# INFORME DE AUDITORÍA AL SISTEMA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL Y CONTINUIDAD DE LA OPERACIÓN

**RESPONSABLE DE LOS PROCESOS AUDITADOS:**

**JAVIER ENRIQUE MARIÑO NAVARRO**
**Jefe Oficina de Tecnologías de la Información**

**ANGELA JANETH CORTÉS HERNÁNDEZ**
**Coordinadora GIT de Seguridad y Privacidad de la Información**

**AUDITORES DE LA OFICINA DE CONTROL INTERNO:**

**DIANA PATRICIA MURILLO CALDERÓN**

**JOSÉ IGNACIO LEÓN FLÓREZ**
**Jefe Oficina de Control Interno**

**OCTUBRE – 2023**
**OFICINA DE CONTROL INTERNO**

## TABLA DE CONTENIDO

## 1. INTRODUCCIÓN

La auditoría se realizó con base en la información suministrada por los responsables de los procesos de Seguridad y Privacidad de la Información, Gestión de TI, entrevistas a los mismos y recolección de datos adicionales.

Cada líder del proceso suministro el contenido de la información como base para su análisis.

Es responsabilidad de la Oficina de Control Interno elaborar un informe que incluye los resultados de la Auditoría ejecutada, las pruebas, procedimientos y análisis de la Auditoría que se practican de acuerdo con las normas vigentes de auditoría, políticas y procedimientos aplicados para el mejoramiento continuo.

Esta Auditoría se enmarca en el Modelo de Seguridad y Privacidad de la Información bajo la recopilación de las mejores prácticas, nacionales e internacionales, así como la normatividad interna aplicable.

El Modelo de Seguridad y Privacidad de la Información enmarcado en el Sistema de Gestión de Seguridad de la información, protege, preserva y administra la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información que circula en el mapa de operación por procesos, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales para prevenir incidentes, propender por la continuidad de la operación de los servicios y dar cumplimiento a los requisitos legales, reglamentarios, regulatorios y a los de las normas técnicas colombianas, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, promoviendo así por el acceso, uso efectivo y apropiación masiva de las Tecnologías de la Información y las Comunicaciones - TIC, a través de políticas y programas.

De acuerdo a lo anterior se hace importante evaluar la implementación y realizar seguimiento a este modelo del Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC y Fondo Único de Tecnologías de la Información y las Comunicaciones – FUTIC.

## 2. OBJETIVOS DE LA AUDITORÍA

### 2.1. Objetivo General

Evaluar el diseño, implementación y seguimiento del Modelo de Seguridad y Privacidad de la Información - MSPI y del Sistema de Gestión de SPI de la Entidad, con base en los lineamientos de la Política de Gobierno Digital, la NTC/IEC ISO 27001, la Política de Seguridad Digital, y los criterios de Continuidad de la operación de los servicios, así como la normatividad interna aplicable, con alcance a los procesos de Gestión de TI y de Seguridad y Privacidad de la Información.

### 2.2. Objetivos Específicos

- Evaluar el estado de la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI
- Realizar la evaluación de cumplimiento que le permita identificar el estado frente a los requisitos establecidos en la Norma NTC-ISO/IEC 27001:2013.
- Validar el estado de la implementación de la seguridad y privacidad de la información en base a los lineamientos de la Política General de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad de la Operación del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones.
- Evaluar los planes de acción que se han establecido, para llevar a cabo el cierre de las brechas identificadas orientados a dar cumplimiento a la norma; en el marco de estándares y buenas prácticas generalmente aceptadas.

## 3. ALCANCE DE LA AUDITORÍA

La auditoría se realizará en las instalaciones del Mintic, ubicada en el Edificio Murillo Toro, Cra 8 # Entre Calles 12 y 13, Bogotá y se encuentra orientada a evaluar la implementación del MSPI y los controles relacionados con la Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación para los procesos los procesos de Gestión de TI y de Seguridad y Privacidad de la Información.

El periodo analizado de la documentación de registros, procedimientos, políticas y manuales comprende desde el 2022 hasta 2023.

Para el caso del objetivo específico 3 el periodo analizado comprende desde el 2021 hasta el 2023 y para el objetivo especifico 4 el periodo analizado comprende desde el 2020 hasta el 2023

## 4. CRITERIOS DE AUDITORÍA

**Marco Jurídico:**

- **Ley 87 de 1993.** Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado.
- **Ley 594 de 2000**. Por medio de la cual se expide la Ley General de Archivos.
- **Ley 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Ley 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 1978 de 2019**. Por la cual se moderniza el sector de las Tecnologías de la Información y las Comunicaciones TIC), se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones.

**Decretos**:

- **Decreto 2609 de 2012.** Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- **Decreto 886 de 2014**. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- **Decreto 1078 de 2015.** Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 1083 de 2015.** Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública.
- **Decreto 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.
- **Decreto 1064 de 2020**. "Por el cual se modifica la estructura del Ministerio de Tecnologías de la Información y las Comunicaciones"

**Resoluciones**:

· **Resolución 2999 del 2008**. Por el cual se adoptan las políticas de seguridad para el manejo de la información y se dictan otras normas para el uso y administración de los bienes y servicios informáticos del Ministerio TIC.
· **Resolución 1151 de 2019.** Por la cual se establecen las condiciones especiales del Teletrabajo en el Ministerio de Tecnologías de la Información y las Comunicaciones, y se deroga la Resolución 0002133 del 3 de agosto de 2018.
· **Resolución 1905 de 2019.** Por la cual se actualiza el Modelo Integrado de Gestión (MIG) del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se deroga la Resolución 911 de 2018.
· **Resolución 924 de 2020.** Por la cual se actualiza la política de tratamiento de datos personales del Ministerio/Fondo Único de TIC y se deroga la resolución 2007 de 2018.
· **Resolución 1124 de 2020.** Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se definen lineamientos frente al uso y manejo de la información y se deroga la resolución 512 de 2019.
· **Resolución 2175 de 2022.** Por la cual se establecen el Modelo Integrado de Gestión (MIG) y el Sistema Integrado de Gestión (SIG) del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones y se deroga la Resolución 1092 de 2021 y sus modificatorias.
· **Resolución 448 de 2022.** Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se deroga la Resolución 2256 de 2020.
· **Resolución 3066 de 2022.** Por la cual se crean grupos internos de trabajo del Ministerio de Tecnologías de la Información y las Comunicaciones, se asignan funciones y se derogan unas resoluciones.

**Documentos del proceso:**

· Gestión de incidentes de Seguridad y Privacidad de la Información V.2. SPI-TIC-PR-001

· Manual de políticas de seguridad y privacidad de la información V.4. SPI-TIC-MA-001
· Lineamientos para la Administración de Riesgos V.13. MIG-TIC-MA-008
· Mapa de Riesgos SPI - Gestión Tecnologías de la Información V5 GTI-TIC-DI-005
· Mapa de Riesgos SPI - Seguridad Privacidad Información V5 SPI-TIC-DI-012
· Plan de tratamiento de riesgos de seguridad y privacidad de la Información V5 SPI-TIC-DI-015
· Gestión de usuarios y perfiles para el acceso a Recursos TI V6 GTI-TIC-PR-007
· Gestión de cambios V3 GTI-TIC-MA-017

**Mejores prácticas:**

· ISO/IEC 27001:2023

**Otros documentos:**

· Plan de Seguridad y Privacidad de Información V7 PI-TIC-DI-017
· Declaratoria de Aplicabilidad
· Plan de recuperación de desastres tecnológicos- DRP V2 PI-TIC- MA-007
· Respaldo, retención y restauración de Información V6 TI-TIC-PR-005
· Borrado de Información V1 GTI-TIC-IN-033
· Gestión del Talento Humano V12 GTH-TIC-PR-001
· Manuales de funciones personal de TI y Seguridad de la Información
· Ingreso de los funcionarios de libre nombramiento y remoción y provisionalidad V12 TH-TIC-PR-001
· Gestión de tecnologías de la Información V1 TI-TIC-PR-042
· Organigrama de Seguridad de la Información
· Procedimientos activos de información V4 DO-TIC-PR-019
· Manual del MIG V22 MIG-TIC-MC-001
· Metodología de gerencia de proyectos V4 DES-TIC-MA-008
· Plan de Continuidad de las Operaciones – BCP V2 SPI-TIC- MA-008
· Estrategias para la continuidad de las operaciones – BCP V2 SPI-TIC-MA-005
· Análisis de Riegos de Interrupción – RIA -MINTIC V2 SPI-TIC- MA-004
· Política de seguridad y control de acceso físico V1 GRA-TIC- MA-004
· Informes de pruebas al BCP.
· Otros documentos del SIMIG

## 5. METODOLOGÍA

Para el desarrollo de la auditoría se tuvieron en cuenta los siguientes procedimientos de auditoría:

· **Consulta:** (entrevistas, encuestas, cuestionarios).
· **Observación**: (a personas, procedimientos o procesos).
· **Inspección**: (estudio de documentos, registros y examen físico de recursos tangibles).
· **Revisión de comprobante**s: (se realiza específicamente para probar la validez de la información documentada o registrada).

### 5.1. Reunión de Apertura

La reunión de apertura de la Auditoría se llevó a cabo el día 10 de mayo 2023 a través de la plataforma Microsoft Teams con los procesos de Gestión de TI y de Seguridad y Privacidad de la Información y los interlocutores designados por cada líder para atender los requerimientos durante el desarrollo de la Auditoría y los temas a tratar en las reuniones.

### 5.2. Reunión de Cierre:

El 19 de septiembre de 2023 a través de reunión virtual por medio de la herramienta Teams, se realizó el cierre de auditoría a los procesos de Gestión de TI y Seguridad y Privacidad de la Información, en la cual se informó y sustentó de forma general los hallazgos evidenciados en el desarrollo de la auditoría, las recomendaciones y las fortalezas.

### 5.3. Resumen de la validación del informe preliminar:

El martes 19 de septiembre de 2023, mediante correo electrónico fue remitido a los procesos de Gestión de TI y Seguridad y Privacidad de la Información, el informe preliminar de la auditoría realizada para su debida revisión y comentarios. Las áreas remitieron la respuesta al informe preliminar el día 26 de septiembre de 2023.

La Oficina de Control Interno realizó la validación de la respuesta al informe preliminar y como resultado de esta actividad se obtuvo.

| Informe Preliminar Hallazgos | Hallazgos excluidos | Hallazgos incluidos en el Informe Final |
|---|---|---|
| 11 | 5<br>(H.1.1) (H.1.2)<br>(H.1.5)<br>(H.2.4)<br>(H.2.5) | 6 |

***Tabla 1. Tabla validación de respuesta de hallazgos***

Los detalles del análisis realizado por la Oficina de Control Interno a las observaciones del auditado sobre el informe preliminar se encuentran en el anexo 1 al final del presente informe.

## 6. DESARROLLO DE LA AUDITORÍA

Como resultado de las entrevistas, verificación y análisis de documentos, se detectaron las siguientes situaciones. Cada situación redactada contiene la evidencia que soporta, el análisis, la situación encontrada, la muestra seleccionada y el criterio de Auditoría incumplido.

El informe está estructurado conforme a los objetivos definidos en el plan de auditoría y en cada objetivo se encuentra un resumen de las actividades realizadas y las situaciones identificadas.

Durante la fase de planeación de la auditoría, se realizó el 18 de abril del 2023 una solicitud preliminar sobre los soportes en sus versiones actualizadas relacionadas con Políticas, manuales, procedimientos, instructivos, declaratoria de aplicabilidad, inventarios de activos, metodologías de riesgos para la seguridad de la información entre otros documentos relacionados con la seguridad y privacidad de la información, seguridad digital y continuidad de la

operación, además de tener en cuenta los controles de la Norma ISO 27001:2013.

Adicionalmente, con el objetivo de revisar e indagar aspectos relacionados con los temas de la auditoría, se llevaron a cabo las siguientes reuniones con los procesos de Gestión de TI y Seguridad y Privacidad de la Información mediante la plataforma teams.

- El 15 de mayo de 2023: Requisitos aplicables al contexto de la Entidad.
- El 18 de mayo de 2023: Liderazgo y compromiso de la alta dirección respecto a la seguridad de la información.
- El 23 de mayo de 2023: Seguimiento al Modelo de Seguridad y Privacidad de la Información- MSPI.
- El 24 de mayo de 2023: Políticas de Seguridad de la Información y los aspectos relacionados con la organización de la Seguridad.
- El 25 de mayo de 2023: Seguridad de los recursos humanos en el antes, durante, terminación o cambio de empleo.
- El 29 de mayo de 2023: Gestión de activos e inventarios de equipos de cómputo e inventarios de software.
- El 30 de mayo de 2023: Seguridad de las operaciones.
- El 02 de junio de 2023: Seguridad de las comunicaciones.
- El 05 de junio de 2023: Requisitos aplicables al cumplimiento de requisitos legales y contractuales.
- El 05 de junio de 2023: Control de acceso a los sistemas y aplicaciones.
- El 06 de junio de 2023: Incidentes de seguridad de la información y ciberseguridad.
- El 07 de junio de 2023: Adquisición, desarrollo y mantenimiento de sistemas.
- El 09 de junio de 2023: Seguridad de la información de la gestión de la continuidad del negocio.
- El 15 de junio de 2023: Se realizó recorrido en las instalaciones para revisar y verificar la seguridad en el centro de cómputo, cableado, racks, ups, planta eléctrica, control de acceso físico al centro de cómputo.
- El 16 de junio de 2023: Recorrido en las instalaciones para realizar entrevistas con los funcionarios y contratistas, a fin de revisar aspectos relacionados con la seguridad de la información y ciberseguridad, además de revisar y verificar las condiciones ambientales y físicas del archivo de gestión documental.

La calificación que se definió para determinar el nivel de cumplimiento de los objetivos 1 y 2, se dieron en base a los lineamientos de escala de evaluación del

"Instrumento de evaluación MSPI", herramienta que fue creada con el fin de identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información así:

| Descripción | Criterio | Calificación |
|---|---|---|
| **Inexistente** | Total, falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles. | **0** |
| **Inicial** | Hay una evidencia de que la organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación depende de cada individuo y es principalmente reactiva.<br>Se cuenta con procedimientos documentados, pero no son conocidos y/o no se aplican. | **20** |
| **Repetible** | Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores. | **40** |
| **Efectivo** | Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada. | **60** |
| **Gestionado** | Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no | **80** |

| | | |
|---|---|---|
| | estén funcionando eficientemente. | |
| **Optimizado** | Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua. | **100** |

***Tabla 2. Escala de evaluación***

**Objetivo específico 1. Evaluar el estado de la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI**

Para realizar la validación de este objetivo se tuvo en cuenta los siguientes criterios de auditoría referenciados bajo el Modelo de Seguridad y Privacidad de la Información el cual imparte los lineamientos en materia de implementación y adopción de buenas prácticas. Lo anterior, para que las entidades incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y, en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

En este modelo se define que en la fase del diagnóstico se permite conocer el estado actual de la implementación de la seguridad y privacidad de la información y para ello se deberá realizar un diagnóstico utilizando el “Instrumento de evaluación MSPI” con el que se identifica de forma específica los controles implementados y faltantes.

El “Instrumento de Evaluación MSPI” es una herramienta que fue creada con el fin de identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades.

El seguimiento de este instrumento evaluado para esta auditoría se obtuvo por solicitud de información al proceso de Seguridad y Privacidad de la Información.

Este instructivo cuenta con las siguientes hojas:

- Portada: Comprende los componentes de nombre de la entidad, fecha, quien lo elabora, Brecha Anexo A ISO 27001:2013 y nivel de madurez.
- Escala de evaluación: Define la calificación de los controles.
- Levantamiento de información.
- Áreas involucradas.
- Pruebas Administrativas: Pruebas orientadas a los temas de seguridad de la información que no están directamente relacionadas con las áreas tecnológicas de la Entidad.
- Pruebas Técnicas.
- Avance PHVA: Nivel de cumplimiento de los componentes Planificación, Implementación, Gestión y Mejora Continua.
- Ciberseguridad: Marco de ciberseguridad de NIST (Instituto Nacional de Estándares y Tecnología)
- Madurez MSPI: Requisitos evaluados previamente en las hojas Administrativas, Técnicas y PHVA.

