MEMORANDO

Código Dependencia

MINDEPORTE 17-05-2022 10:47
Al Contestar Cite Este No.: 2022IE0004853 Fol:2 Anex:1 FA:19
ORIGEN 110-OFICINA DE CONTROL INTERNO / JAMES JILBERT LIZARAZO BARBOSA
DESTINO 100-DESPACHO DEL MINISTRO / GUILLERMO HERRERA CASTAÑO
ASUNTO INFORME FINAL SEGUIMIENTO A LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN, A
OBS

2022IE0004853

PARA: GUILLERMO HERRERA CASTAÑO
Cargo: Ministro del Deporte

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

ASUNTO: Informe Final Seguimiento a los Riesgos de Seguridad de la Información, a los Planes de Mejoramiento AIG, y a los Indicadores del Proceso Gestión TICs.

Respetado Señor Ministro.

Atendiendo el rol de evaluación y seguimiento, estipulado en Decreto Nacional No. 0648/2017, artículo 2.2.21.4.9 Informes, literal k) los demás que establezca la Ley, y en cumplimiento de los requerimientos normativos en materia de Gestión TICs contemplado en el Plan Anual de Auditoría Interno – PAAI, aprobado por el Comité Institucional de Coordinación de Control Interno vigencia 2022, la Oficina de Control Interno remite el Informe Final “Seguimiento a los Riesgos de Seguridad de la Información, a los Planes de Mejoramiento AIG, y a los Indicadores del Proceso "Gestión TICs”.

En el informe se presentan Observaciones para la mejora del proceso con el fin de dar cumplimiento a la normatividad, así mismo, teniendo en cuenta el contenido del presente informe y en cumplimiento de lo establecido en el procedimiento Informe de Seguimiento Normativo, se sugiere la aplicación de las recomendaciones en cumplimiento de los procesos, solicitando la elaboración del Plan de Mejoramiento, en el módulo Mejora de la Plataforma ISOLUCIÓN, a más tardar a los cinco (5) días hábiles a partir del recibo del informe final, igualmente se hace saber que el plazo máximo para el cierre de la observación es de tres (3) meses.

COMITÉ INSTITUCIONAL DE COORDINACIÓN DE CONTROL INTERNO

Dando cumplimiento a lo señalado en el Decreto Nacional No. 0648 de 2017 - Artículo 16, Parágrafo 1 y Resolución Interna No. 001122 de 2017, ARTÍCULO TERCERO, literal a), se remite para conocimiento de los miembros integrantes del Comité Institucional de Coordinación de Control Interno, copia del presente informe de seguimiento en cumplimiento de requerimientos normativos.

Cordialmente,

JAMES JILBERT LIZARAZO BARBOSA
Cargo: Jefe Oficina de Control Interno

Anexos: Informe Final "Seguimiento a los Riesgos de Seguridad de la Información, a los Planes de Mejoramiento AIG, y a los Indicadores del Proceso "Gestión TICs".

Elaboró: José Edgar Hernando Galarza Bogotá

Revisó:
ANDRES GALVIS PINEDA
17-05-2022 10:04

1. DESCRIPCIÓN DEL SEGUIMIENTO

Tipo de Informe: Final

Denominación del Trabajo: Seguimiento a los Riesgos de Seguridad de la Información, a los Planes de Mejoramiento AIG, y a los Indicadores del Proceso "Gestión TICs".

Objetivo(s):

- Verificar el cumplimiento de la normatividad externa e interna aplicable a la medición de los indicadores del proceso Gestión TICs.
- Realizar seguimiento al diseño de los controles y a la implementación de los Planes de Manejo de los Riesgos asociados al Proceso de Gestión TICs.
- Evaluar los indicadores del proceso Gestión TIC.
- Evaluar la eficacia de las acciones de mejora producto de las Auditorías Internas y Seguimientos Normativos realizados y bajo la responsabilidad del proceso Gestión TIC.

Alcance:

Comprende el periodo comprendido entre el entre el 01-01-2022 al 30-03-2022 con el análisis de la información reportada por el Proceso Gestión TIC o gestionada por los sistemas de información del Ministerio del Deporte.

