

- Los indicadores definidos por el Proceso para el control y seguimiento de la gestión del PETI no se aplican de acuerdo con los establecido.

- El proceso Gestión TICs presenta debilidades en la elaboración formal de la documentación de alcance de la implementación de las condiciones mínimas técnicas de Seguridad Digital para el cumplimiento del anexo 3 de la Resolución 1519 de 2020 del MINTIC, de acuerdo con las particularidades específicas de la plataforma tecnológica específica y de gestión que usa del Ministerio

(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