Las **pruebas administrativas** se componen de siete (7) de los 14 dominios de la ISO 27001:2013 y cada dominio cuenta con sus controles distribuidos así:

| Dominio | Control |
|---|---|
| A.5 Políticas de Seguridad de la Información | A.5.1.1 - A.5.1.2 |
| A.6 Responsabilidades y Organización Seguridad Información. | A.6.1.1 - A.6.1.2 - A.6.1.3 - A.6.1.4 - A.6.1.5 - A.6.2.1- A.6.2.2- |
| A.7 Seguridad de los recursos humanos | A.7.1.1 - A.7.1.2 - A.7.2.1 - A.7.2.2 - A.7.2.3- A.7.3.1 |
| A.8 Gestión de Activos | A.8.1.1- A.8.1.2 - A.8.1.3 - A.8.1.4- A.8.2.1- A.8.2.2 - A.8.2.3 - A.8.3.1- A.8.3.2 - A.8.3.3 |
| A.15 Relación con los Proveedores | A.15.1 - A.15.2 |
| A.17 Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio | A.17.1.1 - A.17.1.2 - A.17.1.3 - A.17.2.1 |
| A.18 Cumplimiento | A.18.1.1- A.18.1.2- A.18.1.3- A.18.1.4- A.18.1.5- A.18.2.1 - A.18.2.2 - A.18.2.3 |

***Tabla 3. Dominios ISO27001:2013- Pruebas administrativas***

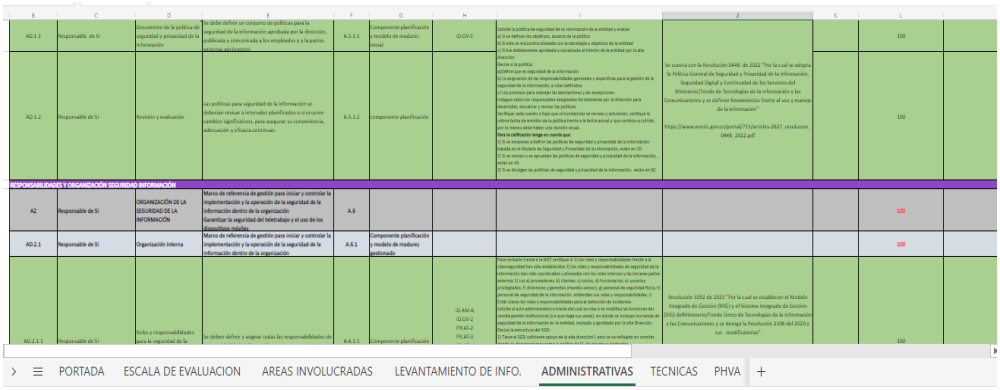
En cuanto a las pruebas técnicas, estas se componen de los siete (7) de 14 dominios de la ISO 27001:2013 y cada dominio cuenta con sus controles distribuidos así:

| Dominio | Control |
|---|---|
| A.9 Control de Acceso | A.9.1.1- A.9.1.2- A.9.2.1- A.9.2.2- A.9.2.3- A.9.2.4- A.9.2.5- A.9.2.6 - A.9.3.1- A.9.4.1- A.9.4.2 - A.9.4.3- A.9.4.4 - A.9.4.5 |
| A.10 Criptografía | A.10.1.1 - A.10.1.2 |
| A.11 Seguridad Física y del Entorno | A.11.1.1 - A.11.1.2 - A.11.1.3- A.11.1.4 - A.11.1.5 -A.11.1.6- A.11.2.1 - A.11.2.2 - A.11.2.3- A.11.2.4 - A.11.2.5 - A.11.2.6- A.11.2.7- A.11.2.8- A.11.2.9 |
| A.12 Seguridad de las Operaciones | A.12.1.1- A.12.1.2- A.12.1.3- A.12.1.4- A.12.2.1- A.12.3.1 - A.12.4.1- A.12.4.2- A.12.4.3- A.12.4.4- A.12.5.1- A.12.6.1- A.12.6.2 - A.12.7.1 |
| A.13 Seguridad de las Comunicaciones | A.13.1.1- A.13.1.2- A.13.1.3- A.13.2.1- A.13.2.2- A.13.2.3 - A.13.2.4 |
| A.14 Adquisición, desarrollo y mantenimiento de sistemas | A.14.1.1- A.14.1.2- A.14.1.3- A.14.2.1- A.14.2.2- A.14.2.3- A.14.2.4- A.14.2.5- A.14.2.6- A.14.2.7- A.14.2.8- A.14.2.9- A.14.3.1 |
| A.16 Gestión de Incidentes de seguridad de la Información | A.16.1.1- A.16.1.2- A.16.1.3- A.16.1.4- A.16.1.5- A.16.1.6- A.16.1.7 |

***Tabla 4. Dominios ISO27001:2013- Pruebas técnicas***

El porcentaje de avance de seguimiento de este instrumento suministrado está definido en el 100% de implementación.

Para este objetivo específico 1, se tuvieron en cuenta los componentes de la hoja de **Pruebas Administrativas** que comprende los controles de la Norma ISO27001:2013 de los dominios A5, A6, A7, A8, A15 A17 y A18 y que hacen parte del modelo.




***Grafica 1. Instrumento de Evaluación MSPI***

## PRUEBAS ADMINISTRATIVAS:

Para la validación y determinar el nivel de cumplimiento de este objetivo específico 1 se tuvo en cuenta el Id. Item del instrumento de evaluación MSPI.

| ID ITEM DEL INSTRUMENTO | | VALIDACIÓN | NIVEL DE CUMPLIMIENTO |
|---|---|---|---|
| **A.5 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN** | | | |
| AD.1.1 | Se debe definir un conjunto de políticas para la seguridad de la información aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes. | -La Resolución 448 del 2022 se encuentra publicada en la página del MINTIC y define los objetivos y el ámbito de aplicación.<br><br>-El Manual de políticas de seguridad y privacidad de la información establece los lineamientos para la adecuada gestión de la seguridad y privacidad de la información en el Ministerio/Fondo Único de TIC, enmarcados en la implementación de un Sistema de Gestión de Seguridad de la Información, basado en la identificación y valoración de los riesgos asociados a ella, propendiendo por la protección de su confidencialidad, integridad, disponibilidad, privacidad, continuidad, autenticidad y no repudio y por el cumplimiento de la normatividad vigente | **100** |

| | | | |
|---|---|---|---|
| | | aplicable, este manual está aprobado y se encuentra publicado en el Sistema Integral de Gestión **ISOLUCIÓN**.<br><br>Se valido que la Subdirección para la Gestión del Talento Humano, anualmente en el Plan Institucional de Capacitación define las capacitaciones asociadas con la seguridad y privacidad de la Información. Así mismo se cuenta con un Plan de Cambio, cultura y apropiación de Seguridad y Privacidad de la Información, el cual tiene como objetivo diseñar estrategias para socializar, apropiar, preservar e impulsar la cultura de seguridad y privacidad de la información en los colaboradores de la Entidad | |
| AD.1.2 | Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas. | La Política de Seguridad y Privacidad, Seguridad digital y continuidad de los servicios de Ministerio/Fondo Único de tecnologías de la información y las comunicaciones, es revisada anualmente o antes si existiesen modificaciones que así lo requieran para que sea siempre oportuna, suficiente y eficaz. | **100** |
| **A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN** | | | |
| AD.2.1.1 | Se deben definir y asignar todas las responsabilidades de la seguridad de la información. | En la Resolución 2175 de 2022 Art 13 Nral 3 se definen las responsabilidades específicas del líder del sistema de seguridad y privacidad de la información. | **100** |
| AD.2.1.2 | Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no | Se tiene un equipo implementador para los temas relacionados con la separación de deberes de la seguridad de la información. | **100** |

| | | | |
|---|---|---|---|
| | intencional, o el uso indebido de los activos de la organización. | | |
| AD.2.1.3 | Las organizaciones deben tener procedimientos establecidos que especifiquen cuándo y a través de que autoridades se debe contactar a las autoridades. | En el Manual del MIG se definen los lineamientos para el contacto con las autoridades Nral. 8.2.2.14 Partes Interesadas Sistema de Gestión seguridad y privacidad de la información.<br><br>En caso de que se presente un incidente de seguridad y privacidad de la información y que sea necesario reportar al CSIRT se aplica el procedimiento Gestión de incidentes de seguridad y privacidad de la información V2 SPI-TIC-PR-001, Actividad Nro 26 **Informar incidente de seguridad y privacidad de la información a entes de control o autoridades competentes.** | **100** |
| AD.2.1.4 | Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad. | En el Manual de políticas de seguridad y privacidad de la información Nral 6.1 está documentado el contacto con los grupos de interés especial.<br>Así mismo se valida que en el Manual del MIG se establecen otros lineamientos para el contacto con las autoridades Nral 8.2.2.14 Partes Interesadas Sistema de Gestión seguridad y privacidad de la información, con el fin de compartir e intercambiar conocimientos en pro a la mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información del Ministerio/Fondo Único de TIC. | **100** |
| AD.2.1.5 | La seguridad de la información se debe integrar al(los) método(s) de gestión de proyectos de la organización, para asegurar que los riesgos de seguridad de la información se identifiquen y | Los lineamientos de Seguridad de la Información en la gestión de proyectos se encuentran definidos en el Manual de Políticas de Seguridad y Privacidad de la Información.<br><br>Las fases del ciclo de vida que se aplican para los proyectos están definidas en la Metodología de Gerencia de proyectos, por ello es importante que se acojan para los proyectos a los que aplique esta metodología, además de los lineamientos de seguridad de la | **100** |

| | | | |
|---|---|---|---|
| | traten como parte de un proyecto. | información que brinda el Manual de políticas de seguridad y privacidad de la información y cada uno de los aspectos que allí se plantean. | |
| AD.2.2.1 | Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles. | La Entidad adopta los lineamientos de seguridad para el uso de dispositivos móviles y en el procedimiento GTI-TIC-PR-030 Trae Tu Propio Dispositivo se definen las actividades para registrar los equipos personales de los servidores públicos, contratistas y terceros (si el contrato lo permite), con el fin de proteger la información del Ministerio TIC a través de la iniciativa Trae Tu Propio Dispositivo.<br><br>El formato GTI-TIC-FM-009 Consentimiento Informado de Participación en la Iniciativa TTPD, aplica para funcionarios y contratistas que usan dispositivos tecnológicos personales y da las indicaciones de las medidas de seguridad para el uso de estos equipos. | **100** |
| AD.2.2.2 | Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo. | Se valida que en el Manual de políticas de seguridad y privacidad de la información se adoptan los lineamientos para el Teletrabajo, se aplica el Acuerdo Teletrabajo V4 GTH-TIC-FM-052 en que se suscribe el acuerdo entre el funcionario y el jefe acordando las obligaciones generales y especificas en las que se relacionan el suministro de herramientas tecnológicas, capacitaciones al teletrabajador, apoyo técnico de equipos y programas informáticos entre otros.<br><br>Desde la Gestión del Talento Humano se evalúan, se seleccionan y vinculan a los teletrabajadores, estas directrices se definen en el procedimiento de Teletrabajo V7 GTH-TIC-PR-018. | **100** |
| **A7 SEGURIDAD DE LOS RECURSOS HUMANOS** | | | |
| AD.3.1.1 | Las verificaciones de los | Se valida que, para el ingreso de funcionarios de Libre Nombramiento y Remoción, provisionalidad y | |

| | | | |
|---|---|---|---|
| | antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos. | nombramiento de cargos de carrera administrativa, se establece la verificación de cumplimiento de requisitos a través del GTH-TIC-FM 031 Estudio Técnico de Requisitos.<br><br>Adicionalmente los funcionarios públicos deben cumplir como requisito de ingreso con el diligenciamiento de GTH-TIC-FM-053 Compromiso de confidencialidad de información funcionario y el SPI-TIC-FM-001 Autorización expresa de recolección y tratamiento de datos personales. | **100** |
| AD.3.1.2 | Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información. | Cada funcionario que ingresa debe cumplir como requisito de ingreso con el diligenciamiento de GTH-TIC-FM-053 Compromiso de confidencialidad de información funcionario y el SPI-TIC-FM-001 Autorización expresa de recolección y tratamiento de datos personales. | **100** |
| AD.3.2.1 | La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización. | Se valida que la Subdirección para la Gestión del Talento Humano, estable anualmente el Plan Institucional de Capacitación el cual incluye capacitaciones asociadas con la Seguridad y Privacidad de la Información.<br><br>Así mismo anualmente se realiza la campaña de actualización de diligenciamiento de formatos de compromiso de confidencialidad y conflicto de interés. | **100** |
| AD.3.2.2 | Todos los empleados de la Entidad, y en donde sea | La Entidad cuenta con un Plan de Cambio, Cultura y Apropiación de Seguridad y Privacidad de la Información. | |

| | | | |
|---|---|---|---|
| | pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo. | La inducción en seguridad de la información se realiza cuando ingresa un funcionario o contratista.<br><br>Durante las sensibilizaciones que se llevan a cabo se realizan encuestas de satisfacción con preguntas específicas de los temas vistos relacionados con la seguridad de la información y ciberseguridad. | **100** |
| AD.3.2.3 | Se debe contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información. | Se valida el procedimiento Investigación disciplinaria GTH-TIC-PR-017 en el cual se definen los lineamientos para determinar y verificar las faltas disciplinarias.<br><br>Anualmente se realiza una campaña de actualización de diligenciamiento de formatos de compromiso de confidencialidad y conflicto de interés. | **100** |
| AD.5.1.3 | Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir. | La Entidad define y aplica los lineamientos sobre las responsabilidades de los colaboradores del Ministerio/Fondo Único de TIC asociados con la seguridad de la información que permanecen validos después de la terminación o cambio de empleo. | **100** |
| **A.8 GESTIÓN DE ACTIVOS** | | | |
| AD.4.1.1 | Se deben identificar los activos asociados con la | La Entidad define y aplica los lineamientos para la identificación y valoración de los activos de información de la Entidad. | **100** |

| | | | |
|---|---|---|---|
| | información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos. | De otra parte, se cuenta con el Manual de Activos de Información donde se definen los criterios básicos para la identificación, clasificación y valoración de activos de información del Ministerio/Fondo Único de TIC.<br><br>La Entidad cuenta con el inventario de activos de información, la última publicación se realizó en octubre del 2022 en la plataforma del SIMIG y la página web (transparencia y acceso a la información pública datos abiertos). | |
| AD.4.1.2 | Los activos mantenidos en el inventario deben tener un propietario. | En el inventario de activos de la información se asocia el propietario de cada activo.<br><br>No obstante, dentro de la revisión al instructivo Asignación o devolución de equipos de cómputo no se detalla en el mismo, quienes pueden ser los propietarios de los equipos, cuál sería el límite de asignación de equipos y quiénes serían los responsables del manejo de la información. | **80** |

**Hallazgo 1.1: Falta de actualización del instructivo Asignación o devolución de equipos de cómputo.**

Se revisó el instructivo “GTI-TIC-IN-002 V2 Asignación o devolución de equipos de cómputo” el cual aplica para todo el personal funcionario o contratista que realice la solicitud de un equipo de cómputo en arriendo. Mediante una toma de muestra de cuatro (4) de diez (10) funcionarios del inventario FUTIC se evidenció que un usuario puede tener asignado dos (2) o más equipos de cómputo; al validar en el instructivo sobre quienes pueden ser los propietarios de los equipos, cuál sería el límite de asignación de equipos y quiénes serían los responsables del manejo de la información según sea el caso, esta información no se especifica en este instructivo.

