Escuela Tecnológica Instituto Técnico Central	**INFORME DE AUDITORÍA**	**CÓDIGO: GCI-FO-05** **VERSIÓN: 5** **VIGENCIA: ABRIL 11 DE 2016** **PÀGINA: 1 de 10**

PROCESO O PROCEDIMIENTO AUDITADO	FECHA INICIO	HORA DE INICIO	FECHA TERMNACIÓN	HORA TERMNACIÓN
Gestión de Seguridad de la Información.	20/03/2018	9:00 a.m	22/03/2018	4:00 p.m.
OBJETIVO	Verificar el diseño e implementación del Modelo de Seguridad y Privacidad de la Información – MSPI de la Escuela Tecnológica Instituto Técnico Central, basado en los criterios establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, proponiendo recomendaciones para su mejora continua.			

RESPONSABLE DEL PROCESO AUDITADO	Yoisel Leopoldo Rojas Hernández
EQUIPO AUDITOR	**FUNCIONARIOS ENTREVISTADOS**
Rosa María Buitrago Barón	Yoisel Leopoldo Rojas Hernández
Tatiana Elizabeth Yepes Zúñiga	
Diana Marcela Córdoba Vargas	

DOCUMENTOS DE REFERENCIA O NORMATIVIDAD APLICABLE

Decreto 1078 de 2015: Por el cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Modelo de Seguridad y Privacidad de la Información. MINTIC. Versión 3.0. del 29/07/2016

Instrumento de Evaluación del MSPI. MINTIC.

Metodología pruebas de efectividad. Guía 1. MINTIC

Política general. Guía 2. MINTIC

Roles y responsabilidades. Guía 4. MINTIC

Gestión y clasificación de activos de información. Guía 5. MINTIC

Referencia sobre gestión documental. Guía 6. MINTIC

Indicadores de Gestión para la seguridad de la información. Guía 9. MINTIC

Plan de capacitación, sensibilización y comunicación de seguridad de la información. Guía 14. MINTIC

Evaluación del desempeño. Guía 16. MINTIC

Caracterización del proceso Gestión de Seguridad de la Información. GDC- FO-01. Versión 3.0

FORTALEZAS

La Oficina de Control Interno, dando cumplimiento al Plan de Auditoria definido, realizó la verificación del cumplimiento de los lineamientos establecidos por MINTIC para las fases del Modelo de Seguridad y Privacidad de la Información desde la fase de diagnóstico hasta la fase de evaluación del desempeño, los resultados se evidencian a continuación:

FASE DIAGNÓSTICO:

Se evidenció que la ETITC diseño e implementó su Modelo de Seguridad y Privacidad de la Información a partir de la vigencia 2016, en la cual, elaboró el respectivo diagnóstico, mediante la aplicación del "*Instrumento de identificación de la línea base de seguridad de la información*" del MINTIC y como resultado se identificó que el Modelo se encontraba en un nivel de madurez "Inicial" y en la fase de "Planificación" del ciclo PHVA.

Con base en el diagnóstico efectuado la ETITC evidenció debilidades en levantamiento de la información y mediante mesas de trabajo y reuniones con los líderes de los procesos se completó dicha información en un **90%.**

Así mismo, con la colaboración del MINTIC, durante el mes de diciembre de 2017, se realizaron las diferentes pruebas de efectividad a cargo del Consorcio PWBC y CROSS Border Tecnology, el cual, efectuó pruebas de seguridad y penetración, suministrando el respectivo Informe de análisis de vulnerabilidades, dando como resultado un **94%** de la efectividad de los controles.

FASE PLANIFICACIÓN:

Se evidenció que la ETITC cuenta con un Manual de Políticas de Seguridad y Privacidad de la Información, del cual, la primera versión se adoptó el 30/09/2016 y la segunda versión se adoptó el 19/04/2017, en esta última versión se contempló la actualización de la Política General de Seguridad de la Información, con base en la integración de los sistemas de gestión. El manual contempla las políticas de Organización de Seguridad de la Información (Estructura organizacional de seguridad de la información, uso de dispositivos móviles y uso de conexiones remotas), Políticas de Seguridad de los Recursos Humanos (Antes de asumir el empleo, durante la ejecución del empleo, terminación y cambio de empleo), Políticas de Gestión de Activos de Información (Responsabilidad por los activos, clasificación y etiquetado de la información, manejo de medios), Políticas de control de acceso (Acceso a redes y recursos de red, administración de acceso de usuarios, responsabilidades de acceso de los usuarios, uso de altos privilegios y utilitarios de administración, control de acceso a sistemas y aplicaciones), Políticas de controles criptográficos, Políticas de Seguridad física y del entorno (Áreas seguras, seguridad para los equipos institucionales, escritorio limpio y pantalla limpia).