Marco Normativo:

- Decreto Nacional No. 1499 de 2017 “CAPÍTULO 3 “MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN, dimensión 7 control interno, componente Actividades de monitoreo “
- Manual Operativo del Sistema de Planeación y Gestión V3 diciembre de 2019. Política de Control Interno.
- Procedimientos “Auditorías Internas” EI-PD-002, “Procedimiento Informe de Seguimiento Normativo” EI-PD-001 y “Gestión de Planes de Mejoramiento Seguimiento Normativo y Auditoria Interna” EI-PD-004 del proceso “Evaluación Independiente y Mejora Continua”
- Ley No. 1474 de 2011, Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública *“Artículo 74. Plan de acción de las entidades públicas”.*
- Decreto Nacional No. 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública Articulo 2.2.21.3.4 literal d. *“La Oficina de Control Interno o quien haga sus veces: Evalúa el proceso de planeación, en toda su extensión; implica, entre otras cosas y con base en los resultados obtenidos en la aplicación de los indicadores definidos, un análisis objetivo de aquellas variables y/o factores que se consideren influyentes en los resultados logrados o en el desvío de los avances. La identificación de estas variables, su comportamiento y su respectivo análisis permite que la formulación de las recomendaciones de ajuste o mejoramiento al proceso se realice*

sobre soportes y criterios válidos y visibles fortaleciendo así la función asesora de estas oficinas".

- Decreto Nacional No. 1670 de 2019 "Por el cual se adopta la estructura interna del Ministerio del Deporte" Artículos 5 y 17.
- 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*.
- Guía para la construcción y análisis de indicadores de gestión del Departamento Administrativo de la Función Pública, versión 4 de mayo de 2018.
- Procedimiento Formulación, Actualización y Medición de Indicadores DE-PD-006 versión 1 aprobado el 6 de febrero de 2022.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5 de diciembre de 2020.
- Política de Administración del Riesgo Mindeporte DE-PO-001, versión 1 del 1 de diciembre de 2021.
- Procedimiento Administración de Riesgos GO-PD-011, versión 1 del 4 de marzo de 2021.
- Manual Operativo Sistema de Gestión Modelo Integrado de Planeación y Gestión - MIPG, versión 4 de marzo de 2021.
- Caracterización Proceso "Gestión TICS", procedimientos, formatos, mapas de riesgos del proceso Gestión TIC.
- Planes de mejoramiento del proceso Gestión TIC registrados en el sistema de información Isolucion.
- Medición de indicadores proceso Gestión TIC registrados en el sistema de información Isolucion.

2. 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 los indicadores de gestión del proceso Gestión TICs formulados en el Módulo Medición del aplicativo Isolucion a reportar durante la vigencia 2021 y 2022 y desde el 15 de diciembre de 2021 al 15 de abril de 2022.

Para el desarrollo formal del ejercicio de seguimiento, se seleccionaron los controles asociados a los riesgos de seguridad de Información del mapa de riesgos del proceso Gestión TIC, para el tema del Mapa de Riesgos en la Auditoria realizada en el último bimestre se generó el hallazgo cuyo plan de mejoramiento se orientó a la actualización del Mapa de Riesgos, dicho plan de mejora está en proceso de ejecución.

Para el seguimiento se identificaron los siguientes insumos:

Tabla No. 1. Insumos proceso Gestión TICs, para el seguimiento.

PLANES DE MEJORAMIENTO		RIESGOS	INDICADORES
Hallazgos	Observaciones		
3	4	2 (11 CONTROLES)	2

Fuente: Aplicativo Isolucion – OCI.

2.1 Indicadores del proceso Gestión TICs

El proceso tiene establecidos los siguientes indicadores:

1. Indicador “Nivel de cumplimiento solicitudes de soporte técnico GIT TIC´s”, con frecuencia de medición mensual.

De acuerdo con la información reportada en el sistema Isolucion se evidencia que el indicador presenta reporte de la medición para los meses de enero, febrero y dos cargues del mes de marzo. De acuerdo con lo indicado por el GIT – TICs la información de detalle y soporte de la medición depende de la suscripción del contrato de mesa de servicio, es decir que durante los periodos de tiempo en los cuales hay cubrimiento de contrato la información de los casos se registra en la herramienta del proveedor de turno y para los periodos de tiempo en los cuales no hay contrato hay que recurrir a otro tipo de herramientas ofimáticas lo cual hace más dispendioso el proceso de consolidación y medición del indicador y generando subregistro de la misma.

Se evidencia que para el mes de enero se logró un cumplimiento del 98,82%, para el mes de febrero el 100%, sin embargo, para el mes de marzo se realizaron dos mediciones parciales una del 1 al 24 y otra del 25 al 31, logrando un indicador del 100% cada una. Cabe destacar que las mediciones para el primer trimestre superan la meta del 95% establecida para el indicador. En el anexo 1 se evidencia lo descrito anteriormente.

2. Indicador: “Percepción del usuario en la calidad del servicio Grupo TIC´s”, con frecuencia de medición semestral

De acuerdo con la información de Isolución se evidencia que el indicador presenta información de la medición para los dos semestres de 2021, dicha medición se obtuvo mediante la aplicación de una encuesta de percepción de calidad del servicio a funcionarios y contratistas.

El resultado fue del 97% de percepción positiva para cada uno de los semestres. De lo anterior se concluye que la percepción positiva se ha mantenido durante la vigencia y se resalta como una fortaleza del proceso Gestión TIC. (en el anexo No. 2 muestra los descrito anteriormente por medio de una imagen).