**VER ANEXO 1.1**

Lo anterior expuesto incumple las pruebas administrativas que comprenden el ítem AD.4.1.2 del Seguimiento Instrumento Evaluación MSPI.
“Solicite el procedimiento para asegurar la asignación oportuna de la propiedad de los activos”

**Recomendación.** Se recomienda la actualización del instructivo GTI-TIC-IN-002 V2 Asignación o devolución de equipos de cómputo indicando quienes pueden ser los propietarios, quienes los responsables, cuál sería el límite de asignación y demás especificaciones que se consideren relevantes.

| ID ITEM DEL INSTRUMENTO | | VALIDACIÓN | NIVEL DE CUMPLIMIENTO |
|---|---|---|---|
| AD.4.1.3 | Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información. | La Entidad define los lineamientos para el buen uso de la información, se encuentran establecidos en el Manual de Políticas de Seguridad de la Información. | **100** |
| AD.4.1.4 | Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo. | Los empleados públicos y contratistas del Ministerio/Fondo Único de TIC deben hacer entrega de los activos bajo su responsabilidad de acuerdo con el formato de Paz y Salvo de los Procesos de Gestión del Talento Humano y Gestión de Compras y Contratación. | **100** |
| AD.4.2.1 | La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada. | En el Manual de políticas de seguridad y privacidad de la información se establecen los lineamientos para la protección de la información de la Entidad, de acuerdo con su criticidad. | **100** |
| AD.4.2.2 | Etiquetado de la Información | La clasificación y rotulación de la información aplica a todos los documentos o correos electrónicos producidos en el marco de la operación | **100** |

| | | | |
|---|---|---|---|
| | | de los procesos del Ministerio/Fondo Único de TIC.<br><br>En el documento de clasificación y rotulado de la información se establecen los lineamientos que deben seguir los funcionarios y/o Contratistas del Ministerio/Fondo Único de TIC, para la clasificación y rotulación de la información física y electrónica.<br><br>La Entidad implementa los criterios para el etiquetado de la información física que conserva Gestión Documental. | |
| AD.4.2.3 | Manejo de activos | Se define en el Manual de políticas de seguridad y privacidad de la información los lineamientos para evitar la divulgación, modificación, retiro o destrucción de la información almacenada en los medios de la Entidad.<br><br>En los planes de Cambio y Cultura de Seguridad y Privacidad de la información se socializa a contratistas y funcionarios sobre la importancia del buen manejo de los Activos. | **100** |
| AD.4.3.1 | Gestión de medios removibles | Para llevar a cabo la gestión de medios removibles se considera el documento Borrado de Información el cual define las acciones que se deben ejecutar para realizar el borrado de la información de la Entidad contenida en los equipos de cómputo, con el fin de salvaguardarla y garantizar su disponibilidad, integridad y confidencialidad.<br><br>De otra parte, para proteger los datos que se consideran importantes y se encuentran en los medios removibles se aplica los lineamientos del Cifrado de disco. | **100** |
| AD.4.3.2 | Disposición de los medios | Se valida que previo a la disposición final de los equipos se aplica el borrado de la Información con el fin de salvaguardarla y garantizar su disponibilidad, integridad y confidencialidad. | **100** |

| | | | |
|---|---|---|---|
| | | Para la Baja y destinación final de los medios se tiene en cuenta el procedimiento GRA-TIC-PR-010 en el que se establece la secuencia de actividades para llevar a cabo la baja y determinar la destinación final de los bienes del Ministerio y/o Fondo Único TIC. | |
| AD.4.3.3 | Transferencia de medios físicos | Se valida que en el momento que se requiera transferir un medio de almacenamiento de información del Ministerio/Fondo Único de TIC a otras Entidades se debe realizar un acuerdo entre las partes<br><br>Para la transferencia de documentos que realiza gestión documental, se aplican los procedimientos Transferencia Primaria de Documentos y Transferencia Secundaria de Documentos. | **100** |
| **A17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.** | | | |
| AD.5.1.1 | Planificación de la continuidad de la seguridad de la información. | Se cuenta con un plan de continuidad de las operaciones - BCP, en el cual se definen los elementos iniciales para recuperar los procesos definidos como críticos del Ministerio, en el BCP se definen los escenarios que se pueden presentar en cuanto a fallas de la infraestructura física, ausencia de personal, fallas tecnológicas e incumplimientos de los proveedores.<br>Los siguientes documentos se relacionan al BCP:<br>Análisis de Impacto al Negocio - BIA<br>Plan de Recuperación de Desastres Tecnológicos - DRP<br>Análisis de Riesgos de Interrupción - RIA<br>Estrategias para la Continuidad de las Operaciones – MinTIC<br><br>Sin embargo y de acuerdo con los nuevos servicios y proceso que han surgido a partir de 2020, falta la actualización de estos documentos asociados al BCP. | **80** |
| **Hallazgo 1.2: Falta de actualización de los documentos asociados al Plan de Continuidad del negocio.** | | | |

Al revisar los soportes relacionados con el Plan de Continuidad de la Operaciones – BCP en el cual se definen los elementos iniciales para recuperar los procesos definidos como críticos del Ministerio, con el fin de hacer frente a una situación que interrumpa la operación normal del Ministerio ante incidentes de gran impacto, este documento se definió en el 2021 y se incluyeron los escenarios de pruebas que se han venido realizando los cuales fueron evidenciados en los informes de las pruebas que se han ejecutado al Plan de continuidad de las Operaciones – BCP como al Plan de Recuperación de Desastres – DRP; sin embargo, de acuerdo con los nuevos servicios que pueden ser críticos y algunos procesos como el caso de Arquitectura empresarial que han surgido a partir de 2020, a lo que respecta estos documentos relacionados con el BCP se encuentran desactualizados.

**VER ANEXO 1.2**

Lo anterior expuesto incumple las pruebas administrativas que comprenden el ítem AD.5.1.1 del Seguimiento Instrumento Evaluación MSPI.
Determine si el BCP aplica para procesos críticos solamente o se han incluido otros procesos o por lo menos se ha reconocido la necesidad de ampliarlo a otros procesos (para determinar el nivel de madurez)

**Recomendación.**

Se recomienda actualizar los documentos relacionados con el Plan de continuidad del negocio –BCP y Planes de Recuperación de Desastres tecnológicos – DRP.

| ID ITEM DEL INSTRUMENTO | | VALIDACIÓN | NIVEL DE CUMPLIMIENTO |
|---|---|---|---|
| AD.5.1.2 | Implementación de la continuidad de la seguridad de la información | Se valida que se cuenta con una estructura que apoya la respuesta a los incidentes asociados a la interrupción de las operaciones.<br><br>El Oficial de seguridad con el apoyo del equipo de implementadores de los temas relacionados con la seguridad de la información y los demás colaboradores implementan los planes de continuidad de operaciones y los planes de recuperación de desastres. | **100** |
| AD.5.1.3 | Verificación, revisión y evaluación de la continuidad de la seguridad de la información. | Se validó de la existencia de informes de las pruebas de continuidad, a través de la realización de estas pruebas se generan acciones correctivas y de mejora. | **100** |
| AD.5.2.1 | Disponibilidad de instalaciones de | En el documento Estrategias para la continuidad de las operaciones - BCP SPI-TIC-MA-005 se definen las | **100** |

| | | | |
|---|---|---|---|
| | procesamiento de información | estrategias de continuidad en el marco de los pilares de continuidad de Personas, Procesos, Instalaciones Físicas y Tecnológicas y Proveedores.<br><br>En la sede del Murillo Toro la Entidad cuenta con canales con redundancia con el proveedor Claro y Tigo.<br><br>La Entidad cuenta con un servicio de datacenter IFX ubicado sobre la avenida el Dorado, frente al edificio del Tiempo. | |
| **A 10. CUMPLIMIENTO** | | | |
| AD.6.1.1 | Identificación de la legislación aplicable y de los requisitos contractuales. | Se valida la identificación, documentación y cumplimiento de los requisitos legales enmarcados en la seguridad y privacidad de la información, de acuerdo con lo establecido por el gobierno nacional, para ello se dispone de una Matriz de Requisitos legales para su control y seguimiento. | **100** |
| AD.6.1.2 | Derechos de propiedad intelectual. | En la Resolución 448 de 2022 Art.17 se define la Política de Cumplimiento y en el Manual de Seguridad se establecen otros lineamientos sobre los derechos de propiedad intelectual entre los que están derechos de autor de software, licencias y código fuente. | **100** |
| AD.6.1.3 | Protección de registros. | La Entidad cuenta con las directrices sobre retención, almacenamiento, manipulación y eliminación de registros e información física y digital del Ministerio/Fondo Único de TIC; establecer e implementar controles para proteger los registros contra perdida, destrucción y falsificación de información física y digital y se encuentran definidas en los documentos asociados a las tablas de retención documental y en el manual de gestión documental. | **100** |
| AD.6.1.4 | Protección de los datos y privacidad de la información relacionada con los datos personales. | La Resolución 924 de 2020 actualiza la Política de Tratamiento de Datos Personales del Ministerio / Fondo Único de Tecnologías de la Información y las comunicaciones. | **100** |
| AD.6.1.5 | Reglamentación de controles criptográficos. | La Resolución 448 de 2022 en el Art. 8 establece la Política de criptografía, así mismo se define en el Manual de Política | **100** |

| | | | |
|---|---|---|---|
| | | de Seguridad los lineamientos para el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad e integridad de la información de la Entidad.<br><br>Entre los controles criptográficos se tienen la protección de claves de acceso a los sistemas, la clasificación de información digital, certificados digitales, cifrado de los discos duros de los equipos de cómputo de la entidad, accesos a la VPN. | |
| AD.6.2.1 | Revisión independiente de la seguridad de la información | Se cuenta con el documento lineamientos previos a la realización del ciclo de auditorías internas del sistema integrado de gestión, dentro de estas revisiones que realiza la Oficina de Control Interno se realizan Auditorías relacionadas con la seguridad de la información. | **100** |
| AD.6.2.2 | Cumplimiento con las políticas y normas de seguridad. | El Oficial de Seguridad y Privacidad de la Información revisa los requisitos legales aplicados a los sistemas de información. Así mismo en la Matriz Identificación de Requisitos Legales y de Otra Índole se definen los requisitos y/o exigencias legales asociados a los procesos de la Oficina de Tecnologías de la Información y Seguridad y privacidad de la Información. | **100** |
| AD.6.2.3 | Revisión de cumplimiento técnico. | En cuanto al cumplimiento técnico se han realizado pruebas de vulnerabilidades y se realiza el debido seguimiento. De igual manera se tiene proyectado para el 2023 realizar próximos análisis de vulnerabilidades, pent testing entre otros servicios con un nuevo proveedor. | **100** |
| **A15 RELACIONES CON LOS PROVEEDORES** | | | |
| AD.7.1 | Seguridad de la información en las relaciones con los proveedores | Para asegurar la protección de los activos de la organización que son accesibles a proveedores de la Entidad, se definen los lineamientos en la Resolución No. 0448 de 2022 y en Manual de Políticas de Seguridad. | **100** |

| | | | |
|---|---|---|---|
| AD.7.2 | Gestión de la prestación de servicios de proveedores | Los controles para el cumplimiento de los ANS en los contratos de los proveedores de la oficina de TI se establecen en el procedimiento de Gestión de proveedores y control de ANS.<br><br>El cumplimiento de la prestación de servicios de TI inicia desde la verificación de los ANS reportados por los proveedores con respecto al anexo técnico y finaliza con la certificación de cumplimiento. | **100** |

***Tabla 5. Validación y nivel de cumplimiento- Pruebas Administrativas***

| **Evaluación de efectividad** | |
|---|---|
| A.5 Políticas de Seguridad de la Información | 100 |
| A.6 Organización de la Seguridad de la Información | 100 |
| A7 Seguridad de los recursos humanos | 100 |
| A.8 Gestión de Activos | 98 |
| A17. Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio | 95 |
| A10. Cumplimiento | 100 |
| A15 Relación con los proveedores | 100 |
| **TOTAL, PROMEDIO** | **98** |

***Tabla 6. Evaluación promedio de efectividad***

La evaluación promedio de efectividad 98 se encuentra en la escala de evaluación "***Gestionado"***

**Objetivo específico 2. Realizar la evaluación de cumplimiento que le permita identificar el estado frente a los requisitos establecidos en la Norma NTC-ISO/IEC 27001:2013**

Para realizar la validación de este objetivo se tuvo en cuenta los criterios de Auditoría referenciados en la Norma NTC-ISO/IEC 27001:2013 que

proporciona el marco de trabajo para los sistemas de gestión de seguridad de la Información SGSI con el fin de proporcionar la confidencialidad, integridad y disponibilidad de la información, así como el cumplimiento legal.

Un sistema de gestión para la Seguridad de la información se compone de una serie de procesos para implementar, mantener y mejorar de forma continua la seguridad de la información tomando como base los riesgos que afectan a la seguridad de la información en una Entidad.

La Norma ISO 27002 se entiende como un inventario de buenas prácticas para la seguridad de la Información desarrollado con la experiencia de la implantación de controles para la seguridad de la información. Por lo tanto, esta norma propone una guía para implantar los controles y las medidas de seguridad.

En cuanto a la estructura de la norma, la ISO 27001 se compone de 14 dominios, 35 objetivos de control y 114 controles.

Para este objetivo específico 2 se revisaron los dominios A9, A10, A11, A12, A13, A14 y A16.

A.9 Control de Acceso
A.10 Criptografía
A.11 Seguridad Física y del Entorno
A.12 Seguridad de las Operaciones
A.13 Seguridad en la Comunicaciones
A.14 Adquisición, desarrollo y mantenimiento de sistemas
A.16 Gestión de incidentes de seguridad de la información.

Cabe resaltar que estos dominios también hacen parte del instrumento de evaluación del MSPI del componente **Pruebas Técnicas**.

Para la validación y determinar el nivel de cumplimiento de este objetivo 2 se tuvo en cuenta los dominios de la ISO27001:2013.

| ISO27001:2013 | | VALIDACIÓN | NIVEL DE CUMPLIMIENTO |
|---|---|---|---|
| **A.9 CONTROL DE ACCESO** | | | |
| **A.9.1** Requisitos | **Objetivo:** Limitar el | Referente a este objetivo Mintic estable en la Resolución 448 de 2022 Art 7 la | |

| | | | |
|---|---|---|---|
| del negocio para control de acceso | acceso a información y a instalaciones de procesamiento de información. | Política de Control de Acceso y en el Manual de Políticas de Seguridad y Privacidad de la Información se definen los lineamientos para controlar el acceso a la información.<br><br>Cada sistema de información tiene un líder funcional, para requerir el acceso a las aplicaciones, este se realiza mediante el paquete OTI.<br><br>Para la administración de acceso a redes y a servicios de red de los funcionarios y contratistas, la Oficina de TI dispone del lineamiento Gestión de Usuarios y Perfiles para el acceso a los Recursos.<br>Para el caso de la creación de los usuarios de administración de recursos de TI, se requiere la autorización del jefe de la Oficina de TI en primera instancia, el Oficial de Seguridad o quien haga sus veces como segunda instancia o la dimensión de seguridad informática como tercera instancia.<br><br>Las solicitudes para la VPN se realizan de acuerdo con el formato Solicitud de VPN site o site. | **100** |
| **A.9.2** Gestión de acceso de usuarios | **Objetivo:** Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios. | Para asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a los sistemas de información y demás servicios, Mintic realiza la administración de manera segura de los accesos a recursos de TI y su asignación para el uso de todos los servicios informáticos dispuestos por la Oficina de TI del Ministerio de Tecnologías de la Información y las Comunicaciones, para lo anterior se cuenta con el procedimiento Gestión de Usuarios y Perfiles para el acceso a Recursos.<br><br>La solicitud de creación de un usuario llega a través de la mesa de ayuda mediante el paquete OTI con los accesos requeridos a nivel de acceso al | **80** |

| | | | |
|---|---|---|---|
| | | dominio, vpn, correo y a algunos sistemas de información.<br><br>La modificación de un perfil de usuario se da cuando se presentan cambios de área, cargo, funciones o roles de funcionarios, contratistas o terceros de su dependencia y se debe hacer la solicitud de las modificaciones de acceso requeridas.<br><br>La Inactivación / activación de un perfil de usuario se da cuando se tiene la certeza de que un funcionario, contratista o tercero cesa sus actividades de manera permanente para ello, se debe solicitar la inactivación de los accesos de todos aquellos recursos de TI que le fueron asignados, o cuando ya no necesite tener acceso a determinado recurso de TI por vacaciones, licencias de maternidad, licencias no remuneradas, cambios de área, cargo, funciones o roles, suspensión de contratos y otras novedades.<br><br>No obstante, en la validación que se realizó se encontraron funcionarios y contratistas que ya no laboran en la Entidad pero que no han sido retirados del Directorio Activo. | |

**Hallazgo 2.1: funcionarios y contratistas que ya no laboran en la Entidad y aun siguen activos en el Directorio Activo.**

Se realizó la validación de los archivos suministrados con el listado de funcionarios y contratistas que ya no laboran en la Entidad. El periodo de revisión fue del 01 de enero 2023 al 20 mayo 2023 y se encontraron (145) funcionarios y (17) contratistas retirados durante dicho periodo.

En respuesta dada, al revisar y validar esta información con base en el archivo suministrado por la Oficina GIT de Servicios tecnológicos se identificaron (2) usuarios que no han sido notificados con la novedad y por ende aún están activos en el Directorio Activo.