Así como las Políticas de seguridad de las operaciones (Asignación de responsabilidades operativas, protección contra códigos maliciosos, copias de respaldo de la información, registro de eventos y monitoreo de los recursos tecnológicos y los sistemas de información, control de software operacional, gestión de vulnerabilidad técnica), Políticas de seguridad de las comunicaciones (Gestión de seguridad de redes, uso de correo electrónico institucional, uso adecuado de internet, política de transferencia de información), Políticas de adquisición, desarrollo y mantenimiento de sistemas de información (Requisitos de seguridad de los sistemas de información, seguridad en los procesos de desarrollo y soporte de los sistemas de información, protección de datos de prueba), Política de relaciones con proveedores (Seguridad de la información en las relaciones con proveedores, gestión de la prestación de los servicios de proveedores), Políticas de gestión de incidentes de seguridad de la información (Gestión de incidentes y mejoras en la seguridad de la información), Políticas de aspectos de seguridad de la información de la gestión de continuidad del negocio (Continuidad de seguridad de la información, redundancias), Políticas de cumplimiento

(Requisitos legales y contractuales, privacidad y protección de datos personales).

Por otro lado, se evidenció que la ETITC cuenta con una metodología para identificar, clasificar y valorar los activos de información - GIC-PC-10 versión 1.0 del 08/02/2018, mediante la cual se establecieron los requisitos de seguridad para cada uno de los activos de información, identificando qué activos posee la Escuela, cómo deben ser utilizados, los roles y responsabilidades que tienen los servidores públicos sobre los mismos y cuyo alcance contempla todos los procesos institucionales (Estratégicos, misionales, de apoyo y evaluación).

Con base en la metodología relacionada anteriormente, se elaboró el respectivo inventario de los activos de información de la ETITC, de tipo Hardware, Software, Documental y Servicios, consolidados en la matriz de identificación, valoración y clasificación de activos de información, dispuesta por MINTIC y teniendo en cuenta las directrices establecidas en la Ley 1712 de 2014 de Transparencia y Derecho de Acceso a la Información Pública Nacional, el Decreto 103 de 2015, la Norma NTC ISO/IEC 27001:2013, las buenas prácticas de Gobierno en Línea, así como las observaciones producto de la revisión efectuada al Modelo de Seguridad y Privacidad de la Información -MSPI, por parte del MINTIC.

La ETITC elaboró el Plan y estrategia de transición de Internet Protocol Versión 4 - IPv4 a IPv6, sin embargo y de acuerdo a la información suministrada por el líder del proceso Gestión de Seguridad de la Información, este requisito fue excluido del MSPI, por el MINTIC para la vigencia 2018, motivo por el cual, en la presente auditoría, no se verificaron los demás componentes asociados a este requisito.

La ETITC mediante la Resolución 275 del 12 de julio de 2017, adoptó el Programa de Gestión Documental, el cual contempla directrices para garantizar la Confidencialidad, Integridad y Disponibilidad de la información, en la gestión documental.

La ETITC, durante la vigencia 2017 contó con un plan de sensibilización y entrenamiento en temas de seguridad de la información, para todo el personal que labora en la entidad, con el fin de consolidar una cultura de seguridad que favorezca la preservación de la Confidencialidad, Integridad y Disponibilidad de la información institucional, dentro de los temas se contempló el análisis de las Políticas de Seguridad y Privacidad de la Información de la Escuela, el uso de contraseñas de acceso a los sistemas de información y recursos informáticos, clasificación y etiquetado de la información, la identificación preservación y recolección de evidencias digitales, entre otros, dando como resultado un cumplimiento de ejecución del plan de un **27%**, en razón a que se sobredimensionó el alcance del plan, programándose una serie de actividades voluminosas, las cuales no se cumplieron en su totalidad, teniendo en cuenta que no se contaba con la cantidad de recurso humano necesaria para darle su respectivo cumplimiento.