2.2 Planes de Mejoramiento

El proceso Gestión TICs, cuanta con los siguientes planes de mejoramiento identificados con los números O-281, O-282, O-283,0-284, H-1196, H-1197, y H-1209, se procede a verificar el estado de avance de acuerdo con la información registrad en la plataforma Isolucion.

El cuadro siguiente muestra cada uno de los planes de mejoramiento y la verificación del avance.

Tabla No. 2. Avance en la Gestión de los Planes de Mejora proceso "Gestión TICs".

NÚMERO	DESCRIPCION	FECHA DE COMPROMISO	AVANCE
281	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. Gesdoc 2021IE0010416 "Informe Final Proceso Gestión de Tecnologías de Información y las Comunicaciones." Auditor: Jose Edgar Hernando Galarza Bogotá	**2022/03/29**	**Reporta avance del 0% en Isolucion**
282	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. Gesdoc 2021IE0010416 "Informe Final Proceso Gestión de Tecnologías de Información y las Comunicaciones." Auditor: Jose Edgar Hernando Galarza Bogotá	**2022/03/29**	**Reporta avance del 0% en Isolución**
283	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" Gesdoc 2021IE0010416 "Informe Final Proceso Gestión de Tecnologías de Información y las Comunicaciones." Auditor: Jose Edgar Hernando Galarza Bogotá	**2022/03/29**	**Reporta avance del 0% en Isolución**
284	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. Gesdoc 2021IE0010416 "Informe Final Proceso Gestión de Tecnologías de Información y las Comunicaciones." Auditor: Jose Edgar Hernando	**2022/03/29**	**Reporta avance del 100% en Isolución**

	Galarza Bogotá		
1197	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). Gesdoc 2021IE0010416 "Informe Final Proceso Gestión de Tecnologías de Información y las Comunicaciones." Auditor: Jose Edgar Hernando Galarza Bogotá	**2022/05/15**	**Reporta avance del 0% en Isolución**
1198	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). Gesdoc 2021IE0010416 "Informe Final Proceso Gestión de Tecnologías de Información y las Comunicaciones." Auditor: Jose Edgar Hernando Galarza Bogotá	**2022/06/30**	**Reporta avance del 0% en Isolución**
1209	H – TICS – 01 – 2022: INSTALACIÏN DE SOFTWARE NO AUTORIZADO Condición: Se comprobó que en los equipos 32949 y 25536 se permitió la instalación de software, con lo cual se evidencia que no se está dando cumplimiento a la Política de Seguridad de la Información, código GT-PO-002, V1, del 13/Dic/2021. Ver Anexo 2 GESDOC 2022IE0002287 "Informe Final Seguimiento al cumplimiento Derechos de Autor -Software Año 2021." Auditor: Yesid Fernando Santoyo	**2022/06/17**	**Reporta avance del 0% en Isolución**

Fuente: Aplicativo Isolucion – OCI.

Se evidencia que al corte 2022/03/30, el proceso logro cerrar uno (1) de los cuatro (4) planes establecidos para el trimestre, el identificado con el número 284. Los 3 planes restantes identificados con los números 281,282 y 283 cuya fecha de compromiso máxima para el 2022/03/29 no presentaron ningún avance.

Para los planes de mejoramiento identificados con los numero 1197,1198 y 1209 no se presenta avance, sin embargo, la fecha de compromiso no ha vencido.

2.3 Controles Seguridad de la Información del Mapa de Riesgos del Proceso de Gestión TIC

El Mapa de Riesgos del Proceso Gestión TIC tiene establecidos los siguientes dos (2) Riesgos de Seguridad Digital:

Riesgo 4: 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.

Riesgo 5: Pérdida y/o modificación de la información contenida en los documentos y herramientas utilizadas en el proceso de Gestión TICs.

Para el tratamiento de dichos riesgos se establecieron los siguientes controles:

Tabla No. 3: 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 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	Divulgación de los datos personales que reposan en documentos y herramientas utilizadas en el proceso de gestión de TI	Seguridad Digital
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	Pérdida y/o modificación de la información contenida en los documentos y herramientas utilizadas	Seguridad Digital

CONTROL	DESCRIPCION CONTROL	RIESGO	TIPOLOGIA
	(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	en el proceso de gestión de TI	
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 la siguiente evidencia: informe de vulnerabilidades y mejoras a realizar	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-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.