**VER ANEXO 2.1**

Lo anterior expuesto incumple la norma ISO 27001:2013 en el dominio A.9.2.6 Retiro o ajuste de los derechos de acceso.
*Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se han cambios.*

**Recomendación.**

Se recomienda fortalecer los controles para mitigar posibles accesos no autorizados en los sistemas de información cuando los funcionarios y contratistas se desvinculan de la Entidad.

| ISO27001:2013 | | VALIDACIÓN | NIVEL DE CUMPLIMIENTO |
|---|---|---|---|
| **A.9.3** Responsabilidades de los usuarios | **Objetivo:** Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación. | Referente a esta descripción se revisó que en el Manual de Políticas de Seguridad y privacidad de la información se definen lineamientos para que los usuarios salvaguarden sus credenciales de acceso a los servicios de la Entidad.<br><br>Se verifico que en el Directorio Activo se tiene configuradas las políticas para el bloqueo de contraseñas, complejidad y tiempo de expiración de las contraseñas. | **100** |
| **A.9.4** Control de Acceso a Sistemas y Aplicaciones | **Objetivo:** Evitar el acceso no autorizado a sistemas y aplicaciones | Para evitar el acceso no autorizado a sistemas y aplicaciones Mintic se tiene definido en el Manual de políticas de seguridad y privacidad de la información los lineamientos para prevenir el acceso no autorizado a sistemas y aplicaciones y servicios de la Entidad.<br><br>Desde el Directorio Activo se tiene la configuración de las políticas para el bloqueo de contraseñas, complejidad y tiempo de expiración de las mismas, lo anterior para controlar el acceso a sistemas y aplicaciones.<br><br>Del uso de programas utilitarios privilegiados ningún funcionario cuenta con permisos de administrador local de su computador para realizar instalación de software sin autorización.<br><br>La Oficina de Tecnologías de la Información monitorea los administradores de los recursos | **100** |

| | | | |
|---|---|---|---|
| | | tecnológicos y servicios de red, para que no hagan uso de programas utilitarios que permitan acceso a los sistemas operativos, firmware o conexión a las bases de datos para anular la seguridad de los sistemas de información alojados sobre la plataforma tecnológica.<br><br>De otra parte, la Oficina de Tecnologías de la Información cuenta con un listado de programas utilitarios privilegiados de la plataforma tecnológica, los servicios de red y sistemas de información autorizados.<br><br>En cuanto al acceso al código fuente de los programas este es limitado, el acceso se da para los ingenieros desarrolladores y de soporte que sean autorizados de la Oficina de Tecnologías de la Información. | |
| **A.10 CRIPTOGRAFIA** | | | |
| **A.10.1** Controles Criptográficos | **Objetivo:** Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información. | Referente a esta descripción se define en la Resolución 448 de 2022 Art 8. La Política Criptografía y en el Manual de Políticas de Seguridad y Privacidad de la Información se establece los lineamientos de seguridad para el uso de recursos criptográficos.<br><br>Por lo anterior se cuenta con protección de claves de acceso a los sistemas, clasificación de información digital, certificados digitales, cifrado de los discos duros de los equipos de cómputo de la entidad, acceso VPN entre otros. | **100** |
| **A.11 SEGURIDAD FISICA Y DEL ENTORNO** | | | |
| **A.11.1** Áreas seguras | **Objetivo:** Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento | Referente a esta descripción se define en la Resolución 448 de 2022 Art 10. Política de Seguridad física y del Entorno y en el Manual de Políticas de Seguridad y Privacidad de la Información se establece los lineamientos para prevenir el acceso físico no autorizado, el daño e interferencia de la información e instalaciones de procesamiento de información de la Entidad. | **100** |

| | | | |
|---|---|---|---|
| | de información de la organización. | La sede donde funciona el MinTIC es un edificio que se compone de un sótano y siete pisos distribuidos así: Sótano: Auditorio, parqueaderos, área de servicios de personal de apoyo, cuarto de transformadores, cuarto técnico (equipos de comunicaciones), garita de control, cuarto de bombas de inyección del edificio, bodegas y cuarto de control de incendios, además de contar con servicios de vigilancia, sistema de detección de incendios y extinción, brigadas de emergencia<br><br>Para las áreas seguras de tecnologías, específicamente los cuartos de cableado y el centro de datos, la Entidad cuenta con control de acceso biométrico o por proximidad del carnet institucional.<br><br>Para registrar el acceso a cada una de las áreas seguras de tecnologías, se cuenta con el formato GTI-TIC-FM-016 Control de Acceso - Áreas seguras de tecnologías. | |
| **A.11.2** Equipos | Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización | Para prevenir la perdida, daño, robo o compromiso de los equipos, la Entidad cuenta con CCTV para cada uno de los pisos y tiene una cobertura sobre las áreas de cada una de las dependencias de la entidad, incluido el sótano del edificio Murillo Toro y el centro de cómputo principal.<br><br>Para los equipos proporcionados por la Entidad se suministra guayas.<br><br>De los servicios de suministro se cuenta con la planta eléctrica, la disposición de los puntos de energía regulada y no regulada. Su mantenimiento se lleva a cabo mediante la ejecución del contrato de mantenimiento de instalaciones técnicas.<br><br>Para la seguridad del cableado se tienen instaladas canaletas que separan la red eléctrica de la red de cableado | **60** |

| | | | |
|---|---|---|---|
| | | estructurado, además se realiza mantenimiento técnico de las instalaciones teniendo en cuenta las consideraciones técnicas de las normas vigentes y el Reglamento Técnico de Instalaciones Eléctricas RETIE.<br><br>Del mantenimiento de equipos se cuenta con un contrato estatal de prestación de servicios con el proveedor COLSOF S.A el cual provee los servicios para escáneres, equipos de cómputo, impresiones, videoproyectores dentro de las obligaciones especificas se incluye:<br><br>-Rendir mensualmente al supervisor los informes técnicos y de gestión dentro de los 10 primeros días hábiles del mes, indicando los niveles de servicio obtenidos con sus respectivos soportes o los informes especiales que se le requieran.<br><br>-Realizar mantenimientos preventivos anuales y los correctivos necesarios durante la ejecución del contrato formalizando cada vez a través de acta firmada por el contratista y por el supervisor del contrato<br><br>Del retiro de activos se define en el Manual de Uso de Instalaciones físicas V7 GRA-TIC-MA-001 los lineamientos para el retiro de equipos.<br><br>En el Manual de Políticas de Seguridad de la Información se definen lineamientos de la seguridad de los equipos y los activos fuera de las instalaciones.<br><br>Para la disposición segura o reutilización de equipos se estableció un mecanismo de borrado seguro de información para los equipos que se van a dar de baja.<br><br>Para los Equipos de usuario desatendidos desde la Oficina de | |

| | | | |
|---|---|---|---|
| | | Tecnología de Información se implementa el bloqueo de pantallas de los computadores automáticamente y que estén en el dominio. De lo contrario si no están en el dominio los colaboradores del Ministerio/Fondo Único de TIC, deben bloquear la pantalla del computador a su cargo cuando se ausenten de su puesto de trabajo, para impedir el acceso de terceros no autorizados a la información almacenada en el equipo de cómputo.<br><br>Se verifico durante los recorridos que tanto funcionarios como contratistas aplican la política de escritorio limpio.<br><br>No obstante, en los recorridos realizados fue identificado la inadecuada ubicación del aire acondicionado en el centro de cómputo y fallas en la seguridad del cableado de los racks del centro de cómputo. | |

**Hallazgo 2.2: Inadecuada ubicación del airea acondicionado en el centro de cómputo, ocasionando bastante ruido y alto consumo de energía.**

Se realizo una inspección física en las instalaciones del MINTIC para revisar y verificar las condiciones del aire acondicionado en el centro de cómputo, se observó la adecuación de un aire portátil para el control de temperatura, sin embargo, no es una opción eficiente ya que está ocupando un espacio transitable dentro y fuera del centro cómputo, además de ocasionar bastante ruido y consumo de energía alto.

***Figura 1. Aire acondicionado***

De otra parte, ocasiona el impedimento de mantener la puerta cerrada del centro de cómputo.


***Figura 2. Aire acondicionado impide mantener la puerta cerrada***

Lo anterior expuesto incumple la norma ISO 27001:2013 en el dominio A.11.2.2 Servicio de suministro.
*Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.*

**Recomendación.**

Se recomienda diseñar, adquirir, instalar y poner en funcionamiento un buen sistema de aire acondicionado en el centro de cómputo del MINTIC/ Fondo Único de TIC que permita la conservación, disponibilidad y buen funcionamiento de los servidores y equipos de almacenamiento, red, seguridad y comunicaciones.

**Hallazgo 2.3: Fallas en la seguridad del cableado de los racks de comunicaciones ubicados en el centro de cómputo principal.**

Se realizo una inspección física en las instalaciones del MINTIC para revisar y verificar las condiciones de la seguridad del cableado, se observó que el cableado del racks del centro de cómputo principal se encuentra en desorden lo que puede ocasionar desconexiones involuntarias de los diferentes equipos, intermitencias en la conectividad y posibles accidentes.

***Figura 3. Cableado de los racks***

Lo anterior expuesto incumple la norma ISO 27001:2013 en el dominio A.11.2.3 Seguridad del cableado.
*Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación. Interferencia o daño.*

**Recomendación.**

Se recomienda implementar controles para la organización y peinado del cableado que se encuentra ubicado en el centro de cómputo principal.

| **A.12 SEGURIDAD DE LAS OPERACIONES** | | | |
|---|---|---|---|
| **A.12.1** Procedimientos operacionales y responsabilidades | **Objetivo:** Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información. | Los procedimientos de operación establecen lineamientos para asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información de la Entidad.<br><br>Entre los procedimientos operacionales que se encuentran publicados en la plataforma SIMIG se tienen:<br><br>GTI-TIC-PR-033 Actualización de Sistemas Operativos<br>GTI-TIC-PR-005 Respaldo, Retención y Restauración de Información<br>GTI-TIC-MA-018 Lineamientos para la recepción o desarrollo de servicios tecnológicos y sistemas<br>SPI-TIC-PR-001 Gestión de incidentes de seguridad y privacidad de la información que definen el contacto con las autoridades | **100** |

| | | | |
|---|---|---|---|
| | | GTI-TIC-IN-033 BORRADO DE INFORMACIÓN<br>GTI-TIC-PR-019 Administrar la operación Gestión de Problemas<br>GTI-TIC-MA-020 Gestión de Incidentes<br>GTI-TIC-PR-021 Administrar la Operación Gestión de Requerimientos e Incidentes<br>GTI-TIC-PR-032 Monitoreo<br><br>Para la administración y control sobre los requerimientos de cambios normales y de emergencia que surgen a partir de las necesidades de mantenimiento y actualización de los servicios de TI, se realizan en base al Manual de Gestión de Cambios.<br>La Entidad gestiona la capacidad y la revisión de las capacidades instaladas tanto de la nube privada, plataforma de comunicaciones y la plataforma de seguridad. | |
| **A.12.2** Protección contra códigos maliciosos | **Objetivo:** Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos. | La Entidad cuenta con la protección contra códigos maliciosos que protege a servidores físicos, virtuales y equipos de cómputo. | **100** |
| **A.12.3** Copias de Respaldo | **Objetivo:** Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de | La Entidad asegura la información gestionada en las plataformas tecnológicas y sistemas de información través de la nube híbrida del Ministerio TIC mediante la Oficina de TI, para que permanezca respaldada y sea recuperable en el momento que se requiera. Para ello se cuenta con el procedimiento GTI-TIC-PR-005 Respaldo, Retención y Restauración de información. | **100** |

| | | | |
|---|---|---|---|
| | copias de respaldo acordadas. | | |
| **A.12.4** Registro y Seguimiento | **Objetivo:** Registrar eventos y generar evidencia. | La Entidad realiza la detección, clasificación y dimensión de los eventos que se presenten en los servicios TIC, lo anterior mediante el procedimiento GTI-TIC-PR-020 Administrar la Operación Gestión de Eventos.<br><br>La secuencia de actividades para realizar el monitoreo de las plataformas tecnológicas de la Entidad se define en el procedimiento GTI-TIC-PR-032 Monitoreo.<br><br>El administrador de las plataformas realiza las correcciones de las condiciones anormales y restauración de la operación normal.<br><br>Mediante las herramientas de monitoreo se realiza la configuración y parametrización de las alertas generadas detectadas en condiciones anormales o que superen los umbrales establecidos.<br><br>La sincronización de los relojes está configurada con la hora legal Republica de Colombia https://horalegal.inm.gov.co/ garantizando la exactitud de los registros de auditoría. | **100** |
| **A.12.5** Control de Software Operacional | **Objetivo:** Asegurarse de la integridad de los sistemas operacionales. | La Entidad controla el uso de software autorizado, se restringe la instalación de software y control de panel de control bloqueado. | **100** |
| **A.12.6** Gestión de la Vulnerabilidad Técnica | **Objetivo:** Prevenir el aprovechamiento de las vulnerabilidades técnicas. | La Entidad realiza el análisis de vulnerabilidades y Ethical Hacking con el fin de fortalecer y asegurar la disponibilidad de los servicios tecnológicos. La oficina de TI realiza el seguimiento a la remedición de estas vulnerabilidades | **100** |

| | | | |
|---|---|---|---|
| | | Se establece en el manual de políticas de seguridad los lineamientos para las restricciones y las reglas para la instalación de software por parte de los usuarios, para la autorización de software se debe diligenciar el formato GTI-TIC-FM-007 Solicitud de Autorización de Software. | |
| **A.13 SEGURIDAD DE LAS COMUNICACIONES** | | | |
| **A.13.1** Gestión de la Seguridad de las Redes | **Objetivo:** Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte. | La Entidad cuenta con perímetros de seguridad mediante la creación de (2) firewalls virtuales, se incluye el soporte, antivirus, control de navegación y control de aplicaciones.<br><br>Se tiene una segmentación de VLANS cableada e inalámbrica.<br><br>Se establece la segmentación de redes y listas de acceso a los servicios del Ministerio/Fondo Único de TIC tales como servidores, administración e invitados. | **100** |
| **A.13.2** Transferencia de Información | **Objetivo:** Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa. | Se define en la Resolución 448 de 2022 en el Articulo 12 la Política de seguridad de las comunicaciones los lineamientos para la transferencia de información, así mismo en el manual de seguridad se establecen otros lineamientos para mantener la seguridad de la información transferida dentro del Ministerio/Fondo Único de TIC y con cualquier entidad externa.<br><br>El intercambio de información se realiza mediante el documento técnico denominado acuerdo de intercambio y confidencialidad de la información entre la Entidad y el MINTIC.<br><br>Todo empleado público o contratista debe firmar el documento o compromiso de confidencialidad y no divulgación de la información con el Ministerio/Fondo Único de TIC. | **100** |
| **A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS** | | | |

| | | | |
|---|---|---|---|
| **A.14.1** Requisitos de Seguridad de los sistemas de información | **Objetivo:** Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas. | La Entidad identifica y recibe las solicitudes y necesidades de los requerimientos que tienen los lideres funcionales sobre los sistemas de información de los cuales son responsables, el alcance inicia con la recepción y estudio de las solicitudes o requerimientos y finaliza con la aprobación de los documentos requeridos para dar inicio al desarrollo.<br><br>Mediante el formato solicitud ajuste o requerimiento de software, se detalla la descripción de la nueva solución o mantenimiento a desarrollar, el objetivo, la justificación, el alcance, los criterios de aceptación y la descripción detallada de los requerimientos.<br><br>De otra parte, para la recepción o desarrollo de servicios tecnológicos y sistema se tiene en cuenta el lineamiento GTI-TIC-MA-018**,** en el que se establece que las aplicaciones deben contar con características de seguridad entre las que se incluye permitir la administración de roles, perfiles, usuarios, permisos y niveles de acceso a las diferentes funcionalidades de sus componentes y datos. | **100** |
| **A.14.2** Seguridad en los procesos de desarrollo y de soporte | **Objetivo:** Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información. | En la Resolución 448 de 2022 se define la Política de seguridad para la adquisición, desarrollo y mantenimiento de sistemas; la Oficina de Tecnologías de la Información verifica que los desarrollos internos y externos de los sistemas de información, cumplan con los requerimientos de seguridad adecuados para la protección de la información del Ministerio/Fondo Único de TIC, para lo cual, establecerá una metodología que detalle los requerimientos de seguridad para el desarrollo, pruebas, puesta en producción y mantenimiento de los sistemas de información. | **100** |

| | | | |
|---|---|---|---|
| | | Para la gestión de cambios en los sistemas se cuenta con un formato de solicitud ajuste o requerimiento de software donde se detalla la descripción de la nueva solución o mantenimiento a desarrollar.<br><br>El comité de cambios se realiza los días martes y jueves. | |
| **A.14.3** Datos de Prueba | **Objetivo:** Asegurar la protección de los datos usados para pruebas. | Mediante la herramienta de ofuscamiento de datos la Entidad proteger los datos sensibles de acuerdo con la normatividad colombiana. | **100** |
| **A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN** | | | |
| **A.16.1** Gestión de incidentes y mejoras en la seguridad de la Información | **Objetivo:** Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades | La Entidad realiza la gestión de incidentes y eventos de seguridad y privacidad de la información, seguridad digital siguiendo los siguientes lineamientos.<br><br>-Procedimiento gestión de incidentes de seguridad y privacidad de la información<br>-Formatos incidentes de seguridad y privacidad de la Información<br>-Formato de recolección de evidencias digitales<br><br>Mediante las sensibilizaciones que se vienen realizando se informan de los canales para reportar los incidentes como lo son:<br><br>-Correo electrónico a la cuenta mesadeservicios@mintic.gov.co<br>-mensaje a través de la herramienta teams: mesadeservicio<br>-Modulo del portal servicios TIC serviciosti.mintic.gov.co<br>-Mesa de Servicio ext. 3300<br><br>La categoría de los incidentes se asigna para especificar la línea de servicio con la que está relacionado el incidente, el tipo de producto que está asociado, el | **100** |

| | | | |
|---|---|---|---|
| | | tipo de problema y la posible causa. Para asignar la categoría se deben seleccionar los siguientes campos de manera obligatoria en la herramienta: Clasificación, Subcategoría y Detalle.<br><br>El impacto y la urgencia se asigna para calcular la prioridad del incidente y de esta manera ser atendido. | |