FASE IMPLEMENTACIÓN:

La ETITC, teniendo en cuenta los lineamientos establecidos por MINTIC en la Guía de indicadores de gestión para la seguridad de la información (Guía No. 9), elaboró e implemento diez y seis (16) indicadores de gestión, mediante los cuales identifica el nivel de cumplimiento de los requisitos del MSPI, así como el nivel de concienciación del recurso humano que labora para la Escuela, dichos indicadores se describen a continuación:

Indicador 01. Organización de Seguridad de la Información:

Este indicador permite hacer seguimiento, al compromiso de la dirección, en cuanto a seguridad de la información, en lo relacionado con la asignación de personas y responsabilidades relacionadas a la seguridad de la información, al interior de la ETITC. El indicador está enfocado, no solo a la contratación de nuevos servidores públicos, sí no a la asignación de responsabilidades. Por consiguiente, se evidenció que en el periodo en que se realizó la medición del indicador (02/10/2017) se obtuvo un cumplimiento del **100%**, en razón a que la ETITC cuenta con el documento de asignación del recurso humano, asignación de roles y responsabilidades, así mismo cuenta con un Comité de Seguridad de la Información, creado mediante la Resolución No. 349 del 26 de septiembre de 2016.

Indicador 02. Cubrimiento del MSPI en los activos de información que contienen datos personales:

Este indicador permite determinar y hacer seguimiento a la administración segura de los sistemas de información de la ETITC, que contienen datos personales, dentro del marco de seguridad y privacidad de la información. Por consiguiente, se evidenció que en el periodo que se midió el indicador (02/10/2017) obtuvo un cumplimiento del **47%**, en razón a que, se identificó que existían sistemas de información que almacenaban datos personales de titulares que no estaban siendo administrados de manera segura, teniendo en cuenta que estaban siendo custodiados por áreas que no tenían las competencias requeridas en temas de tecnología.

Indicador 03. Tratamientos de Eventos Relacionados con el Marco de Seguridad y Privacidad de la Información.

Este indicador permite determinar la eficacia en el tratamiento de eventos, relacionados con la seguridad de la información. Por consiguiente, se evidenció que en el periodo en que se realizó la medición del indicador (02/10/2017) obtuvo un cumplimiento del **50%**, en razón a que, si bien, el total de los incidentes reportados fueron cerrados por mesa de ayuda, no obstante, once (11) de las acciones que permiten mantener el control sobre los riesgos residuales, no se encontraron implementadas al 100%.

Indicador 04. – Plan de Sensibilización.

Este indicador permite medir la aplicación de los temas sensibilizados en seguridad de la información, por parte de los usuarios finales. Estas mediciones se realizan por medio de auditorías internas y/o externas o mediante exámenes aplicados, por los responsables de ejecutar la sensibilización. Por consiguiente, se evidenció que en el periodo en que se realizó la medición del indicador (02/10/2017) obtuvo un cumplimiento del **27%**, en razón a que, durante la elaboración del respectivo plan de sensibilización, y como se indicó anteriormente, se sobredimensionó el alcance del mismo, programándose una serie de actividades voluminosas, las cuales no se cumplieron en su totalidad, teniendo en cuenta que no se contaba con la cantidad de recurso humano necesaria para darle su respectivo cumplimiento.

Indicador 05. Cumplimiento de Políticas de Seguridad de la Información en la ETITC.

Este indicador permite identificar el nivel de cumplimiento de políticas de seguridad de la información en los procesos de la ETITC. Por consiguiente, se evidenció que en el periodo en que

se realizó la medición del indicador (02/10/2017) ***se cumplió***, en razón a que la ETITC elaboró e implemento la política general de seguridad de la información, así como definió la respectiva organización interna, en términos de personas y responsabilidades, con el fin de cumplir las políticas de seguridad de la información.

Indicador 06. – Identificación de Lineamientos, Políticas, Procedimientos y/o Controles de Seguridad de la ETITC.