Durante el último bimestre de 2021 la OCI realizó Auditoría al proceso Gestión TIC y evidenció el hallazgo H – GT– 01 – 2021 – EVIDENCIAS DE REGISTRO DE LA APLICACIÓN DE LOS CONTROLES DE LOS RIESGOS DE SEGURIDAD DIGITAL, registrado en Isolución con el número 1197. El Líder del proceso estableció el Plan de Mejoramiento correspondiente el cual tiene las actividades: “Revisar y Actualizar matriz de riesgos de seguridad 2022” y “Hacer Seguimiento semestral a las evidencias reportadas en la matriz de riesgos de seguridad”, dichas actividades tienen como plazo de ejecución el 15/05/2022.

Se evidencia que en el sistema Isolucion no se han reportado formalmente avances de dichas actividades, sin embargo, el proceso GIT-TIC reporta avances en la actualización de la matriz de riegos y en la aplicación de los controles.

Cabe aclarar que el GIT informa que para la actualización del mapa de riesgos ha realizado sesiones de trabajo con la Oficina Asesora de Planeación y la publicación de este depende del proceso interno de dicha Oficina.

A continuación, se realiza un cuadro comparativo del Mapa de Riesgos, en los que corresponde a los riesgos de seguridad de la información y sus respectivos controles.

Tabla No. 4: Comparativo Mapa de Riesgos Isolucion vs Mapa de Riesgos propuestos Plan de Mejoramiento en estudio de la OAP.

Mapa de Riesgos Publicado en Isolucion	Mapa de Riesgos del Plan de Mejoramiento.
Riesgo 4: 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.	Riesgo 3: 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.
Riesgo 5: Pérdida y/o modificación de la información contenida en los documentos y herramientas utilizadas en el proceso de Gestión TICs.	Posibilidad de modificaciones no autorizadas a los datos contenidos en las plataformas tecnológicas de la entidad afectando la integridad de los mismos.

Fuente: Mapa de Riesgos proceso Gestión TICs – Información Reportada Proceso Gestión TICs.

Se observa que la nueva descripción del riesgo precisa de forma explícita los tipos de riesgo de pérdida de confidencialidad y perdida de integridad, lo anterior de acuerdo con lo establecido en la “Guía para la administración del riesgo y el diseño de controles en entidades públicas VERSIÓN 5” y su anexo 4 “ANEXO 4 LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN ENTIDADES PÚBLICAS”.

Se observa que en el nuevo mapa de riesgos se proponen los siguientes controles:

Tabla No. 5: Controles Mapa de Riesgos del Proceso Gestión TIC ACTUALIZADO:

CONTROL	DESCRIPCION CONTROL	RIESGO	TIPOLOGIA	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	Posibilidad de afectación económica y reputacional por perdida de información e indisponibilidad de canales y servicios. (Correo, servidores,	Gestión	A la fecha no se ha generado el informe de mantenimientos

CONTROL	DESCRIPCION CONTROL	RIESGO	TIPOLOGIA	EVIDENCIA DE APLICACIÓN
	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.	aplicaciones etc), debido a fallas en la plataforma tecnológica.		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	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

CONTROL	DESCRIPCION CONTROL	RIESGO	TIPOLOGIA	EVIDENCIA DE APLICACIÓN
	evidencia: Reportes de actividades de la plataforma de ciberseguridad de la entidad (Antispam en la Nube, SIEM, UTM, Consola Antivirus-DLP).			plataformas: SOPHOS AntiSpam, FireWall Av 68, FireWall CAR, SIEM, Sistema de Deteeciòn 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 v	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	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

CONTROL	DESCRIPCION CONTROL	RIESGO	TIPOLOGIA	EVIDENCIA DE APLICACIÓN
	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.			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).	Pérdida y/o modificación de la información contenida en los documentos y herramientas utilizadas en el proceso de gestión de TI	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.	Pérdida y/o modificación de la información contenida en los documentos y herramientas utilizadas en el proceso de gestión de TI	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.	Pérdida y/o modificación de la información contenida en los documentos y herramientas utilizadas en el proceso de gestión de TI	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: Mapa de Riesgos proceso Gestión TICs.

De acuerdo con las evidencias se observa que el proceso Gestión TIC ha aplicado el control y aporta las evidencias establecidas para 7 de los 12 controles establecidos, para los 5 controles restantes se presentan debilidades por falta de completitud o pertinencia de las mismas.

Adicionalmente se recomienda que dicho mapa de riesgos sea revisado a la luz de la normatividad reciente del MINTIC, como es el Decreto 338 del 8 de marzo de 2022 y la Resolución 746 del 11 de marzo de 2022, lo anterior con el fin de determinar su aplicabilidad e impacto en la gestión de los riesgos de Seguridad de la Información.

De otra parte, se observa que es necesario de forma prioritaria se publique por parte de la Oficina Asesora de Planeación el nuevo Mapa de Riesgos en la Plataforma Isolucion y que el proceso Gestión TIC registre los avances del plan de mejoramiento relacionado.