***Tabla 7. Validación y nivel de cumplimiento- ISO27001:2013***

| **Evaluación de Efectividad – ISO 27001: 2013 PRUEBAS TECNICAS** | |
|---|---|
| A.9 Control de Acceso | 95 |
| A.10 Criptografía | 100 |
| A.11 Seguridad física y del entorno | 80 |
| A.12 Seguridad de las Operaciones | 100 |
| A.13 Seguridad de las comunicaciones | 100 |
| A.14 Adquisición, desarrollo y mantenimiento de sistemas | 100 |
| A.16 Gestión de incidentes de seguridad de la Información | 100 |
| **TOTAL, PROMEDIO** | **96,4** |

***Tabla 8. Evaluación promedio de efectividad***

La evaluación promedio de efectividad 96,4 se encuentra en la escala de evaluación "***Gestionado"***

**Objetivo específico 3. Validar el estado de la implementación de la seguridad y privacidad de la información en base a los lineamientos de la Política General de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad de la Operación del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones.**

Para realizar la validación de este objetivo se tuvo en cuenta el marco de la Resolución 448 de 2022 Capitulo II Políticas específicas de manejo de información y el Manual de Políticas de Seguridad y Privacidad de la Información V4 SPI-TIC-MA-001.

La Resolución aplica a todos los niveles funcionales y organizacionales del Ministerio/Fondo Único de TIC, a todos sus funcionarios, contratistas, proveedores, operadores, entidades adscritas y del sector de las Tecnologías de la Información y las Comunicaciones, así como aquellas personas o terceros que en razón del cumplimiento de sus funciones y las del Ministerio de TIC compartan, utilicen, recolecten, procesen, intercambien o consulten su información, al igual que a las entidades de control y demás entidades relacionadas que accedan, ya sea interna o externamente a cualquier activo de información, independientemente de su ubicación.

El Manual de Políticas de Seguridad y Privacidad de la Información establece los lineamientos para la adecuada gestión de la seguridad y privacidad de la información en el Ministerio/Fondo Único de TIC, enmarcados en la implementación de un Sistema de Gestión de Seguridad de la Información y se encuentra publicada en el Sistema Integrado de Gestión- ISOLUCION.

El listado maestro de los documentos que hacen parte de la implementación de la seguridad y privacidad de la información se encuentran aprobados, vigentes y publicados en la aplicación ISOLUCION.

Para la validación de este objetivo se tomó como muestra (5) lineamientos de los 15 artículos del Capítulo II **Políticas específicas de manejo de información** que contiene de la Resolución 448 de 2022 y (5) lineamientos de los 15 principios orientados a la seguridad de la información que contiene el Manual de Políticas de Seguridad y Privacidad de la Información.

Se hizo la validación de cómo está siendo implementado cada lineamiento y la existencia de los documentos en SIMIG que lo apoyan para el cumplimiento de los mismos.

El periodo analizado de la documentación de registros, procedimientos y manuales de este objetivo específico 3, comprende desde el 2021 hasta el 2023.

| RESOLUCIÓN 448 DE 2022 | Lineamiento de la Resolución 448 de 2022 | Validación del lineamiento | Documento SIMIG | Versión y fecha aprobación | Cumple/No cumple/Cumple parcialmente |
|---|---|---|---|---|---|
| | Los activos de información deben ser identificados, clasificados, valorados y controlados para garantizar su uso, protección y recuperación ante desastres. | Se cuenta con el Manual de Activos de Información donde se definen los criterios básicos para la identificación, clasificación y valoración de activos de información del Ministerio/Fondo Único de TIC.<br><br>Se valido el registro de los activos de información que se encuentran publicados en octubre del 2022 en la plataforma del SIMIG y la página web (transparencia y acceso a la información pública datos abiertos). | GDO-TIC-MA-014 Manual de Activos de Información | V5-08/mar./2023 | **Cumple** |
| | | | GDO-TIC-PR-019 Procedimiento de Activos de Información | V5 08/mar./2023 | |
| | | | GDO-TIC-DI-020 Consolidado activos de la información MinTIC | V3 13/oct./2022 | |
| | Se deberá establecer medidas de control de acceso a nivel de red, sistema operativo, sistemas de información, servicios de tecnologías e infraestructura física. | Cada sistema de información tiene un líder funcional, para requerir el acceso a las aplicaciones, este se realiza mediante el paquete OTI.<br><br>La oficina de TI dispone de los lineamientos para la gestión de usuarios y perfiles para la administración de acceso a las redes y a servicios de red de los funcionarios y contratistas. | GTI-TIC-PR-007 Gestión de usuarios y perfiles para el acceso a recursos TI | V6 22/Ago/2022 | **Cumple** |

| | | | | | |
|---|---|---|---|---|---|
| **RESOLUCIÓN 448 DE 2022** | Se deberá establecer controles necesarios para la protección de la información de los empleados públicos, contratistas y partes interesadas externas, en los términos de la Ley 1581 de 2012 y sus decretos reglamentarios, así como la política de tratamiento de datos personales del Ministerio/Fondo Único de TIC. | Para la protección de la información de los empleados públicos, contratistas y partes interesadas se cuenta con la autorización expresa de recolección de datos personales el cual debe ser diligenciado por el funcionario o contratista además se les informa sobre la Política de tratamiento de datos personales. | SPI-TIC-FM-001 Autorización expresa de recolección y tratamiento de datos personales. | V3 23/abr./2021 | **Cumple** |
| | Se deberá velar por la identificación, documentación de los requisitos legales, entre ellos los referentes a derechos de autor y propiedad intelectual | Se establece en los contratos con los proveedores los controles para proteger adecuadamente la propiedad intelectual del Ministerio/Fondo Único de TIC, tales como derechos de autor de software, licencias y código fuente. | GTI-TIC-FM-007 Solicitud de Autorización de Software | V2 22/Oct/2021 | **Cumple** |
| | Los empleados públicos, contratistas y visitantes que se encuentren en las instalaciones físicas del Ministerio de Tecnologías de la Información y las Comunicaciones | Se valido durante la revisión al centro de cómputo que tanto los empleados públicos como los contratistas portan el carné de manera visible. | GRA-TIC-MA-001 Manual de Uso de Instalaciones Físicas | V7-18/jul./2022 | **Cumple** |

| | | | | | |
|---|---|---|---|---|---|
| | deben estar debidamente identificados, el carné, documento o distintivo que acredite su tipo de vinculación, en caso de carné debe portarse en un lugar visible. | | | | |

***Tabla 9. Validación de lineamientos – Resolución 448 de 2022***

| **MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN SPI-TIC-MA-001 V4** | **Lineamiento del Manual de Políticas de seguridad y privacidad de la información** | **Validación del lineamiento** | **Documento SIMIG** | **Versión y fecha aprobación** | **Cumple/No cumple/Cumple parcialmente** |
|---|---|---|---|---|---|
| | Revisar la documentación necesaria que se brinde a las dependencias la orientación con respecto a la autorización, configuración y uso de los dispositivos móviles de propiedad de empleados públicos, contratistas o terceros que requieran tener acceso a la información a través de los servicios tecnológicos del Ministerio/Fondo Único de TIC. | La oficina de tecnologías de información brinda a las dependencias la orientación para la aprobación y la configuración para el uso de los dispositivos móviles, aplicando la Política de trae tu propio dispositivo.<br><br>Para los funcionarios y contratistas se aplica el consentimiento informando de la participación de la iniciativa trae tu propio dispositivo TTPD. | GTI-TIC-MA-012 Manual de Política Trae tu Propio Dispositivo | V3-22/Oct/2021 | **Cumple** |
| | | | GTI-TIC-PR-030 Trae Tu Propio Dispositivo | V2-22/Oct/2021 | |
| | | | GTI-TIC-FM-009 Consentimiento Informado | V4-10/Sep/2021 | |
| | Revisar el mecanismo de verificación del | Gestión del Talento Humano aplica el procedimiento para el | GTH-TIC-FM-031 Estudio | V4-10/Dic/2021 | **Cumple** |

| | | | | | |
|---|---|---|---|---|---|
| | personal en el momento en que se postula al cargo. Dicho mecanismo deberá incluir los aspectos legales y procedimentales de vinculación del Ministerio/Fondo Único de TIC. | Ingreso de funcionarios de Libre Nombramiento y Remoción y provisionalidad y el de Nombramiento de cargos de carrera administrativa. Para ambos casos se establece la verificación de cumplimiento de requisitos a través del Estudio Técnico de Requisitos. | técnico de requisitos. | | |
| | | | GTH-TIC-PR-001 Ingreso de los funcionarios de Libre Nombramiento y Remoción y Provisionalidad. | V12-04/nov./2022 | |
| | | | GCC-TIC-MA-003 Manual de Contratación | V4-25/mar./2021 | |
| | | | GTH-TIC-FM-053 Compromiso de confidencialidad de información-funcionario y para contratistas | V3-07/dic./2022 | |
| | | | GCC-TIC-FM-046-Estudio Previo Convenio Interadministrativo | V5-05/feb./2020 | |
| | Todos los puntos de acceso deberán tener un área de recepción con vigilancia u otro medio para controlar el acceso físico al sitio o instalación | La sede donde funciona el MinTIC es un edificio que se compone de un sótano y siete pisos distribuidos así: Sótano: Auditorio, parqueaderos, área de servicios de personal de apoyo, cuarto de | GRA-TIC-MA-001 Manual de Uso de Instalaciones Físicas | V7-18/jul./2022 | **Cumple** |
| | | | SPI-TIC-FM-006 Identificación áreas | V1-03/may./2021 | |

| | | | | | |
|---|---|---|---|---|---|
| | | transformadores, cuarto técnico (equipos de comunicaciones), garita de control, cuarto de bombas de inyección del edificio, bodegas y cuarto de control de incendios, además de contar con servicios de vigilancia, sistema de detección de incendios y extinción, brigadas de emergencia<br><br>Para las áreas seguras de tecnologías, específicamente los cuartos de cableado y el centro de datos, la Entidad cuenta con mecanismo de acceso biométrico o por proximidad del carnet institucional. | seguras Mintic | | |
| | | | SPI-TIC-DI-013 Consolidado Área Segura | V3-08/nov./2022 | |
| | | | GTI-TIC-FM-017 Solicitud de activación tarjeta de acceso áreas seguras de tecnologías | V3-13/sept./2022 | |
| | Revisar los controles para proteger la información que se transmite como documentos adjuntos a través del correo electrónico del Ministerio/Fondo Único de TIC. | Para el intercambio de información se cuenta con un documento técnico denominado acuerdo de intercambio y confidencialidad de la información entre la Entidad y el MINTIC esto con el objeto de especificar las características técnicas y mínimos semánticos de la información que será compartida entre las partes o el mecanismo que usaran para el intercambio y las consideraciones | SPI-TIC-FM-010 Acuerdo de intercambio de información. | V1-28/Dic/2022 | **Cumple** |
| | | | SPI-TIC-FM-009 Compromiso de confidencialidad y no divulgación para el intercambio de información | V1-06/Dic./2022 | |

| | | | | | |
|---|---|---|---|---|---|
| | | sobre la seguridad y la protección de los datos personales. | | | |
| | Revisar el mecanismo para la gestión de incidentes de seguridad de la información. | Para el reporte de los incidentes de seguridad de la información se aplica el procedimiento de gestión de incidentes de seguridad y privacidad de la información para la oportuna identificación, atención y respuesta de los incidentes con el fin de mitigar el impacto asociado a la pérdida de la confidencialidad, integridad y disponibilidad de la información del Ministerio/Fondo Único de Tecnologías de la información y comunicaciones.<br><br>Los canales para reportar los incidentes son:<br><br>-Correo electrónico a la cuenta mesadeservicios@mintic.gov.co<br>-Mensaje a través de la herramienta teams mesadeservicio<br>-Modulo del portal servicios TIC serviciosti.mintic.gov.co<br>-Mesa de Servicio ext 3300 | SPI-TIC-PR-001 Gestión de incidentes de seguridad y privacidad de la información | V2-23/Jun/2022 | **Cumple** |
| | | | SPI-TIC-FM-004 Formato de recolección de evidencias digitales | V1 05/abr./2021 | |

***Tabla 10. Validación lineamientos – Manual de Políticas de Seguridad y Privacidad de la Información***

Del listado maestro y la validación de la implementación de estos documentos asociados a la seguridad y privacidad de la información cumplen con los requisitos que establece la Resolución 448 de 2022 y el Manual de Políticas de Seguridad de la Información.

**Objetivo específico 4. Evaluar los planes de acción que se han establecido, para llevar a cabo el cierre de las brechas identificadas orientados a dar cumplimiento a la norma; en el marco de estándares y buenas prácticas generalmente aceptadas**.

El periodo analizado de la documentación de registros, procedimientos y manuales de este objetivo específico 4, comprende desde el 2020 hasta el 2023.

**Plan de Continuidad de la Operación para el Ministerio TIC – BCP.**

El Ministerio de Tecnologías de la Información y las Comunicaciones, según la Ley 1341 o Ley de TIC, es la Entidad que se encarga de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones.

Propendiendo por garantizar la prestación de servicios con calidad y seguridad se da la necesidad de realizar el Plan de Continuidad de la operación de los servicios en el cual se determinen las estrategias para llevar a cabo la operación en contingencia y lograr recuperar los servicios críticos de la Entidad en tiempos óptimos, después de una interrupción no deseada o desastre, mitigando la perdida de información, impacto financiero, credibilidad y productividad, basados en los procesos críticos de las áreas misionales y su relación operativa con los procesos estratégicos, de apoyo del Ministerio.

Por lo anterior en el año 2020 la Entidad realizó una consultoría al Plan de Continuidad de la Operación para el Ministerio TIC – BCP, producto de esta consultoría se obtuvieron unos entregables, teniendo en cuenta los siguientes criterios de selección:

- ✓ Análisis de Impacto a la Operación
- ✓ Gestión de Riesgos
- ✓ Estrategias para la Continuidad de negocio (BCP)
- ✓ Plan de Recuperación de Desastres (DRP)

- ✓ Pruebas de Escritorio y Escenarios controlados bajo simulación de Continuidad de la Operación de los Servicios.