Este indicador permite identificar la existencia de lineamientos, políticas, procedimientos y/o controles de seguridad de la información, que garanticen preservar la protección de las instalaciones físicas, equipos de cómputo y el entorno, evitando accesos no autorizados. Por consiguiente, se evidenció que en el periodo en que se realizó la medición del indicador (02/10/2017) ***se cumplió***, en razón a que, mediante el Manual de Políticas de Seguridad y Privacidad de la Información, la ETITC definió lineamientos, políticas, procedimientos y/o controles, que garanticen la protección de las instalaciones físicas, equipos de cómputo y su entorno, evitando, accesos no autorizados y minimizando los riesgos de la seguridad de la información.

Indicador 07. – Verificación del Control de Acceso.

Este indicador permite identificar la existencia de lineamientos, normas, estándares, políticas, procedimientos y controles de seguridad, en cuanto al control de acceso en la ETITC. Por consiguiente, se evidenció que en el periodo en que se realizó la medición del indicador (02/10/2017) ***se cumplió***, en razón a que, mediante el Manual de Políticas de Seguridad y Privacidad de la Información, la ETITC definió lineamientos, políticas, procedimientos y/o controles de seguridad para el acceso de los usuarios a la plataforma tecnológica, así como para controlar el uso y el acceso a los sistemas de información, las aplicaciones, depósitos de información y dispositivos móviles.

Indicador 08. – Aseguramiento en la Adquisición y Mantenimiento de Software.

Este indicador permite identificar la existencia de lineamientos, normas, estándares, políticas, procedimientos y controles de seguridad, en cuanto a la adquisición o desarrollo de aplicaciones. Por consiguiente, se evidenció que en el periodo en que se realizó la medición del indicador (02/10/2017) ***se cumplió***, en razón a que, mediante el Manual de Políticas de Seguridad y Privacidad de la Información, la ETITC definió lineamientos, políticas, procedimientos y/o controles de seguridad, para el desarrollo o adquisición de software, sistemas y aplicaciones y gestión de incidentes de seguridad de la información.

Indicador 09. – Implementación de los Procesos de Registro y Auditoria.

Este indicador permite identificar la existencia de lineamientos, normas, estándares, políticas, procedimientos y/o controles de seguridad, en cuanto a registro y auditoria, para la seguridad de la información. Por consiguiente, se evidenció que en el periodo en que se realizó la medición del indicador (02/10/2017) ***se cumplió***, en razón a que, mediante el Manual de Políticas de Seguridad y Privacidad de la Información, la ETITC definió lineamientos, políticas, procedimientos y/o controles de seguridad, para el registro y control de eventos que sucedan sobre sus sistemas, redes y servicios, así mismo, verifica periódicamente, de manera interna y/o a través de terceros, sus procesos de seguridad de la información y sistemas, para asegurar el cumplimiento del modelo.

Indicador 10. – Detección de Anomalías en la Prestación de los Servicios de la ETITC.

Este indicador permite medir el grado de implementación de los mecanismos encaminados a la detección de anomalías e irregularidades. Por consiguiente, se evidenció que durante el periodo que se realizó la medición (02/10/2017) ***no se cumplió***, en razón a que, no se habían implementado actividades relacionadas con análisis de vulnerabilidades, pruebas de penetración, auditoria de redes y de sistemas de información.

Indicador 11. – Políticas de Privacidad y Confidencialidad.

Este indicador permite identificar el nivel de implementación de políticas, lineamientos, normas, estándares, procedimientos y/o controles de seguridad, relacionados con la privacidad y confidencialidad de la información de la ETITC. Por consiguiente, se evidenció que en el periodo en que se realizó la medición del indicador (02/10/2017) ***se cumplió***, en razón a que, mediante el Manual de Políticas de Seguridad y Privacidad de la Información, la ETITC definió lineamientos, políticas, procedimientos y/o controles de seguridad, para proteger la información personal y privada, de los ciudadanos que utilizan sus servicios.

Indicador 12. – Verificación de las Políticas de Integridad de la Información.

Este indicador permite identificar el nivel de implementación de lineamientos, normas, estándares, políticas, procedimientos, controles de seguridad y soluciones tecnológicas, que permitan preservar la integridad de la información en la ETITC. Por consiguiente, se evidenció que durante el periodo que se realizó la medición (02/10/2017) ***no se cumplió***, en razón a que, si bien la ETITC cuenta con lineamientos, normas, estándares, políticas, procedimientos y controles de seguridad aplicados, las soluciones tecnológicas no se encontraron implementadas al 100%, como es el caso de la solución de backup automatizada mediante la herramienta backula, de acuerdo con la información suministrada por el líder del proceso.