Se recomienda que para la definición de los controles a los Riesgos de Seguridad de la información se tenga en cuenta lo establecido en el numeral "*5.4 Controles asociados a la seguridad de la información: Las entidades públicas podrán mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. "Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas", siempre y cuando se ajusten al análisis de riesgos*.", de la *"Guía para la administración del riesgo y el diseño de controles en entidades públicas VERSIÓN 5"*

3. FORTALEZAS

- Se evidencia que la percepción de la calidad de los servicios tecnológicos es muy positiva por parte de los funcionarios y contratista del Ministerio del Deporte, lo anterior a la vez que genera confianza en los usuarios, se convierte en un reto para el proceso para mantener y mejorar los servicios tecnológicos.
- El Ministerio del Deporte cuenta con un equipo de funcionarios especializado en temas de Seguridad de la Información ya que cuenta con el Rol de Líder Seguridad de la Información y el Rol de Líder de Ciberseguridad. Lo anterior permite generar y fortalecer las capacidades de liderazgo y gestión para la implementación del marco normativo en materia de Seguridad Digital.

4. RESULTADOS:

RESUMEN TABAL DE HALLAZGOS Y OBSERVACIONES:

Código	Título	Observación
O–GT–01–2022	Fechas de Compromiso Planes de Mejoramiento.	Se Levanta
O–GT–02–2022	Procedimiento para la actualización de la Matriz de Riesgos del proceso Gestión TICS.	Se Levanta
O–GT–03–2022	Medición del Indicador "Nivel de cumplimiento solicitudes de soporte técnico GIT TIC´s", con frecuencia de medición mensual.	Se Mantiene

O – GT – 01 – 2022 – FECHAS DE COMPROMISO PLANES MEJORAMIENTO:

Para el 43% de los Planes de mejoramiento del Proceso Gestión TICs, se evidencia debilidad en el cumplimiento de las fechas de compromiso de acuerdo con lo evidenciado en el aplicativo Isolucion, Observaciones números 281, 282 y 283, teniendo en cuenta que presentan un avance del 0% y su fecha de compromiso se venció el pasado 29/03/2022. Lo anterior puede generar incumplimientos en la Mejora Continua del proceso.

Replica Presentada por parte del proceso:

Mediante comunicación radicada con el número 2022IE0004650 del 12 de mayo el GIT – TIC informa que "*Se ha solicitado en dos oportunidades vía correo electrónico la ampliación de fechas, como se evidencia en el archivo adjunto denominado: Correo_ Carolina Rodríguez Forero – Outlook*".

El GIT – TIC aporta el formato EI-FR-003 SOLICITUD MODIFICACIÓN PLAN DE MEJORAMIENTO en el cual solicita ampliación de plazo para los Planes de Mejoramiento identificados con los números 281,282,283, ante dicha solicitud la OCI respondió mediante memorandos 2022IE0002884 del 30 de marzo y 2022IE0004134 del 3 de mayo aprobando la ampliación con fecha de cierre proyectada el 15 de junio de 2022.

Análisis y Respuesta de la Oficina de Control Interno

Las evidencias aportadas por el GIT – TIC permiten concluir que se levanta la observación, teniendo en cuenta que el trámite de ampliación de plazo se surtió y aprobó por parte de la OCI y por lo tanto los planes de mejoramiento referidos se encuentran vigentes al corte del presente seguimiento.

Recomendación Específica:

La OCI recomienda, dar cumplimiento en términos a las actividades propuestas dentro del plan de mejoramiento a fin de evitar solicitudes de aplazamiento en las fechas de cumplimiento de estas.

O – GT – 02 – 2022 –*PROCEDIMIENTO DE *ACTUALIZACION DE LA MATRIZ DE RIESGOS DEL PROCESO GESTION TICs.

Se evidencia que las actividades de revisión y actualización del Mapa de Riesgos del proceso establecidas en el Plan de Mejoramiento No. 1197 en Isolucion ha requerido ampliación de plazo, sin embargo, el proceso ha aplicado nuevos controles por la necesidad de control de las operaciones.

Replica Presentada por parte del proceso:

Mediante comunicación radicada con el número 2022IE0004650 del 12 de mayo el GIT – TIC informa que las evidencias del control 4 del riesgo 2 fueron aportadas, una vez revisada dicha evidencia se concluye que el control se aplicó de acuerdo con lo establecido en el diseño de este.

Análisis y Respuesta de la Oficina de Control Interno

Se hace claridad que la observación no hace referencia a la no aplicación de los controles, por el contrario, la observación resalta que se aplicaron varios controles teniendo en cuenta la necesidad operativa a pesar de que el proceso de publicación del nuevo mapa de riesgos en el aplicativo Isolucion no se había realizado. Por lo anterior y debido a que con la réplica se aclara lo evidenciado por el Auditor, la observación se levanta.

