Nombre de la Empresa	**:**	**Ministerio de Tecnologías de la información y las Comunicaciones - MINTIC**
Cliente Nº	**:**	**SG-049**
Tipo de auditoría	**:**	Otorgamiento
Norma de Referencia	**:**	**NTC ISO/IEC 27001:2013**
Fecha de Auditoría	**:**	19 al 20 de octubre de 2021
Alcance	**:**	Asegurar la confidencialidad, integridad y disponibilidad de la información en la gestión y control de la prestación del servicio Público de las Tecnologías de la Información y las Comunicaciones.
Auditor Líder	**:**	Gustavo Sanchez (GS)
Experto técnico	**:**	N/A
Auditores	**:**	Jesús David Díaz (JD)
Objetivo	**:**	Determinar la conformidad del sistema de gestión de la compañía **Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC**, con los criterios de la norma **NTC ISO/IEC 27001:2013**; evaluando la capacidad del sistema de gestión para asegurar que la organización cumple los requisitos legales, reglamentarios y contractuales aplicables; evalúa su eficacia e identifica las áreas de mejora.

1. RESUMEN DE AUDITORÍA

Antes de la Auditoría de Certificación, el **Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC**, facilitó su Informe de Análisis de Impacto al Negocio - BIA – MinTIC, Informe de Análisis de Riesgos de Interrupción - RIA – MinTIC, Informe Estrategias para la Continuidad de las Operaciones – MinTIC, Plan de Recuperación de Desastres Tecnológicos - DRP – MinTIC, Prueba #1 - Plan de Continuidad de las Operaciones - MinTIC V1.0, Prueba #2 - Plan de Continuidad de las Operaciones - MinTIC V1.0, GTI-TIC-MA-017 Gestión de cambios, GTI-TIC-MA-018 Lineamientos recepción desarrollo de servicios tecnológicos y sistemas, GTI-TIC-PR-005 Respaldo Retención Restauración Información, GTI-TIC-PR-007 Gestión de Accesos a Recursos de TI, GTI-TIC-PR-010 Mesa de Servicio, GTI-TIC-PR-011 Cambios normales, GTI-TIC-PR-020 Administrar la operación gestión de eventos, GTI-TIC-PR-021 Administrar Operación Gestión Requerimientos-

Incidentes, GTI-TIC-PR-026 Seguimiento Monitoreo Datos Abiertos, GTI-TIC-PR-028 Recepción de recursos y_o sistemas, GTI-TIC-PR-029 Actualización de equipos de usuario, GTI-TIC-PR-030 Trae Tu Propio Dispositivo, GTI-TIC-PR-031 Cambios de emergencia, GTI-TIC-PR-032 Monitoreo, GTI-TIC-PR-033 Actualización de Sistemas Operativos, Acta Alcance RxD_SPI 21092021, Acta RxD 27052021, Listado Asistencia 27052021, Listado Asistencia Alcance 21092021, PPT Revisión_por_Direccion_27052021_Comité MIG 47, EAC-TIC-FM-005 INFORME AUDITORIA INTERNA SGSI, GDO-TIC-MA-014 Manual de Activos de Información, GDO-TIC-PR-019 Procedimiento de Activos de información, Informe gestión riesgos SPI 1-Sem 2021, Manual de políticas del SGSPI Mintic, Manual del MIG, MIG-TIC-MA-008 Lineamientos para la Administración de Riesgos, MIG-TIC-MC-001 Manual del MIG, MIG-TIC-PR-006 Identificación de requisitos legales y de otra índole,Plan_tratamiento_riesgos_seguridad_2021, Politica_seguridad_privacidad_ informacion_Resolucion_2256_2020,Politica_tratamiento_datos_personales_Resolucion_924_2020,Resolucion_politica_seguridad_privacidad_informacion_resolucion_2256_2020, SPI-TIC-PR-001 Procedimiento de Incidentes, Cartas descriptivas.. El Auditor Líder realizó el Análisis del Sistema Documental y envió a la Entidad los hallazgos encontrados durante este Análisis.

La Auditoría de fase I se llevó a cabo en las instalaciones de GLOBAL COLOMBIA Ubicadas en la Calle 94 11-20 en la ciudad de Bogotá D.C y se han mantenido conversaciones con miembros de todos los Departamentos. El alcance original de la Auditoría fue revisado y se ha considerado apropiado para las actividades que se están llevando a cabo. El tiempo de duración fue de 2 días.