Indicador 13. – Política de Disponibilidad del Servicio y de la Información.

Este indicador permite identificar el nivel de implementación de políticas, lineamientos, normas, estándares, procedimientos y/o controles de seguridad, de disponibilidad del servicio y de la información de la ETITC. Por consiguiente, se evidenció que durante el periodo que se realizó la medición (02/10/2017) ***no se cumplió***, en razón a que, si bien la ETITC cuenta con políticas, lineamientos, normas, estándares, procedimientos y controles de seguridad implementados, no contaba con un plan de contingencia, recuperación y retorno a la normalidad, aprobado e implementado.

Indicador 14. – Ataques Informáticos a la ETITC.

Este indicador permite identificar el porcentaje de ataques informáticos recibidos en la ETITC, que impidieron la prestación de servicios ofrecidos. Por consiguiente, se evidenció que durante la vigencia 2017, no se presentaron ataques informáticos.

Indicador 15. – Calidad de los Servicios Prestados por Proveedores.

Este indicador permite identificar la existencia de acuerdos de nivel de servicios en la relación con proveedores, evidenciando la definición de los aspectos que permiten garantizar un servicio de calidad. Por consiguiente, se evidenció que en el periodo que se realizó la medición (02/10/2017) ***se***

cumplió, en razón que, los acuerdos de niveles de servicio – ANS estaban siendo anexados a la propuesta suministrada por el proveedor del servicio.

Indicador 16. – Implementación de Controles de Seguridad.

Este indicador permite identificar el grado de avance en la implementación de controles de seguridad. Por consiguiente, se evidenció que en el periodo que se realizó la medición (02/10/2017) se cumplió con la implementación del **94%** de los controles de seguridad, en razón que, de un total de ciento once (111) controles aplicables, la ETITC tenía implementados ciento cuatro (104) controles.

De acuerdo a la información suministrada por el líder del proceso y evidenciada en el instrumento de evaluación de MINTIC, el Modelo de Seguridad y Privacidad de la Información de la ETITC se encuentran en un nivel de madurez "**Definido**", lo que significa que la entidad tiene documentado, estandarizado y aprobado por la Dirección el MSPI, así mismo, todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados. De igual manera, se evidenció que la ETITC cuenta con un **80%** de avance en el ciclo PHVA del Modelo y se encuentra en la fase de Evaluación de Desempeño, quedando pendiente la fase de mejora continua.

FASE EVALUACIÓN DEL DESEMPEÑO:

Se evidenció que la ETITC elaboró e implementó el Plan de Seguimiento y Revisión del Modelo de Seguridad y Privacidad de la Información y el Sistema de Seguridad de la Información, versión 1.0 del 09/10/2017. Mediante de dicho plan la ETITC determina la eficacia, eficiencia y efectividad de los controles y conforme a la valoración de los riesgos realizada por el líder del proceso, se evidenció que, para el total de riesgos identificados, se aplicaron los controles respectivos, conforme al Anexo A de la NTC ISO7IEC 27001:2013, los cuales han sido eficaces, eficientes y efectivos. Así mismo y como se evidenció anteriormente, el líder del proceso efectuó el 02/10/2017 la medición respectiva a los indicadores de gestión.

De igual manera, se evidenció que, mediante dicho plan, la ETITC realiza seguimiento a la programación y ejecución de las auditorías internas y externas efectuadas al MSPI, sobre las cuales, de acuerdo con la información suministrada por el líder del proceso, actualmente se encuentra en ejecución el ciclo de auditorías internas, así mismo, se evidenció que durante la vigencia 2017, se recibió la visita de los funcionarios del MINTIC quienes realizaron una evaluación al Modelo, evidenciando fortalezas y hallazgos, sobre los que se suscribieron los respectivos planes de mejoramiento.