Recomendación:

Fortalecer y establecer Acuerdos de Niveles de Servicio para los procedimientos para Actualización y publicación del Mapa de Riesgos o cualquier otro elemento de control del proceso de Gestión TIC se realice de forma oportuna ante la Oficina Asesora de Planeación.

***O – GT – 03 – 2022 – MEDICION DEL INDICADOR "*Nivel de cumplimiento solicitudes de soporte técnico GIT TIC´s"**

Se evidencia que para el mes de marzo de 2022 la medición del indicador "Nivel de cumplimiento solicitudes de soporte técnico GIT TIC´s" se realizó de forma parcializada, es decir se realizó una medición del 1 al 24 de marzo y otra del 25 de marzo a final de mes, lo anterior no es consistente con la ficha técnica del indicador que establece que su frecuencia es mensual.

Replica

Mediante comunicación radicada con el número 2022IE0004650 del 12 de mayo el GIT – TIC informa *"debido a que el 25 de marzo inicio el nuevo servicio de mesa de ayuda contratado por el Ministerio se realizan dos mediciones en el mismo mes una del 1 al 24 de marzo y otra del 25 al 31 de marzo, pero se está cumpliendo con la frecuencia de medición mensual; debido que la primera parte del mes el servicio se cumplió con personal de la entidad y la segunda parte del mes con personal de la empresa Selcomp no consideramos que esto de alguna forma este incumpliendo con la ficha del indicador de realizar la medición mensual puesto que solo se busca dar mayor claridad a la medición teniendo en cuenta que el soporte se brindó por dos servicios diferentes (uno por personal de la entidad y otro por el proveedor contratado), en las observaciones del mismo*

indicador se realizó precisión a la situación y esto permite medir la gestión del servicio de una forma más precisa y medir independientemente al proveedor que inicio desde el 25 de marzo; pero se está cumpliendo con el reporte mensual del indicador.".

Análisis y Respuesta de la Oficina de Control Interno

La observación de la OCI enfatiza en la debilidad de la consistencia de la medición con respecto al diseño del indicador y no hace referencia al incumplimiento de la medición, por lo tanto, la observación se mantiene.

Recomendaciones

Realizar una medición consolidada mensual de acuerdo con lo definido en el indicador, independientemente del responsable operativo de la prestación del servicio.

HALLAZGOS Y OBSERVACIONES REPETITIVOS

Para el presente Informe no se evidenciaron Hallazgos ni Observaciones repetitivos.

5. DESCRIPCIÓN DE LOS BENEFICIOS DEL SEGUIMIENTO.

La Oficina de Control Interno, reconoce el avance en la actualización del Mapa de Riesgos del proceso y su aplicación durante lo corrido de 2022, dando como resultado que no se han presentado incidentes de seguridad de la información durante el primer trimestre de 2022.

De otra parte se reconoce que la percepción de calidad del servicio prestado por el GIT-TIC se ha mantenido en niveles sueriores a la meta propuesta durante la vigencia 2021.

6. CONCLUSION(ES):

Del informe de seguimiento normativo realizado, se evidencia:

- La actualización del Mapa de Resgos del proceso permite la gestión adecuada de los riesgos identificados y su frecuente revisión permite fortalcer la capacidad de gestióm ante la dinámica de las amanezas de tipo informático.
- Los indicadores del proceso indican que los casos presentados a la mesa de ayuda se atienden de forma eficiente, de otra parte la percepción de la calidad de los servicio de TI por parte de los funcionarios tiene un alto grado de satisfacción.

7. RECOMENDACIÓN GENERAL:

- Se recomienda a los responsables del proceso analizar las observaciones contenidas en el presente informe y gestionar de forma oportuna las mejoras y/o actulizaciones que se requieran.
- Se recomienda propender por el cumplimiento oportuno de las actividades plasmadas en cada uno de los los planes de mejora a los cuales se les amplió en plazo de cierrre.
- Mantener y/o mejorar la percepción de calidad del servicio de TI que presta el GIT-TIC a la Entidad.

Cordialmente,

JAMES JILBERT LIZARAZO BARBOSA
Jefe Oficina de Control Interno

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

Anexos:

Anexo 1. Indicador Nivel de cumplimiento solicitudes de soporte técnico GIT TIC´s

Resumen

Valores	Valor	Fecha
Inicial	98.8201	01/ene./2022
Final	100	01/mar./2022
Máximo	100	01/mar./2022
Mínimo	98.8201	01/ene./2022
Variación del período	1,19%	01/ene./2022 - 01/mar./2022
Fórmula	(Número de solicitudes de soporte técnico atendidas/Número de solicitudes de soporte técnico generadas)*100	