A continuación, se presenta un análisis sobre las entregas realizadas de acuerdo con los objetivos de cada uno de los criterios que se definieron en el Anexo Técnico 2020 Plan de Continuidad de la Operación para el Ministerio TIC – BCP.

| Objetivo | Entregable | Validación del entregable | Cumple/No cumple/Cumple parcialmente |
|---|---|---|---|
| **Análisis de Impacto a la Operación** | | | |
| Realizar la Identificación de los procesos críticos misionales del MINTIC e identificación el impacto frente a la interrupción en un peor escenario. | Informe de Análisis de Impacto al Negocio - BIA | Resultado del análisis del entregable se identificaron 18 procesos que tuvieron criticidad mayor y son indispensables para la continuidad de las operaciones. | **Cumple** |
| Realizar la identificación del impacto operacional asociado a una interrupción o incidente interno o externo pueda afectar negativamente los procesos misionales de la Entidad. | Informe de Análisis de Impacto al Negocio - BIA | Resultado del análisis del entregable se definieron las diferentes categorías y análisis de impactos (legal, operacional, participación ciudadana, reputacional y financiero) | **Cumple** |
| **Gestión de Riesgos** | | | |
| Realizar la identificación los posibles Riesgos (amenazas, vulnerabilidades, controles e impactos) que podrían ocasionar interrupciones e impactar la operación normal. | Documento con el contenido que relaciona los siguientes ítems: -Actualización y alineación de la metodología de riesgos de la Entidad con BCP | Resultado del análisis del entregable se definieron 24 matrices de riesgos de interrupción, se encuentran alineados con la metodología de riesgos y cuentan | **Cumple** |

| | | | |
|---|---|---|---|
| | -Entrevistas con listados de verificación,<br>-Matriz de riesgos<br>-Matriz con el mapa de calor (calificación de controles)<br>-Plan de acción o remediaciones y Matriz de resultados. | con los memorandos de aceptación de los riesgos. | |
| **Estrategias para la Continuidad de negocio (BCP)** | | | |
| -Desarrollar la identificación y definición de las Estrategias de Continuidad de Negocio en el marco de los pilares de continuidad (Personas, Procesos, Instalaciones Físicas y Proveedores) y realizar el análisis de ventajas y desventajas de las estrategias de continuidad.<br>-Desarrollar el análisis costo/beneficio de las estrategias<br>-Presentar ante la alta dirección las estrategias, con el fin de seleccionar y aprobar las mismas | Documentación compilada con las Estrategias de Continuidad de Negocio para los Procesos del MinTIC, análisis de ventajas y desventajas de las estrategias de continuidad, tabla de análisis costo/beneficio de las estrategias. | En el informe de estrategias para la continuidad de las operaciones – BCP se considera el análisis y la definición de los distintos escenarios de falla para los pilares de la continuidad procesos, personas, instalaciones físicas, tecnológicas y proveedores.<br><br>Cabe resaltar que estas estrategias no fueron aprobadas en el comité directivo. | **Cumple Parcialmente** |
| **Observación 4.1:** La consultora realizó el informe de estrategias para la continuidad de las operaciones – BCP, cabe resaltar que estas estrategias no se han implementado teniendo en cuenta que la alta dirección del MINTIC no las aprobó por tema presupuestal. | | | |
| **Objetivo** | **Entregable** | **Validación del entregable** | **Cumple/No cumple/Cumple parcialmente** |

| | | | |
|---|---|---|---|
| **Plan de Recuperación de Desastres (DRP)** | | | |
| -Construir el DRP teniendo en cuenta el catálogo de servicios de TIC del MinTIC | Documentación del DRP el cual deberá contener objetivos; alcance; escenarios; supuestos; roles; árbol de comunicaciones; plan de sucesión; activación; Contingencia y retorno | Resultado del análisis del entregable del DRP este, establece los procedimientos para recuperar los servicios de TI más críticos del ministerio y define las actividades, recursos y procedimientos necesarios para recuperar el funcionamiento de los servicios de TI ante una situación de desastre. | **Cumple** |
| -Desarrollar el documento Plan de Continuidad. BCP | El documento deberá contener detalladamente:<br>-Alcance<br>-Escenarios<br>-Supuestos<br>-Roles<br>-Árbol de comunicaciones<br>-Plan de sucesión<br>-Activación<br>-Contingencia<br>-Retorno. | Como resultado del análisis del entregable del BCP, se dio alcance a los 18 procesos definidos como críticos de la Entidad, se definieron los escenarios de falla o indisponibilidad, los supuestos generales, el gobierno, roles y responsabilidades que desarrollaran las actividades de la gestión de la continuidad, así mismo se definió el árbol de comunicaciones con la lista de contactos claves para notificar la activación del BCP y demás elementos para recuperar los procesos definidos | **Cumple** |

| | | | |
|---|---|---|---|
| | | como críticos del MINTIC, con el fin de hacer frente a una situación que pueda interrumpir la operación normal del Ministerio. | |
| **Pruebas de Escritorio y Escenarios controlados bajo simulación de Continuidad de la Operación de los Servicios.** | | | |
| Realizar las pruebas necesarias con el fin de evaluar el nivel de efectividad del plan de continuidad e identificar las posibles oportunidades de mejora al plan. | Documento plan de pruebas debe contener como mínimo: objetivos de la prueba; objetivos específicos; alcance de la prueba; tipo de prueba; tiempo de la prueba; escenario de la prueba; supuestos; método de la prueba; riesgos e impactos; integrantes de la prueba; resultados esperados; actividades de la prueba; acciones a seguir. | Se entregaron (2) informes de pruebas realizadas el 16 y 17 de diciembre del 2020 enfocados en los siguientes escenarios:<br><br>-**Terrorismo con Ciberterrorismo**: Suceso de ciberataque directo al MINTIC obligando a una evacuación inmediata.<br><br>-**Situación de desastre natural y interrupción temporal de los portales territoriales**: Desastre natural (Ola invernal) en Mocoa, al mismo tiempo se presenta la interrupción de los portales territoriales provistos por MINTIC.<br><br>Ambos informes cuentan con el alcance de la | **Cumple** |

| | | | |
|---|---|---|---|
| | | prueba, tipo de prueba, tiempos y demás actividades de la prueba.<br><br>Los resultados de ambas pruebas fueron satisfactorios en los tiempos de ejecución, se incluye en los informes las recomendaciones para fortalecer los planes de pruebas de la gestión de continuidad. | |

***Tabla 11. Validación entregables- Anexo Técnico 2020 Plan de Continuidad para el Ministerio TIC- BCP***

Con respecto a los entregables asociados al criterio de las Estrategias para la Continuidad de Negocio – BCP es importante la implementación de las mismas y llevar a cabo las pruebas necesarias con el fin de evaluar el nivel de efectividad del plan de continuidad e identificar las posibles oportunidades de mejora al plan.

**Plan de mejoramiento al proceso de Gestión de Tecnologías de la Información- TI.**

La Oficina de Control Interno del Ministerio de Tecnologías de la Información y las Comunicaciones en desarrollo de su función constitucional y legal, y en cumplimiento de su Programa Anual de Auditoría Interna durante el 06 de abril 2022 al 14 de junio 2022 realizo una Auditoría al Proceso de Gestión de TI.

Como producto de lo anterior y con el fin de realizar el respectivo seguimiento de estos planes de acción al proceso de Gestión de TI se revisó el plan de mejoramiento Gestión TI.

A continuación, se presenta el resultado del seguimiento de las acciones registradas en la herramienta SIMIG

| No Acción SIMIG | |
|---|---|
| **Abiertas** | **Cerradas** |
| 1956 | 1952 |
| 1957 | 1953 |
| 1958 | 1954 |
| 1960 | 1955 |
| 1963 | 1073 |
| | 1961 |
| | 1962 |
| | 1069 |
| | 1070 |
| | 1964 |

***Tabla 12. No Acción SIMIG***

| Acciones Correctivas | |
|---|---|
| **Abiertas** | **Cerradas** |
| 5 | 10 |
| **Total 15** | |

***Tabla 13. Estado acciones de mejora SIMIG***

Con relación al resultado obtenido del seguimiento, las (5) acciones que se encuentran abiertas están en ejecución, las acciones 1956, 1957, 1958 y 1960 tenían fecha programada para cierre entre 28 febrero 2023 y 30 marzo 2023.

Las acciones se catalogaron así:

• Acciones abiertas: Acciones abiertas que a la fecha de corte se encuentran en estado de ejecución por parte del proceso.

• Acciones cerradas: Acciones gestionadas por el proceso y que, de acuerdo con el resultado de la evaluación realizada por el auditor de la OCI, se les realizó el respectivo cierre.

• Acciones vencidas: Acciones que tenían fecha programada de cierre entre el 28 febrero 2023 y 30 marzo 2023.

**Hallazgo 4.1: Acciones registradas en la herramienta SIMIG que encuentran vencidas.**

Al revisar las acciones registradas en la herramienta SIMIG de la Auditoría interna que se realizó durante el 06 de abril 2022 al 14 de junio 2022 al Proceso de Gestión de TI se encontraron 5 acciones que están vencidas.

**Recomendación.**

Se sugiere revisar y registrar en la herramienta SIMIG los avances y cargar las evidencias para el cumplimiento de estas teniendo en cuenta el procedimiento "Formulación, Seguimiento y Cierre de Acciones de Mejora- MIG-TIC-PR003 V13"

## 7. TABLA DE HALLAZGOS IDENTIFICADOS

Durante el desarrollo de la auditoría se generaron 6 hallazgos, los cuales se relacionan a continuación:

**Hallazgos:**

| N. del Hallazgo | Riesgo identificado en-la matriz de riesgos del proceso | Resumen del Hallazgo |
|---|---|---|
| **Hallazgo 1.1**: Falta de actualización del instructivo Asignación o devolución de equipos de cómputo | **Incluido.** Posibilidad de afectación reputacional por hallazgos de entes de control y posible pérdida de la certificación en la norma ISO27001 debido a la Incumplimiento del Plan de Seguridad y Privacidad de la información | Se revisó el instructivo "GTI-TIC-IN-002 V2 Asignación o devolución de equipos de cómputo" el cual aplica para todo el personal funcionario o contratista que realice la solicitud de un equipo de cómputo en arriendo. Mediante una toma de muestra de cuatro (4) de diez (10) funcionarios del inventario FUTIC se evidenció que un usuario puede tener asignado dos (2) o más equipos de cómputo; al validar en el instructivo sobre quienes pueden ser los propietarios de los equipos, cuál sería el límite de asignación de equipos y quiénes serían los responsables del manejo de la información según sea el caso, esta información no se especifica en este instructivo. |

| N. del Hallazgo | Riesgo identificado en la matriz de riesgos del proceso | Resumen del Hallazgo |
|---|---|---|
| **Hallazgo 1.2:** Falta de actualización de los documentos asociados al Plan de Continuidad del negocio. | **Incluido.** Posibilidad de afectación reputacional por hallazgos de entes de control y posible pérdida de la certificación en la norma ISO27001 debido a la Incumplimiento del Plan de Seguridad y Privacidad de la información | Al revisar los soportes relacionados con el Plan de Continuidad de la Operaciones – BCP en el cual se definen los elementos iniciales para recuperar los procesos definidos como críticos del Ministerio, con el fin de hacer frente a una situación que interrumpa la operación normal del Ministerio ante incidentes de gran impacto, este documento se definió en el 2021 y se incluyeron los escenarios de pruebas que se han venido realizando los cuales fueron evidenciados en los informes de las pruebas que se han ejecutado al Plan de continuidad de las Operaciones – BCP como al Plan de Recuperación de Desastres – DRP; sin embargo, de acuerdo con los nuevos servicios que pueden ser críticos y algunos procesos como el caso de Arquitectura empresarial que han surgido a partir de 2020, a lo que respecta estos documentos relacionados con el BCP se encuentran desactualizados. |
| **Hallazgo 2.1:** funcionarios y contratistas que ya no laboran en la Entidad y aún siguen activos en el Directorio Activo. | **Incluido.** Posibilidad de afectación reputacional por hallazgos de entes de control y posible pérdida de la certificación en la norma ISO27001 debido a la Incumplimiento del Plan de Seguridad y Privacidad de la información | Se realizó la validación de los archivos suministrados con el listado de funcionarios y contratistas que ya no laboran en la Entidad. El periodo de revisión fue del 01 de enero 2023 al 20 mayo 2023 y se encontraron (145) funcionarios y (17) contratistas retirados durante dicho periodo.<br><br>En respuesta dada, al revisar y validar esta información con base en el archivo suministrado por la Oficina GIT de Servicios tecnológicos se identificaron (2) usuarios que no han sido notificados con la novedad y por ende aún están activos en el Directorio Activo. |
| **Hallazgo 2.2:** Inadecuada ubicación del aire acondicionado en el centro de cómputo, ocasionando bastante ruido y alto consumo de energía. | **Incluido.** Posibilidad de afectación reputacional por hallazgos de entes de control y posible pérdida de la certificación en la norma ISO27001 debido a la Incumplimiento del Plan de Seguridad y | Se realizo una inspección física en las instalaciones del MINTIC para revisar y verificar las condiciones del aire acondicionado en el centro de cómputo, se observó la adecuación de un aire portátil para el control de temperatura, sin embargo, no es una opción eficiente ya que está ocupando un espacio transitable dentro y fuera del centro cómputo, además de ocasionar bastante ruido y consumo de energía alto. |

| N. del Hallazgo | Riesgo identificado en-la matriz de riesgos del proceso | Resumen del Hallazgo |
|---|---|---|
| | Privacidad de la información | |
| **Hallazgo 2.3:** Fallas en la seguridad del cableado de los racks de comunicaciones ubicados en el centro de cómputo principal. | **Incluido.** Posibilidad de afectación reputacional por hallazgos de entes de control y posible pérdida de la certificación en la norma ISO27001 debido a la Incumplimiento del Plan de Seguridad y Privacidad de la información. | Se realizo una inspección física en las instalaciones del MINTIC para revisar y verificar las condiciones de la seguridad del cableado, se observó que el cableado del rack del centro de cómputo principal se encuentra en desorden lo que puede ocasionar desconexiones involuntarias de los diferentes equipos, intermitencias en la conectividad y posibles accidentes. |
| **Hallazgo 4.1:** Acciones registradas en la herramienta SIMIG que encuentran vencidas. | No se observa riesgo registrado en la matriz de riesgos del proceso auditado. | Al revisar las acciones registradas en la herramienta SIMIG de la Auditoría interna que se realizó durante el 06 de abril 2022 al 14 de junio 2022 al Proceso de Gestión de TI se encontraron 5 acciones que están vencidas. |

***Tabla 14. Tabla de hallazgos identificados***

## 8. FORTALEZAS

- Con relación a la Gestión de Incidentes de Seguridad y Privacidad de la Información se evidenciaron lineamientos y estándares implementados para la identificación, atención y respuesta a los incidentes y eventos de seguridad y privacidad de la información y seguridad digital, lo anterior con el fin de mitigar la pérdida de la confidencialidad, integridad y disponibilidad de la información del Ministerio/Fondo Único de Tecnologías de la información y comunicaciones.

- La Entidad define e implementa los criterios básicos en el manejo de la Gestión Documental del Ministerio de Tecnologías de la Información y las Comunicaciones garantizando la conservación y preservación documental.

- Con relación al inventario de activos de información se realiza la identificación, validación, clasificación, valoración, aprobación y publicación de los activos de información dando cumplimiento con la ***Ley 1712 de 2014 Art. 13. Registro de Activos de Información***.

- La disposición y competencia del equipo profesional de los procesos de Gestión de TI y de Seguridad y Privacidad de la Información

## 9. CONCLUSIONES

- Con relación al estado de la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI en los componentes de la hoja de Pruebas Administrativas que comprende los controles de la Norma ISO27001:2013 de los dominios A5, A6, A7, A8, A10, A15 y A17, la evaluación promedio de efectividad es del 98 en escala de evaluación ***gestionado;*** no obstante hay aspectos de mejora y como resultado de la evaluación se presenta debilidades en la apropiación de la Gestión de Activos y Aspectos de Continuidad del Negocio

- Con relación al estado frente a los requisitos establecidos en la Norma NTC-ISO/IEC 27001:2013 en los dominios A9, A10, A11, A12, A13, A14 y A16 y que hacen parte de Modelo de Seguridad y Privacidad de la Información – MSPI, la evaluación promedio de efectividad es del 96,4 en escala de evaluación ***gestionado*** no obstante hay aspectos de mejora y como resultado de la evaluación se presenta debilidades en la Gestión de Acceso de usuarios y Seguridad Física y del Entorno,

- Del listado maestro y la validación de la implementación de estos documentos asociados a la seguridad y privacidad de la información cumplen con los requisitos que establece la Resolución 448 de 2022 y el Manual de Políticas de Seguridad de la Información.