Por lo anterior, la Oficina de Control Interno revisó el cumplimiento de dichos planes de mejoramiento, evidenciando que en total para el proceso Gestión de Seguridad de la Información se dejaron seis (6) hallazgos, sobre los que el líder del proceso suscribió nueve (9) acciones de mejoramiento de tipo correctivo. De dichas acciones la Oficina de Control Interno, solicitó las evidencias, sobre las cuales constato su respectivo cumplimiento y eficacia, por lo que procedió a dar el respectivo cierre de las mismas, tal como se evidencia en la siguiente tabla:

No. HALLAZGO	SITUACIÓN ENCONTRADA	ACCION CORRECTIVA	ACCIONES A IMPLEMENTAR	FECHA INICIO	FECHA FINAL	RESPONSABLE IMPLEMENTACIÓN	CALIDAD O CONTROL INTERNO (Seguimiento al Plan)					VERIFICACIÓN EFICACIA ACCIONES IMPLEMENTADAS
							SEGUIMIENTO REALIZADO	ESTADO ACCIÓN	ESTADO HALLAZGO	RESPONSABLE DEL SEGUIMIENTO	FECHA DEL SEGUIMIENTO	
1	Los roles y responsabilidades de seguridad de la información, pueden ampliarse un poco, para designar a otras áreas que deben participar en actividades de seguridad de la información.	X	Actualización del documento Asignación de Recurso Humano, Roles y Responsabilidades.	22/01/2018	12/02/2018	Yoisel L Rojas.	Se realizó el seguimiento a la ejecución de la accion de mejora planteada, evidenciando su cumplimiento, en donde el documento "Asignación de recurso humano, roles y responsabilidades" fue actualizado a la Version 2.0 del 30/01/2018 y en el que se incluyeron nuevos roles con sus respectivas responsabilidades, como lo es el caso de: Talento Humano, Control Interndo Disciplinario, Infraestructura eléctrica, Gestion Documental y Seguridad Fisica.	Terminada	Cerrado	Rosa María Buitrago Barón	21/03/2018	La acción implementada fue eficáz.
2	La Metodología de Gestión de Riesgos está bien estructurada y alineada con lo que maneja la Entidad, sin embargo, hace falta hacer hincapié en el análisis de riesgos, basado en los activos de la Entidad, dado que el análisis se enfoca en encontrar riesgos generales en cada proceso y puede faltar detalle o profundidad en algunos casos.	X	Adicionar y diligenciar los campos Activo de Información Afectado y Criterio Afectado (Confidencialidad, Integridad y/o Disponibilidad), en la Matriz de Riesgos.	29/01/2018	26/02/2018	Yoisel L Rojas.	Se realizó el seguimiento a la ejecución de la accion de mejora planteada, evidenciando su cumplimiento, en donde el documento "Metodología de Gestion de Riesgos ETITC" se actualizó a la Version 2.0 del 15/12/2017, donde se modificó el numeral 7,1. Análisis del Riesgo, adicionandose actividades relacionadas con la identificación del activo de información afectado y el criterio de seguridad afectado con la materialización del riesgo. Se evidenció su aplicabilidad en la Matriz de Riesgos de Seguridad de la Información.	Terminada	Cerrado	Rosa María Buitrago Barón	21/03/2018	La acción implementada fue eficáz.
3	Existe un levantamiento de información de activos bien estructurado, sin embargo, es conveniente ejecutar un análisis relacionado a la confidencialidad, integridad y disponibilidad, no solo de los activos que contienen datos personales (Ley 1581), sino que pueden existir activos críticos, para el funcionamiento de la Entidad y es importante determinar cuáles son.	X	Clasificar los activos de información tipo software y servicios, en cuanto a Confidencialidad, Integridad y Disponibilidad.	22/01/2018	5/02/2018	Yoisel L Rojas.	Se realizó el seguimiento a la ejecución de la accion de mejora planteada, evidenciando su cumplimiento, en donde en el documento "Metodología para identificar y clasificar activos de información de la ETITC" se actualizó a la Version 2.0 del 08/02/2018, en la cua se modificó el numeral 4,4. Claisificación de los activos de información, asi mismo, se evidneció su aplicabilidad en las matrices de inventario de activos tipo software y servicios.	Terminada	Cerrado	Rosa María Buitrago Barón	21/03/2018	La acción implementada fue eficáz.
			Clasificar los activos de información tipo hardware, en cuanto a Disponibilidad.	5/02/2018	19/02/2018	Yoisel L Rojas.	Se realizó el seguimiento a la ejecución de la accion de mejora planteada, evidenciando su cumplimiento, en donde en el documento "Metodología para identificar y clasificar activos de información de la ETITC" se actualizó a la Version 2.0 del 08/02/2018, en la cua se modificó el numeral 4,4. Claisificación de los activos de información, asi mismo, se evidneció su aplicabilidad en las matrices de inventario de activos tipo hardware.	Terminada	Cerrado	Rosa María Buitrago Barón	21/03/2018	La acción implementada fue eficáz.
4	No existen los documentos, deberá iniciarse la gestión para su creación. Nota: La numeración de los items, relacionados con el presente hallazgo, corresponden a los numerales del 24 al 27, de la nueva versión de la herramienta de seguimiento del MINTIC y no a los numerales del 28 al 31, especificados en el acta de revisión.	X	Elaboración y aprobación del documento Inventario de Partes Externas o Terceros a los que se Transfiere Información de la Entidad.	15/01/2018	29/01/2018	Yoisel L Rojas.	Se realizó el seguimiento a la ejecución de la accion de mejora planteada, evidenciando su cumplimiento, en donde se elaboró y aprobó el documento "Inventario de partes externas o terceros a los que se transfiere informacion de la ETITC, versión 1.0 del 25/01/2018	Terminada	Cerrado	Rosa María Buitrago Barón	21/03/2018	La acción implementada fue eficáz.
			Elaboración del Formato de Acuerdo de Transferencia de Información.	29/01/2018	5/02/2018	Yoisel L Rojas.	Se realizó el seguimiento a la ejecución de la accion de mejora planteada, evidenciando su cumplimiento, en el que se elaboró y aprobo el documento con la justificación de la no implementación del formato de transferenia de información, en razón a que la ETITC ya cuenta con una serie de elementos que garantizan una transferencia de informacion segura, tales como: Cláusula de confidencialidad, Política de Transferencia de Información y Procedimientos de intercambio de información fisica y digital.	Terminada	Cerrado	Rosa María Buitrago Barón	21/03/2018	La acción implementada fue eficáz.
			Inventario de proveedores que tengan acceso a los activos de información, indicando el servicio que prestan o bienes que venden.	5/02/2018	19/02/2018	Yoisel L Rojas.	Se realizó el seguimiento a la ejecución de la accion de mejora planteada, evidenciando su cumplimiento, en el que se elaboró y aprobo el documento "Inventario de proveedores con acceso a los activos de información de la ETITC", versión 1.0 del 25/01/2018.	Terminada	Cerrado	Rosa María Buitrago Barón	21/03/2018	La acción implementada fue eficáz.