Observaciones del Indicador

Fecha	Meta	Medición	Numerador	Denominador	Valor estimado	Límite superior	Límite inferior	Observación medición	Acciones implantadas	Anexo
01/mar./2022	95	100	587	587	100	100	90	Se realiza el registro de 587 casos sumando incidentes y requerimientos de servicio para el mes de febrero de 2022. Se resolvió el 100% de las solicitudes.		Registros(1)
01/feb./2022	95	100	379	379	100	100	90	Se realiza el registro de 379 casos sumando incidentes y requerimientos de servicio para el mes de enero de 2022. Se resolvió el 100% de las solicitudes.		Registros(1)
01/ene./2022	95	98,8201	335	339	98,8201	100	90	Se realiza el registro de 339 casos sumando incidentes y requerimientos de servicio para el mes de diciembre de 2021. Se resolvió el 98.8% de las solicitudes. El Ministerio cuenta con los servicios de una mesa de ayuda contratada con la empresa SELCOMP.		Registros(1)

Se muestras las últimas 3 mediciones
Medición menor que la Tol. Inferior Medición mayor o igual que la Tol. Superior Medición entre la Tol. Superior e Inferior

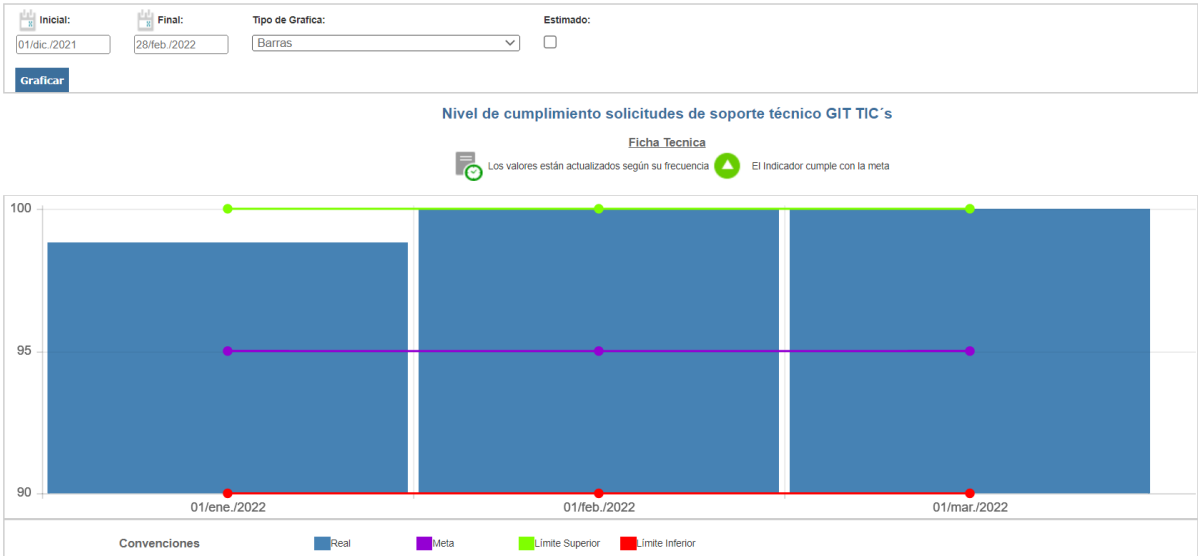
Fuente: Aplicativo Isolucion.