2. HALLAZGOS DE LA EVALUACIÓN DOCUMENTAL ETAPA I

Durante la revisión realizada a la documentación Informe de Análisis de Impacto al Negocio - BIA – MinTIC, Informe de Análisis de Riesgos de Interrupción - RIA – MinTIC, Informe Estrategias para la Continuidad de las Operaciones – MinTIC, Plan de Recuperación de Desastres Tecnológicos - DRP – MinTIC, Prueba #1 - Plan de Continuidad de las Operaciones - MinTIC V1.0, Prueba #2 - Plan de Continuidad de las Operaciones - MinTIC V1.0, GTI-TIC-MA-017 Gestión de cambios, GTI-TIC-MA-018 Lineamientos recepción desarrollo de servicios tecnológicos y sistemas, GTI-TIC-PR-005 Respaldo Retención Restauración Información, GTI-TIC-PR-007 Gestión de Accesos a Recursos de TI, GTI-TIC-PR-010 Mesa de Servicio, GTI-TIC-PR-011 Cambios normales, GTI-TIC-PR-020 Administrar la operación gestión de eventos, GTI-TIC-PR-021 Administrar Operación Gestión Requerimientos-Incidentes, GTI-TIC-PR-026 Seguimiento Monitoreo Datos Abiertos, GTI-TIC-PR-028 Recepción de recursos y_o sistemas, GTI-TIC-PR-029 Actualización de equipos de usuario, GTI-TIC-PR-030 Trae Tu Propio Dispositivo, GTI-TIC-PR-031 Cambios de emergencia, GTI-TIC-PR-032 Monitoreo, GTI-TIC-PR-033 Actualización de Sistemas Operativos, Acta Alcance RxD_SPI 21092021, Acta RxD 27052021, Listado Asistencia 27052021, Listado Asistencia Alcance 21092021, PPT Revisión_por_Direccion_27052021_Comité MIG 47, EAC-TIC-FM-005 INFORME AUDITORIA INTERNA SGSI, GDO-TIC-MA-014 Manual de Activos de Información, GDO-TIC-PR-019 Procedimiento de Activos de información, Informe gestión riesgos SPI 1-Sem 2021, Manual de

políticas del SGSPI Mintic, Manual del MIG, MIG-TIC-MA-008 Lineamientos para la Administración de Riesgos, MIG-TIC-MC-001 Manual del MIG, MIG-TIC-PR-006 Identificación de requisitos legales y de otra índole,Plan_tratamiento_riesgos_seguridad_2021, Politica_seguridad_privacidad_informacion_Resolucion_2256_2020,Politica_tratamiento_datos_personales_Resolucion_924_2020,Resolucion_politica_seguridad_privacidad_informacion_resolucion_2256_2020, SPI-TIC-PR-001 Procedimiento de Incidentes, Cartas descriptivas. Dentro del alcance solicitado asegurar la Confidencialidad, Integridad y Disponibilidad de la información en la gestión y control de la prestación del Servicio Público de las Tecnologías de la Información y las Comunicaciones De la organización **Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC**

Se evidenciaron cero hallazgos los cuales se describen a continuación: NA

Se evidencia como fortaleza que el sistema está ampliamente documentado y ofrece al lector una visión amplia y detallada de los controles y procedimientos aplicables.

Temas de preocupación que podrían ser clasificados como no conformidad en el transcurso de la etapa 2:

- En el informe de auditoría interna de Sistema de Gestión, de fecha 06 09 2021 se indica frente a cada hallazgo, una “Recomendación” que al parecer surge del equipo auditor lo cual puede llegar a afectar el principio de imparcialidad del proceso de auditoría así como el análisis de causas exigido para la mejora.

- No es posible establecer si se evaluó todo el alcance del SGSI. En sitio se evaluarán las evidencias respectivas.

- Se evidencian espacios en blanco dentro del documento GESTIÓN DE ATENCIÓN A GRUPOS DE INTERÉS, específicamente. Teniendo en cuenta que este fue un punto sobre el que llamó la atención el Informe de Auditoría interna, se revisará en sitio su corrección.

- Sobre el acta 48 de fecha 27 de mayo a 3 de junio de 2021:
  - ✓ No es posible establecer el tratamiento a las acciones correctivas. Se indica en el numeral 4.4: “No se presentaron acciones de mejora registradas en SIMIG-ISOLUCION durante la vigencia del 2020”, lo cual podría afectar el cumplimiento del numeral 10. Mejora.
  - ✓ En el numeral 4.6.1 de la misma acta “Resultados Auditorías Internas II Semestre 2020 Sistema de Seguridad y Privacidad de la Información” se indica que algunas tareas se encuentran incumplidas, sin embargo, en el punto “Decisión”, no se indica ninguna decisión frente a esta situación sino que señala “El Comité MIG analiza y evalúa la gestión y avance de las acciones presentadas como resultado de auditorías

al Sistema de Seguridad y Privacidad de la Información – SGSPI, donde se validó el estado, compromiso y cumplimiento frente a dichas acciones"

- ✓ No se evidencia retroalimentación **DE** las partes interesadas sino **A** las partes interesadas.
- ✓ No se evidencian las tendencias relativas a no conformidades y acciones correctivas, seguimiento y resultado de las mediciones, resultados de las auditorías o cumplimiento de los objetivos.

- No fue posible evidenciar gestión de oportunidades dado que no se nos aportó documento al respecto.