No. HALLAZGO	SITUACIÓN ENCONTRADA	ACCION CORRECTIVA	ACCIONES A IMPLEMENTAR	FECHA INICIO	FECHA FINAL	RESPONSABLE IMPLEMENTACIÓN	CALIDAD O CONTROL INTERNO (Seguimiento al Plan)					VERIFICACIÓN EFICACIA ACCIONES IMPLEMENTADAS
							SEGUIMIENTO REALIZADO	ESTADO ACCIÓN	ESTADO HALLAZGO	RESPONSABLE DEL SEGUIMIENTO	FECHA DEL SEGUIMIENTO	
5	En este caso el indicador nunca nos daria 100%, dado que no todos los activos contienen datos personales, sería mejor considerar que el indicador apunte a su valoración adecuada, de una manera un poco más general (y esto incluiría datos personales), dado que el análisis debe realizarse a todos los activos.	X	Ajustar el indicador 02, del documento Descripción Indicadores de Gestión, con el objetivo de identificar la cantidad de sistemas de información, que contienen datos personales, y están siendo administrados de manera segura.	22/01/2018	12/02/2018	Yoisel L Rojas.	Se realizó el seguimiento a la ejecución de la accion de mejora planteada, evidenciando su cumplimiento, en donde el documento "Descripción indicadores de gestión ETITC" se actulizó a la versión 2.0 del 15 de enero de 2018, en lo que concierne al Indicador 02. Cubrimiento del MSPI en los activos de información que contienen datos personales.	Terminada	Cerrado	Rosa María Buitrago Barón	21/03/2018	La acción implementada fue eficáz.
6	La declaración de aplicabilidad, aparte de demostrar cuáles controles se aplican, debe justificar la razón por la cual se excluyen determinados controles.	X	Justificar, en el documento Declaración de Aplicabilidad, la no aplicación de los controles excluyentes.	15/01/2018	29/01/2018	Yoisel L Rojas.	Se realizó el seguimiento a la ejecución de la accion de mejora planteada, evidenciando su cumplimiento, en donde el documento "Declaración de aplicabilidad", se actualizó a la versión 2.0 del 18/01/2018, en lo que concierne a la justificacion de la no implementación de los controles del Anexo A de la norma NTC ISO/IEC 20071:2013, asi mismo, se actualizó la hoja de levantamiento de informacion del instrumento de seguimiento de MINTIC, con los controles que no aplican en la entidad.	Terminada	Cerrado	Rosa María Buitrago Barón	21/03/2018	La acción implementada fue eficáz.