Observaciones del Indicador

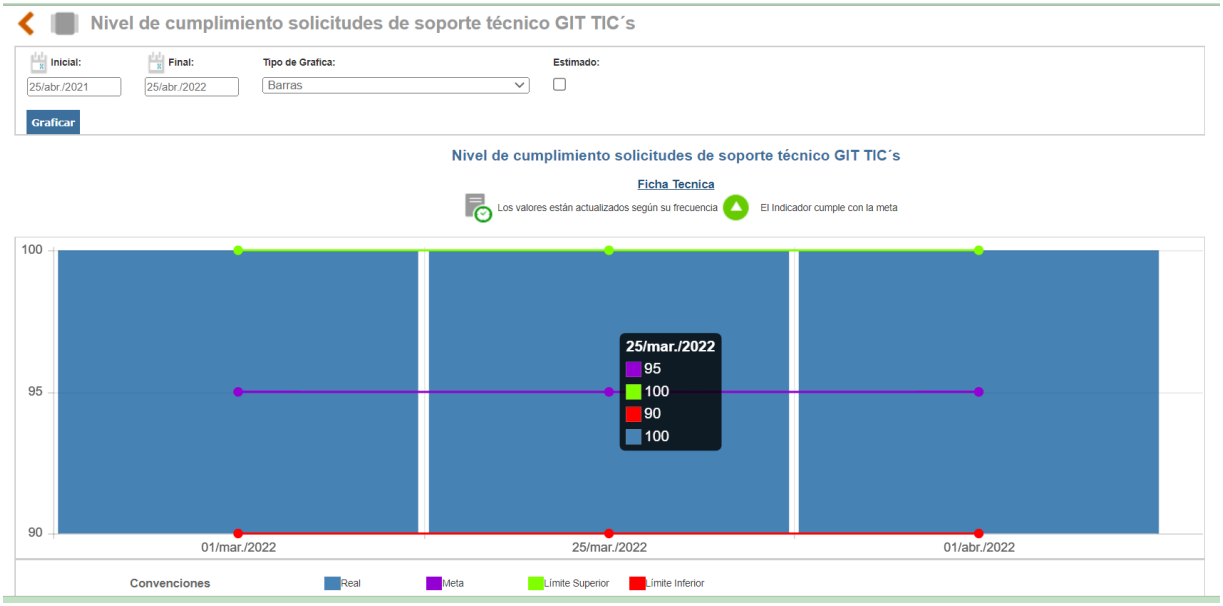
Fecha	Meta	Medición	Numerador	Denominador	Valor estimado	Límite superior	Límite inferior	Observación medición	Acciones implantadas	Anexo
01/abr./2022	95	100	97	97	100	100	90	Se realiza el registro de 97 casos sumando incidentes y requerimientos de servicio para el mes de marzo de 2022. (desde el día 25 hasta el día 31) Se resolvió el 100% de las solicitudes. El Ministerio cuenta con los servicios de una mesa de ayuda contratada con la empresa SELCOMP.		Registros(1)
25/mar./2022	95	100	319	319	100	100	90	Se realiza el registro de 319 casos sumando incidentes y requerimientos de servicio para el mes de marzo de 2022. (hasta el día 24) Se resolvió el 100% de las solicitudes.		Registros(1)
01/mar./2022	95	100	587	587	100	100	90	Se realiza el registro de 587 casos sumando incidentes y requerimientos de servicio para el mes de febrero de 2022. Se resolvió el 100% de las solicitudes.		Registros(1)

muestras las últimas 3 mediciones
Medición menor que la Tol. Inferior Medición mayor o igual que la Tol. Superior Medición entre la Tol. Superior e Inferior

Fuente: Aplicativo Isolucion.

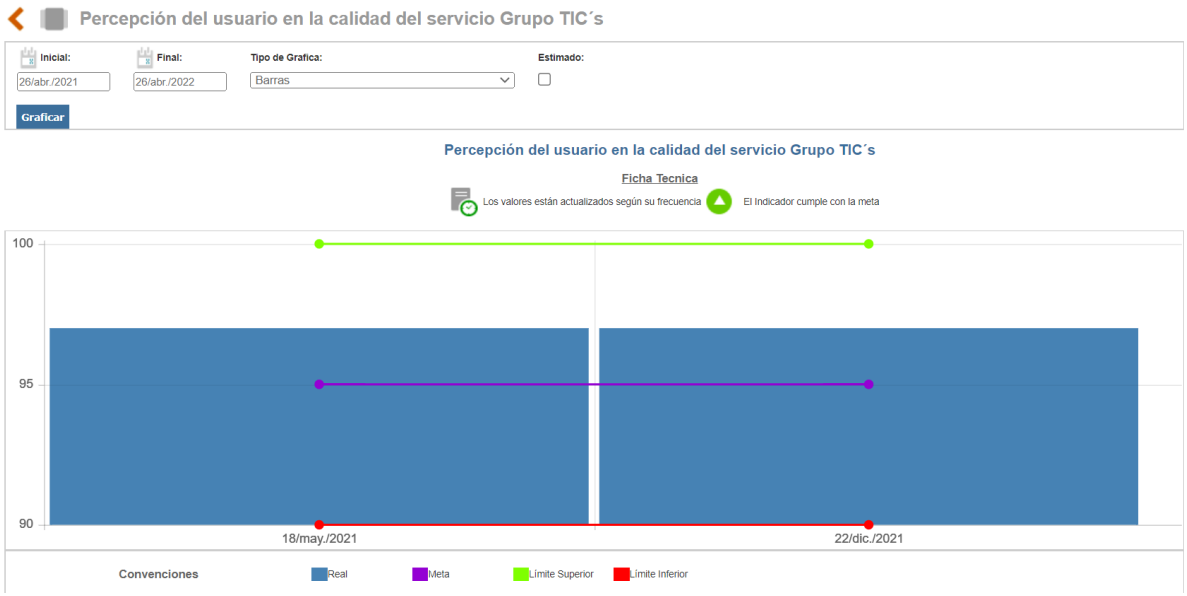


Fuente: Aplicativo Isolucion.



Fuente: Aplicativo Isolucion.

Anexo No. 2. Indicador “Percepción del usuario en la calidad del servicio Grupo TIC´s”



Fuente: Aplicativo Isolucion.