- No fue posible evaluar los criterios objetivos de probabilidad e impacto requeridos para la calificación de los riesgos. Con base en lo indicado en el documento Plan_tratamiento_riesgos_seguridad_2021el equipo auditor se refirió a la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016) pero no fue posible su ubicación. Este punto será objeto de revisión en sitio.

- En la Declaración de aplicabilidad v1.3 no se evidencia la justificación de las inclusiones de los controles de la norma. Se incluye una columna denominada "Estado del control", pero este señala los artefactos relacionados, no la justificación.

- En el informe de auditoría interna de Sistema de Gestión, de fecha 06 09 2021 se indica que "el sistema no se han documentado o excluido formalmente procedimientos que no fueron presentados en la auditoria para… "y menciona algunos controles. Sin embargo, no es posible evidenciar la corrección realizada dado que la Declaración de Aplicabilidad no cuenta con control de cambios.

Análisis sobre la empresa:

ITEM	COMENTARIOS DEL AUDITOR
Ubicación y condiciones específicas del sitio del cliente, estado de preparación para la etapa 2.	La ubicación del cliente es el Edificio Murillo Toro Cra. 8a entre calles 12A y 12B, Bogotá D.C
Estado del cliente y grado de compresión de los requisitos de la norma. * *Si el cliente no está preparado y el grado de comprensión de los requisitos de la norma es poco no podrá ser pasado a etapa 2.	Se logra evidenciar que la organización cumple con los criterios establecidos por la norma ISO/IEC 27001:2013, y se determina la comprensión de los requisitos establecidos.

Se recopilo información necesaria correspondiente: -Alcance del sistema de gestión -Procesos de la Organización -Ubicaciones de la organización del cliente -Aspectos legales y reglamentarios relacionados y su cumplimiento	La identificación de los elementos actuales permitió evaluar el progreso del cumplimiento de los controles aplicables definidos para la implementación del SGSI, de manera que los elementos identificados para el Alcance del Sistema de Gestión se encuentra definido dentro del documento Acta Alcance RxD_SPI 21092021, Acta RxD 27052021, PPT Revisión_por_Direccion_27052021_Comité MIG 47, Resolución_politica_seguridad_privacidad_informacion_resolucion_2256_2020,Politica_seguridad_privacidad_informacion_Resolucion_2256_2020, procesos de la organización y ubicaciones de la organización definidos en el MIG-TIC-MC-001 Manual del MIG, a su vez se identifica el informe de análisis de impacto – BIA, Plan de recuperación de Desastres tecnológicos y plan de continuidad de las operaciones. Sobre aspectos legales y reglamentarios se identifica el procedimiento MIG-TIC-PR-006 Identificación de requisitos legales y de otra índole.
Asignación de recursos para la auditoria etapa 2 y acordar con el cliente detalles para la auditoria etapa 2.	Se cuenta con la logística requerida para la ejecución de la evaluación y se han acordado detalles con las personas encargadas del Ministerio.
Se ha obtenido una compresión suficiente del sistema de gestión del cliente y de las operaciones del sitio en el contexto de los posibles aspectos significativos.	Dentro de la información recolectada se alcanza a obtener una comprensión suficiente del Sistema de Gestión de Seguridad de la información implementado por la organización y de las operaciones que realiza.
Se planifican y realizan las auditorías internas y revisión por la dirección y el nivel de implementación del sistema de gestión confirma que la organización del cliente está preparada para la auditoria de etapa 2.	Se logra evidenciar que las auditorías internas se realizan de forma planificada. Se describe dentro del documento PPT-Revisión_por_dirección_27052021_Comité MIG 47, se especifica realización de pre-auditorías internas por cada uno de los sistemas de gestión. El último informe de auditoría interna fue realizado el 25 de agosto de 2021. La revisión de la dirección se encuentra establecido dentro del documento Acta Alcance RxD_SPI 21092021 y el acta Acta RxD 27052021.

Si es una evaluación de sistema de gestión multisitio por favor diligencie a continuación:

Se ha seleccionado la muestra	NA
Por favor indique la muestra	NA

¿Se ha planificado la Etapa 2, teniendo en cuenta los procesos / actividades a auditar en cada sitio?	NA
¿El equipo auditor cuenta con la competencia?	NA

En consecuencia a los anteriores resultados SI Se recomienda por parte del auditor el paso de la evaluación de la conformidad según el referente **NTC ISO/IEC 27001:2013 A la etapa II**

En la etapa 2 se realizará seguimiento a los hallazgos identificados y a los demás temas de preocupación que podría ser clasificado como no conformidad en el transcurso de la auditoria etapa 2. Por tanto esto será tenido en cuenta cuando el auditor elabore el plan de auditoria de la etapa 2.

Nota: ¿Es un ejercicio simulado para una testificación? SI ____ NO _X__

Fecha de Realización del Informe	Martes 20 de Octubre de 2021.
Realizado Por	Jesús David Díaz Quiceno
Cargo	Auditores

Este documento es válido sin Firma y ha sido revisado y emitido por el auditor Líder indicado en el mismo.