ASPECTOS POR MEJORAR (RECOMENDACIÓN O DEBILIDAD)

FASE DIAGNÓSTICO:

Obtener el 100% de la información requerida en esta fase, en razón a que como lo indico el líder del proceso, se encuentra en proceso de elaboración: el *Diagrama de red de alto nivel o arquitectura de TI*, sobre el cual el Área de Informática y Comunicaciones contrató, un profesional para realizar el respectivo diagrama, el cual se espera obtener durante la presente vigencia y así dar cumplimiento con este requisito, así mismo el *Plan de continuidad de la Entidad aprobado*, el cual se encuentra en proceso de elaboración y se espera terminarlo en la presente vigencia.

FASE PLANIFICACIÓN:

Programar las actividades de sensibilización sobre el MSPI necesarias, teniendo en cuenta el recurso humano disponible para tal fin.

FASE IMPLEMENTACIÓN:

- Fortalecer la seguridad de los sistemas de información que almacenan datos personales.
- Implementar la totalidad de acciones que permiten mantener el control sobre los riesgos residuales.
- Cumplir el 100% de las actividades programadas en el plan de sensibilización y entrenamiento para cada vigencia sobre el Modelo de Seguridad y Privacidad de la Información.
- Implementar actividades relacionadas con el análisis de vulnerabilidades, pruebas de

penetración, auditoria de redes y auditorias de sistemas de información.
- Implementar las soluciones tecnológicas que sean necesarias para garantizar la integridad de la información.
- Elaborar, aprobar e implementar un plan de contingencia, recuperación y retorno a la normalidad de los servicios prestados por la ETITC.
- Implementar el 100% de los controles que le son aplicables a la ETITC, de acuerdo al Anexo A de la NTC ISO/IEC 27001:2013

NO CONFORMIDADES O HALLAZGOS
(Incumplimiento de un requisito interno, normativo o de parte interesada)

No.	NORMA	DESCRIPCIÓN	TIPO	
			MAYOR	MENOR

OBSERVACIONES

AUDITOR LIDER	22/3/18. RESPONSABLE DEL PROCESO

Nota 1: Definición de No Conformidad Mayor:
Incumplimiento de un requisito normativo, propio de la institución y/o legal, que vulnera o pone en serio riesgo la integridad del sistema de gestión. Puede corresponder a la o aplicación de una cláusula de una norma (requerida por la organización), el desarrollo de un proceso sin control, ausencia consistente de registros declarados por la organización o exigidos por la norma, o la repetición permanente y prolongada a través del tiempo de pequeños incumplimientos asociados a un mismo proceso o procedimiento.
Ejemplos de no conformidad Menor: No realización de las auditorías y Ausencia de un documento de procedimiento para el Control de Documentos.

Nota 2: Definición de No Conformidad Menor:
Desviación mínima en relación con requisitos normativos, propios de la organización y/o legales, estos incumplimientos, son esporádicos, dispersos y parciales y no afecta mayormente la eficiencia e integridad del sistema de gestión.
Ejemplos de no conformidad Menor: Ausencia de una firma en un registro de un conjunto de varios registros. Incumplimiento esporádico de una actividad dentro de un procedimiento o proceso.
Nota 3: Definición de Hallazgo: El hallazgo de auditoría es un hecho relevante que se constituye en un resultado determinante en la evaluación de un asunto en particular, al comparar la condición [situación detectada- SER] con el criterio [deber ser]. Igualmente, es una situación determinada al aplicar pruebas de auditoría que se complementará estableciendo sus causas y efectos.