- En relación con la consultoría al Plan de Continuidad de la Operación-BCP para el ministerio TIC y con respecto a los entregables asociados al criterio de las Estrategias para la Continuidad de Negocio – BCP se recomienda la implementación de las mismas y llevar a cabo las pruebas necesarias con el fin de evaluar el nivel de efectividad del plan de continuidad e identificar las posibles oportunidades de mejora al plan.

- Como resultado obtenido del seguimiento de la Auditoría Interna realizada al Proceso de Gestión de TI corresponde a 15 acciones, de las cuales 5 se encontraron abiertas y 10 cerradas en la herramienta

SIMIG, entre las acciones que se encontraron abiertas 1956, 1957, 1958 y 1960 tenían fecha programada para cierre entre 28 febrero 2023 y 30 marzo 2023.

## 10. RECOMENDACIONES

Al final de cada uno de los objetivos 1 y 2 se presentaron las recomendaciones asociadas a las oportunidades de mejora para los procesos de Seguridad y Privacidad de la Información y Gestión de TI.

En relación con el objetivo 4 se recomienda implementar las estrategias para la continuidad de negocio y llevar a cabo las pruebas necesarias con el fin de evaluar el nivel de efectividad del plan de continuidad e identificar las posibles oportunidades de mejora.

Se sugiere revisar y registrar en la herramienta SIMIG los avances y cargar las evidencias para el cumplimiento de estas teniendo en cuenta el procedimiento "Formulación, Seguimiento y Cierre de Acciones de Mejora- MIG-TIC-PR003 V13"

## 11. PLAZO MÁXIMO PARA ENVÍO DE PLANES DE MEJORAMIENTO:

10 días hábiles a partir de la entrega del informe definitivo.

Observación:

Todos los hallazgos deben ser contemplados en el plan de mejoramiento, lo cual será verificado por el auditor líder.

**Aprobó:**

*[Firmado electrónicamente]*

**(Nombre del jefe de la Oficina de Control Interno)**
Jefe Oficina de Control Interno

**Elaboró:** **Equipo auditor:**

**Auditor Líder:** Diana Patricia Murillo

## 12. ANEXO 1. RESPUESTA A LAS OBSERVACIONES DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACIÒN Y SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÒN.

| Hallazgo | Resumen del Hallazgo | Respuesta del Área (Tecnologías de la Información y Seguridad y Privacidad de la Información) | Observación de la OCI |
|---|---|---|---|
| **Hallazgo 1.1.** Falta de apropiación de las Políticas de seguridad de la Información por parte de los usuarios. | El día 17 de junio de 2023 se tomó una muestra de (4) macroprocesos estratégicos, misionales, apoyo y evaluación se seleccionó el macroproceso de apoyo encontrando en su momento de manera presencial (12) usuarios (Nomina, Contabilidad y Tesorería); se tomó una muestra con (7) de estos usuarios a quienes se les indago sobre sí conocían las políticas de seguridad de la información y la ubicación de las mismas, de los cuales (6) respondieron que no conocen la ubicación, pero respondieron con algunos lineamientos que se definen en la política. | No se acepta hallazgo, pues la entidad cuenta con el Plan de Cambio, cultura y apropiación de Seguridad y Privacidad de la Información, en el cual tiene como objetivo el diseñar estrategias para socializar, apropiar, preservar e impulsar la cultura de seguridad y privacidad de la información en los colaboradores de la entidad, dentro de este plan se establecen las diferentes estrategias que se llevarán a cabo durante todo el año, temáticas a abordar, medios y herramientas de comunicación para tal fin.<br><br>Ahora bien, en cuanto a la ubicación de la Política de Seguridad y Privacidad de la Información, el Sistema de Seguridad y Privacidad de la Información ha establecido una serie de estrategias con el fin de fortalecer este aspecto, así: ·<br><br>Como actividad del Plan Operativo del Mes de Junio para Cambio, Cultura y Apropiación se pidió a todos los gestores de los procesos que enviaran correo | **Se retira el hallazgo**.<br><br>Dado que en el mes de agosto fue realizado un recorrido por las instalaciones del Ministerio/Fondo Único de TIC por parte del equipo de Seguridad y Privacidad la Información en el cual se les socializo a funcionarios, contratistas, proveedores/terceros, la ubicación de la Política, tips y buenas prácticas de Seguridad y Privacidad de la Información (Incentivo en donde se encontraba en código QR enlace directo a la Política de Seguridad y Privacidad de la Información) se excluye el hallazgo del informe por los argumentos expuestos por el área.<br><br>No obstante, es importante continuar promoviendo las campañas para la apropiación de las políticas de seguridad de la información por parte de los funcionarios, contratistas, proveedores/terceros. |

| Hallazgo | Resumen del Hallazgo | Respuesta del Área (Tecnologías de la Información y Seguridad y Privacidad de la Información) | Observación de la OCI |
|---|---|---|---|
| | | electrónico a sus colaboradores con la ubicación de las Políticas de Seguridad y Privacidad de la Información, Tratamiento de datos personales, Manual de Seguridad y Privacidad de la Información y Manual de Lineamientos de Seguridad para la Protección y Tratamiento de Datos Personales. Ver: Difusión de Ubicación Política ·<br><br>En el mes de agosto se realizó un recorrido por las instalaciones del Ministerio/Fondo Único de TIC en el cual se les socializo a funcionarios, contratistas, proveedores/terceros, la ubicación de la Política, así como una serie de Tip's y buenas prácticas de Seguridad y Privacidad de la Información. Esto estuvo acompañado de un incentivo (dulce) en donde se encontraba en código QR enlace directo a la Política de Seguridad y Privacidad de la Información, este incentivo permitió recompensar a las personas que tenían claro temas relacionados a la política de Seguridad y Privacidad de la Información y conocimientos generales del sistema. | |
| **Hallazgo 1.2.** Algunos componentes tecnológicos no | Al revisar el Inventario de componentes tecnológicos activos centro de cableado MINTIC, el cual fue recibió el | Se carga el documento en el repositorio creado por el GIT de SPI con nombre "SEPTIEMBRE 2023 inventario datacenter.pdf", la relación de todos los | **Se retira el hallazgo**.<br><br>Se revisó el inventario SEPTIEMBRE 2023 en el que se evidenciaron los componentes tecnológicos |

| Hallazgo | Resumen del Hallazgo | Respuesta del Área (Tecnologías de la Información y Seguridad y Privacidad de la Información) | Observación de la OCI |
|---|---|---|---|
| están definidos dentro del inventario de componentes tecnológicos activos centro de cableado MINTIC. | 29 de junio 2023; se validó que no se encuentran los componentes tecnológicos como el Firewalls, UPS, Acces Point y Router. | servidores y demás equipos que conforman la plataforma tecnológica on premise de la entidad en la cual se relacionan entre otros: Firewalls (FORTIGATE 1800F), UPS (APC 250 KBA SOTANO Y APC 100 KBA PISO 3), Access Point (todos los relacionados con el prefijo AP en el grupo de conectividad de redes). La entidad no cuenta con equipos router, toda vez que la capa 3 del modelo OSI es gestionada por los firewalls. | como el Firewalls, UPS y Acces Point, equipos que conforman la planta tecnológica de MINTIC; por lo anterior se excluye el hallazgo del informe conforme a los argumentos expuestos por el área. |
| **Hallazgo 1.3.** Falta de actualización del instructivo Asignación o devolución de equipos de cómputo | Se revisó el instructivo "GTI-TIC-IN-002 V2 Asignación o devolución de equipos de cómputo" el cual aplica para todo el personal funcionario o contratista que realice la solicitud de un equipo de cómputo en arriendo. Mediante una toma de muestra de cuatro (4) de diez (10) funcionarios del inventario FUTIC se evidenció que un usuario puede tener asignado dos (2) o más equipos de cómputo; al validar en el instructivo sobre quienes pueden ser los propietarios de los equipos, cuál sería el límite de asignación de equipos y | Por directrices de Secretaria General no se asignará equipos de cómputo a contratistas del ministerio, por tal motivo los directivos, jefes y coordinadores pueden solicitar equipos de cómputo para que los colaboradores que tienen a cargo puedan cumplir con las funciones del área. Se verificará el instructivo GTI-TIC-IN-002 y se procederá con su correspondiente actualización de acuerdo con las recomendaciones dadas en el informe de auditoría. | **Se mantiene el hallazgo** (Este hallazgo en el informe preliminar correspondía al 1.3 y en el informe final corresponde al 1.1)<br><br>Una vez revisado el argumento expresado por el proceso Gestión de TI, queda claro que se revisará la asignación actual de los equipos de cómputo, se verificará y se actualizará el instructivo GTI-TIC-IN-002. |

| Hallazgo | Resumen del Hallazgo | Respuesta del Área (Tecnologías de la Información y Seguridad y Privacidad de la Información) | Observación de la OCI |
|---|---|---|---|
| | quiénes serían los responsables del manejo de la información según sea el caso, esta información no se especifica en este instructivo. | | |
| **Hallazgo 1.4.** Falta de actualización de los documentos asociados al Plan de Continuidad del negocio. | Al revisar los soportes relacionados con el Plan de Continuidad de la Operaciones – BCP en el cual se definen los elementos iniciales para recuperar los procesos definidos como críticos del Ministerio, con el fin de hacer frente a una situación que interrumpa la operación normal del Ministerio ante incidentes de gran impacto, este documento se definió en el 2021 y se incluyeron los escenarios de pruebas que se han venido realizando los cuales fueron evidenciados en los informes de las pruebas que se han ejecutado al Plan de continuidad de las Operaciones – BCP como al Plan de Recuperación de Desastres – DRP; sin embargo, de acuerdo con los nuevos servicios que pueden | No se acepta el hallazgo, pues es importante mencionar que el Plan de Continuidad de la Operación y demás documentación de esta gestión están vigentes, así mismo, se ha realizado seguimiento a los riesgos de interrupción en periodicidad mensual, por medio del Plan Operativo del Sistema. Teniendo en cuenta la necesidad de actualizar los nuevos servicios de la entidad en el Plan de Continuidad de la Operación, la entidad durante la presente vigencia avanzó en el proceso contractual por modalidad de Concurso de méritos abierto según | **Se mantiene el hallazgo**. (Este hallazgo en el informe preliminar correspondía al 1.4 y en el informe final corresponde al 1.2)<br><br>De conformidad el ítem AD.5.1.1 del Seguimiento Instrumento Evaluación MSPI.<br>***Determine si el BCP aplica para procesos críticos solamente o se han incluido otros procesos o por lo menos se ha reconocido la necesidad de ampliarlo a otros procesos (para determinar el nivel de madurez)***<br><br>Por lo anterior se considera importante avanzar en la actualización de los nuevos servicios de la Entidad en el Plan de Continuidad de la Operación.<br><br>Además de lo anterior y teniendo en cuenta el soporte entregado en respuesta el ***"Estudio Previo General" y el "Anexo Técnico Actualización del Plan de Continuidad (BCP) del MINTIC basado en la norma ISO 22301 en su última versión"*** es claro que a la Entidad le corresponde verificar el |

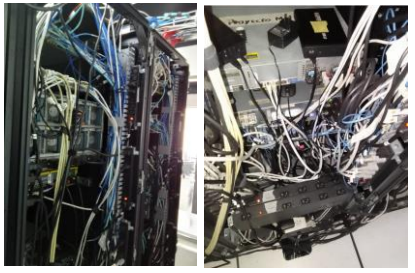
| Hallazgo | Resumen del Hallazgo | Respuesta del Área (Tecnologías de la Información y Seguridad y Privacidad de la Información) | Observación de la OCI |
|---|---|---|---|
| | ser críticos y algunos procesos como el caso de Arquitectura empresarial que han surgido a partir de 2020, a lo que respecta estos documentos relacionados con el BCP se encuentran desactualizados. | número FTIC-CM-004-2023 el cual tiene el siguiente cronograma establecido:<br><br>**CRONOGRAMA DEL PROCESO**<br>**Actividad** / **Fecha**<br>Publicación del aviso de convocatoria pública, estudios previos y proyecto de pliego de condiciones — 17/08/2023<br>Observaciones al proyecto de Pliego de Condiciones — 25/08/2023<br>Respuesta a las observaciones al Proyecto Pliego de Condiciones — 30/08/2023<br>Fecha prevista de publicación de Pliego de Condiciones definitivo y acto administrativo de apertura del proceso de selección — 31/08/2023<br>Respuesta a las observaciones al Pliego de Condiciones — 6/09/2023<br>definitivo<br>Presentación de Ofertas — 11/09/2023<br>Publicación del informe de evaluación de las Ofertas — 15/09/2023<br>Firma del Contrato — 26/09/2023<br>Aprobación de las garantías o pólizas e inicio de ejecución del contrato — 27/09/2023 | cumplimiento de todas las condiciones establecidas en el anexo técnico y supervisar el cumplimiento.<br><br>En cuanto al Anexo Técnico 5.3.1 Estrategias para la Continuidad de negocio (BCP) y el 5.1.7 Pruebas y escenarios controlados bajo simulación de Continuidad de la Operación de los Servicios se Entiende que se llevarán a cabo las pruebas teniendo en cuenta los escenarios y las estrategias definidas. |
| **Hallazgo 1.5.** Falta de actualizaciones y servicio de soporte técnico para el sistema ISOLUCIÓN. | Se revisó el Contrato Estatal No 655 de Prestación De Servicios con el proveedor de ISOLUCIÓN Sistemas Integrados de gestión S.A, el cual terminó su plazo de ejecución el 31 de diciembre de 2022, por lo anterior se indagó con la Oficina de TIC quiénes informan que actualmente el contrato está en proceso de contratación. | No se acepta el hallazgo, toda vez que la oficina de TI adelantó todas las gestiones pertinentes para contratar a los proveedores del sistema Isolucion, esto con el fin de realizar la debida contratación en el menor tiempo posible, sin embargo, se debe tener en cuenta que durante este proceso intervienen actores externos a esta oficina, los cuales son; Subdirección de contratación, Proveedor, Firma que analiza riegos contractuales (Coral Asociados), realización de pólizas y matriz de riesgos. Además, la oficina siempre mantuvo la aplicación funcional y operativa, los casos que se presentaron en dicho periodo fueron solucionados dado que eran solicitudes que podían ser | **Se retira el hallazgo**<br><br>Dado que se recibió el Contrato estatal de prestación de servicios No 728-2023 suscrito entre el Fondo Único de Tecnologías de la Información y la Comunicaciones e ISOLUCION Sistemas Integrados de Gestión S.A. con un plazo de ejecución hasta el 31 de diciembre de 2023 contados a partir del acta de inicio firmada el 30 de junio de 2023, se excluye el hallazgo del informe por los argumentos expuestos. |

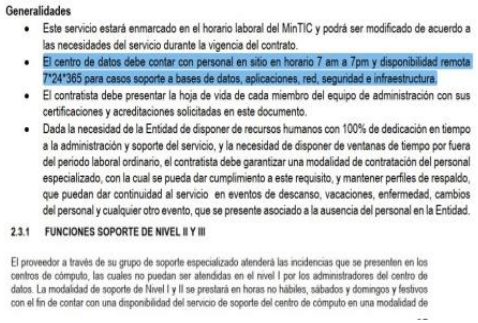
| Hallazgo | Resumen del Hallazgo | Respuesta del Área (Tecnologías de la Información y Seguridad y Privacidad de la Información) | Observación de la OCI |
|---|---|---|---|
| | | atendidas por los profesionales del área funcional. Es importante mencionar que se dio inicio al contrato número 728 el 29 de junio de 2023. | |
| **Hallazgo 2.1.** Funcionarios y contratistas que ya no laboran en la Entidad y aún siguen activos en el Directorio Activo. | Se realizó la validación de los archivos suministrados con el listado de funcionarios y contratistas que ya no laboran en la Entidad. El periodo de revisión fue del 01 de enero 2023 al 20 mayo 2023 y se encontraron (145) funcionarios y (17) contratistas retirados durante dicho periodo.<br><br>Al revisar y validar esta información con base al archivo suministrado por la Oficina GIT de Servicios tecnológicos se identificaron (12) usuarios que aún están activos en el Directorio Activo. | No acepta el hallazgo, se realizaron las validaciones correspondientes donde se indica el por qué los usuarios seguían activos en el DA<br><br>Con el fin de fortalecer los controles para mitigar posibles accesos no autorizados en los sistemas de información cuando los funcionarios y contratistas se desvinculan de la entidad se remitió memorando a talento humano y gestión contractual bajo el radicado 232069337 donde se indica: Con el fin de cumplir con los objetivos de la Resolución 0448 del 2022 “Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, en la cual se definen los lineamientos frente al uso y manejo de la información y se deroga la Resolución 2256 de 2020”, les recordamos que es de suma importancia dar cumplimento al el procedimiento GTI-TIC-PR-007-Gestión de usuarios y perfiles para el acceso a Recursos TI. Este procedimiento en su numeral uno (1) indica la manera en la cual | **Se mantiene el hallazgo** (Este hallazgo en el informe preliminar correspondía al 2.1 y en el informe final se mantiene en el 2.1)<br><br>De acuerdo al memorando radicado el 27 de Julio 2023 el cual fue remitido al subdirector de Gestión de Talento Humano se informa la importancia de dar cumplimiento al procedimiento GTI-TIC-PR-007-Gestión de usuarios y perfiles para el acceso a Recursos TI.<br><br>Por lo anterior para evitar cualquier intento de acceso no autorizado o suplantación de identidad se solicita a la Entidad la gestión oportuna del envió de novedad de los funcionarios que ya no laboran en la Entidad en base al archivo suministrado por Talento humano.<br><br>**VER ANEXO 2.1** |

| Hallazgo | Resumen del Hallazgo | Respuesta del Área (Tecnologías de la Información y Seguridad y Privacidad de la Información) | Observación de la OCI |
|---|---|---|---|
| | | se deben tramitar las novedades como vacaciones, licencias, desvinculación definitiva, de la cual hacen parte las áreas que ustedes representan. La desactivación de usuarios garantiza que no existan riesgos de filtración de información sensible y minimiza la posibilidad de daños, alteraciones o uso indebido de los recursos informáticos de la entidad. Con esta acción se revocan los privilegios de acceso y se impide cualquier intento de suplantación de identidad o acceso no autorizado. La gestión oportuna es una medida crucial para evitar la exposición de información confidencial y restringir el acceso a terceros no autorizados. En este sentido, es imperativo que nos mantengan informados de cualquier cambio en el estado administrativo y/o contractual de los usuarios remitiendo los documentos que soportan dicho trámite, en caso de requerir apoyo en esta actividad, por favor contactarse con la mesa de servicio vía Teams o a través de la línea telefónica en la extensión 3300. | |

| Hallazgo | Resumen del Hallazgo | Respuesta del Área (Tecnologías de la Información y Seguridad y Privacidad de la Información) | Observación de la OCI |
|---|---|---|---|
| **Hallazgo 2.2.** Inadecuada ubicación del aire acondicionado en el centro de cómputo, ocasionando bastante ruido y alto consumo de energía. | Se realizo una inspección física en las instalaciones del MINTIC para revisar y verificar las condiciones del aire acondicionado en el centro de cómputo, se observó la adecuación de un aire portátil para el control de temperatura, sin embargo, no es una opción eficiente ya que está ocupando un espacio transitable dentro y fuera del centro cómputo, además de ocasionar bastante ruido y consumo de energía alto | Actualmente se encuentran operando, tres aires acondicionados portátiles de precisión instalados temporalmente en el Data Center de MinTic como contingencia debido a los daños irreparables presentados en los Aires Acondicionados con que cuenta MinTic. La OTI abrió un Proceso de selección abreviada para la adquisición de bienes y servicios de características técnicas uniformes por Subasta Inversa Electrónica No. FTIC-SASI-002-2023, con el siguiente Objeto: “Adquisición, instalación y puesta en funcionamiento de aires acondicionados que permitan la conservación, disponibilidad y buen funcionamiento de los servidores y equipos de almacenamiento, red, seguridad y comunicaciones ubicados en el Data Center del Ministerio / Fondo Único de TIC con el fin de fortalecer la infraestructura tecnológica de la entidad”. Con características eficientes y menor consumo de Energía. Así las cosas, los aires acondicionados serán remplazados por los nuevos aires, garantizando así las condiciones climáticas para el DataCenter, es de aclarar que a la fecha no se ha presentado indisponibilidad de ningún servicio por temas relacionados con el aire acondicionado. Link proceso contractual: https://community.secop.gov.co/Public/Te | **Se mantiene el hallazgo** (Este hallazgo en el informe preliminar correspondía al 2.2 y en el informe final se mantiene en el 2.2)<br><br>Una vez revisado el argumento se cuenta con la FICHA TECNICA aprobada en el mes de septiembre con el objeto Adquisición, instalación y puesta en funcionamiento de aires acondicionados que permitan la conservación, disponibilidad y buen funcionamiento de los servidores y equipos de funcionamiento, red, seguridad y comunicaciones ubicados en el Data Center del Ministerio/ Fondo Único de TIC con el fin de fortalecer la infraestructura tecnológica de la Entidad.<br><br>La puesta en funcionamiento de este aire acondicionado según las especificaciones dadas en la FICHA TECNICA permitirá la conservación, disponibilidad y buen funcionamiento de los servidores y equipos de almacenamiento, red, seguridad y comunicaciones. |

| Hallazgo | Resumen del Hallazgo | Respuesta del Área (Tecnologías de la Información y Seguridad y Privacidad de la Información) | Observación de la OCI |
|---|---|---|---|
| | | ndering/OpportunityDetail/Index?noticeUID=CO1.NTC.4880374&isFromPublicArea=True&isModal=False | |
| **Hallazgo 2.3.** Fallas en la seguridad del cableado de los racks de comunicaciones ubicados en el centro de cómputo principal. | Se realizo una inspección física en las instalaciones del MINTIC para revisar y verificar las condiciones de la seguridad del cableado, se observó que el cableado del racks del centro de cómputo principal se encuentra en desorden lo que puede ocasionar desconexiones involuntarias de los diferentes equipos, intermitencias en la conectividad y posibles accidentes. | Se realizó organización de cableado estructurado y de conectividad en los Rack del Data Center del Edificio Murillo Toro, piso 3, como se evidencia en la siguiente Imagen:<br>   <br>Durante el día de la visita por parte de la Auditoría al Data Center, se informó que se estaba realizando el proceso de desmonte de los servidores (Enclosure CISCO) y otros equipos que ya habían cumplido su | **Se mantiene el hallazgo** (Este hallazgo en el informe preliminar correspondía al 2.3 y en el informe final se mantiene en el 2.3)<br><br>Se realizó una inspección de manera presencial en el Data center del Edificio Murillo Toro, piso 3 y se |

| | | | |
|---|---|---|---|
| | | vida útil y que, por su obsolescencia tecnológica, presentaban daño irreparable, originando así el estado del cableado por desconexión de los equipos en proceso de desmonte. La Oficina de TI garantiza la seguridad del cableado de los racks de comunicaciones ubicados en el centro de cómputo principal, mediante los controles de acceso al Data Center y a través de los servicios de mantenimientos preventivos según anexo técnico del contrato 0785 de 2019. | verificó que se le realizaron ajustes, sin embargo, el cableado sigue presentando desorden lo que puede ocasionar desconexiones involuntarias, intermitencias entre otros posibles accidentes<br><br>.<br><br>  <br>  <br><br>En una adecuada gestión del cableado, por ejemplo, se puede utilizar una combinación de colores para identificar cuales puntos de red o conexiones pueden ser de extrema criticidad, realizar una adecuada marcación de los puntos de red, el patch panel entre otros. De otra parte, los cables que están |

| Hallazgo | Resumen del Hallazgo | Respuesta del Área (Tecnologías de la Información y Seguridad y Privacidad de la Información) | Observación de la OCI |
|---|---|---|---|
| | | | sueltos se les debe revisar su funcionalidad o retirarlos sea el caso.<br><br>Es de tener en cuenta que la marcación de los cables, en el caso de que ocurra un daño o el cambio de cableado se puede perder el etiquetado. |
| **Hallazgo 2.4.** No se cuenta con un encargado directo para administrar y analizar las 24 horas del día y 7 días de la semana los ciberataques. | Se valido que la Entidad cuenta con herramientas que permiten el continuo monitoreo de infraestructura, herramientas de seguridad, aplicaciones y servicios tecnológicos. Sin embargo, al verificar sobre el responsable para la gestión de este monitoreo, se evidenció que no se cuenta con un encargado directo para administrar y analizar las 24 horas del día y 7 días de la semana los ciberataques que puede enfrentar la Entidad. | No se acepta el hallazgo toda vez que el ministerio desde el 2019 cuenta con el contrato 785-2019 cuyo objeto es contratar el fortalecimiento de las herramientas de análisis y servicios tecnológicos de la entidad en materia de tecnología, informática y TIC asegurado una información oportuna y de calidad ofreciendo los mecanismos necesarios para el cumplimiento, y donde en su anexo técnico se evidencia que se tiene soporte 7*24*365 ,para analizar las 24 horas del día y 7 días de la semana los ciberataques.<br><br>  <br>**Generalidades**<br>• Este servicio estará enmarcado en el horario laboral del MinTIC y podrá ser modificado de acuerdo a las necesidades del servicio durante la vigencia del contrato.<br>• El centro de datos debe contar con personal en sitio en horario 7 am a 7pm y disponibilidad remota 7*24*365 para casos soporte a bases de datos, aplicaciones, red, seguridad e infraestructura.<br>• El contratista debe presentar la hoja de vida de cada miembro del equipo de administración con sus certificaciones y acreditaciones solicitadas en este documento.<br>• Dada la necesidad de la Entidad de disponer de recursos humanos con 100% de dedicación en tiempo a la administración y soporte del servicio, y la necesidad de disponer de ventanas de tiempo por fuera del periodo laboral ordinario, el contratista debe garantizar una modalidad de contratación del personal especializado, con la cual se pueda dar cumplimiento a este requisito, y mantener perfiles de respaldo, que puedan dar continuidad al servicio en eventos de descanso, vacaciones, enfermedad, cambios del personal y cualquier otro evento, que se presente asociado a la ausencia del personal en la Entidad.<br>2.3.1 FUNCIONES SOPORTE DE NIVEL II Y III<br>El proveedor a través de su grupo de soporte especializado atenderá las incidencias que se presenten en los centros de cómputo, las cuales no puedan ser atendidas en el nivel I por los administradores del centro de datos. La modalidad de soporte de Nivel I y II se prestará en horas no hábiles, sábados y domingos y festivos con el fin de contar con una disponibilidad del servicio de soporte del centro de cómputo en una modalidad de | **Se retira el hallazgo**.<br><br>En respuesta dada se observó como evidencia dentro de las Generalidades del Anexo Técnico.<br><br>***"El centro de datos debe contar con personal en sitio en horario 7am a 7pm y disponibilidad remota 7*24*365 para casos de soporte a bases de datos, aplicaciones, red, seguridad e infraestructura"*** por lo anterior se excluye el hallazgo del informe con los argumentos expuestos por el área.<br><br>No obstante, teniendo en cuenta las respuestas a las observaciones preliminares que fueron presentadas a esta Auditoría el pasado 29 de junio del 2023 por parte del proceso Gestión TI, ***"desde la oficina ti se viene adelantando el proceso de contratación del SOC / NOC , el cual fue aprobado en el comité de PAA y se realizó la solicitud del CDP".*** es importante seguir avanzando en el fortaleciendo de controles para la seguridad de la información de tal manera que se permita la supervisión y monitoreo continuo frente a las amenazas como malware, ransomware, phishing, ataques de fuerza bruta entre otros. |

| Hallazgo | Resumen del Hallazgo | Respuesta del Área (Tecnologías de la Información y Seguridad y Privacidad de la Información) | Observación de la OCI |
|---|---|---|---|
| **Hallazgo 2.5.** La hoja de vida de INTEGRATIC no especifica las medidas de seguridad. | Se valido sobre las medidas de seguridad para los sistemas de información, que se describen en el documento "GTI-TIC-FM-028 hoja de vida sistemas de información" en la que se incluye una lista de chequeo de lineamientos de seguridad para los sistemas de información que deberá cumplir el proveedor de la aplicación, sin embargo, al validar la hoja de vida de INTEGRATIC, esta no especifica las medidas de seguridad de la información. | Se acoge la recomendación y se solicita al proveedor de la aplicación INTEGRATIC actualizar y diligenciar debidamente los requisitos de medidas de seguridad en las hojas de vida de los sistemas de información, esto con el objetivo de atender las buenas prácticas y medidas de protección del sistema Integratic, se adjunta evidencia en el repositorio. | **Se retira el hallazgo**.<br><br>En respuesta dada se observó como evidencia los correos que fueron enviados, solicitando al proveedor de INTEGRATIC el debido diligenciamiento de los lineamientos de seguridad con el que cuenta el sistema de información INTEGRATIC y se realiza dicho diligenciamiento. Por lo anterior se excluye el hallazgo del informe por los argumentos expuestos por el área.<br><br>No obstante, es importante tener en cuenta previo a la adquisición de los sistemas de información el cumplimiento del "***Lineamiento para la recepción o desarrollo de servicios tecnológicos y sistemas***" Nral 2.4.1.5 **Seguridad** - La aplicación debe contar con las siguientes características de seguridad:<br><br>-Inicio de sesión único, utilizando el estándar LDAP (integrando nativamente con el Directorio Activo de Microsoft Windows o Directorio Activo Azure) o consumiéndolo a través del bus de servicios (ESB) de la entidad.<br>-Debe permitir la administración de roles, perfiles, usuarios, permisos y niveles de acceso a las diferentes funcionalidades de sus componentes y datos<br>-Utilizar de Certificados SSL (TLS) para todo |

| Hallazgo | Resumen del Hallazgo | Respuesta del Área (Tecnologías de la Información y Seguridad y Privacidad de la Información) | Observación de la OCI |
|---|---|---|---|
| | | | intercambio de mensajes (incluidos los de interoperabilidad)<br>-Poseer mecanismos para evitar ataques de XSS (Cross Site Scripting), en todo elemento o componente de la Solución donde pueda existir recepción de datos o aplicaciones externas<br>-Todas las contraseñas deben estar encriptadas (base de datos o Archivos de configuración. Conf)<br>-El proveedor deberá someter la aplicación a un Ethical hacking y previo a la puesta en producción se debe presentar la evidencia de la implementación de la solución a los problemas identificados. |
| **Hallazgo 4.1.** Acciones registradas en la herramienta SIMIG que encuentran vencidas. | Al revisar las acciones registradas en la herramienta SIMIG de la auditoría interna que se realizó durante el 06 de abril 2022 al 14 de junio 2022 al Proceso de Gestión de TI se encontraron 5 acciones que están vencidas. | Se está trabajando y haciendo seguimiento para poder dar cierre a las acciones correctivas producto de la auditoría interna realizada en la vigencia 2022 | **Se mantiene el hallazgo** (Este hallazgo en el informe preliminar correspondía al 4.1 y en el informe final se mantiene en el 4.1)<br><br>En respuesta dada por el proceso de Gestión de TI y Seguridad y privacidad de la Información, se mantiene el hallazgo. |

# REGISTRO DE FIRMAS ELECTRONICAS

Informe final auditoria al Modelo de Seguridad y Privacidad de la Información

Ministerio de Tecnología de la Información y las Comunicaciones
gestionado por: azsign.com.co

Id Acuerdo: 20231005-072530-21d144-10955608
Creación: 2023-10-05 07:25:30
Estado: Finalizado
Finalización: 2023-10-05 07:28:12

Escanee el código para verificación

**Firma: Firma**

José Ignacio León Flórez
79271841
jleon@mintic.gov.co

# REPORTE DE TRAZABILIDAD

Informe final auditoria al Modelo de Seguridad y Privacidad de la Información

Ministerio de Tecnología de la Información y las Comunicaciones
gestionado por: azsign.com.co

Id Acuerdo: 20231005-072530-21d144-10955608 Creación: 2023-10-05 07:25:30

Estado: Finalizado Finalización: 2023-10-05 07:28:12

Escanee el código para verificación

| TRAMITE | PARTICIPANTE | ESTADO | ENVIO, LECTURA Y RESPUESTA |
|---|---|---|---|
| Firma | José Ignacio León Flórez<br>jleon@mintic.gov.co | Aprobado | Env.: 2023-10-05 07:25:30<br>Lec.: 2023-10-05 07:28:01<br>Res.: 2023-10-05 07:28:12<br>IP Res.: 190.145.189.98 |