CLIENTE: Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC

Nº CLIENTE: SG-049

ALCANCE DE LA ORGANIZACIÓN: 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.

NOMBRE COMPLETO Y VERSIÓN VIGENTE DE LA DECLARACIÓN DE APLICABILIDAD: Declaración de Aplicabilidad, vigencia 2023

TIPO DE AUDITORIA: Segundo Seguimiento

FECHA(S) DE LA AUDITORÍA: 30/10/2023 - 31/10/2023

NORMA DE REFERENCIA: NTC ISO/IEC 27001:2013

AUDITOR LÍDER: Edgar Fernando Suarez

AUDITOR(ES): Adriana Sandoval

---

1 OBJETIVOS:

El propósito de la evaluación es evaluar la implementación, incluida la eficacia del sistema de gestión de seguridad de la información de **Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC**

2 ALCANCE DE LA AUDITORIA:

El alcance de la evaluación es el sistema de gestión de seguridad de la información de **Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC**

3 PROCESOS AUDITADOS:

- Todos los Procesos que hacen parte del Sistema Integrado de Gestión del Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC que apoyan las actividades del Sistema de Gestión de Seguridad de la Información- SGSI.

4 RESUMEN DE AUDITORÍA

Antes de la Auditoría de Certificación, el **Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC**, facilitó su Alcance del SGSI, Políticas y objetivos de seguridad de la información, Proceso de evaluación y tratamiento de riesgos, Declaración de aplicabilidad, Plan de tratamiento del riesgo, Informe de evaluación de riesgos, Uso aceptable de los activos, Política de control de acceso, Procedimientos operativos para gestión de TI, Principios de ingeniería para sistema seguro, Política de seguridad para proveedores, Procedimiento para gestión de incidentes, Procedimientos de la continuidad del negocio, Requisitos legales, normativos y contractuales, Ultima revisión Gerencial y Último informe de auditoría interna para que fuesen revisados. El Auditor Líder realizó el Análisis del Sistema Documental y envió a la empresa los hallazgos encontrados durante este Análisis.

La Auditoría se llevó a cabo de forma presencial y se han mantenido conversaciones con miembros de todos los Procesos. El alcance original de la Auditoría fue revisado y se ha considerado apropiado para las actividades que se están llevando a cabo.

La documentación interna y procedimientos que han sido mostrados, en la mayoría de los casos cumplen coherentemente los requisitos acordados como se determina mediante evidencias revisadas y entrevistas realizadas.

En la reunión de Cierre, la Dirección fue informada de la eficacia del sistema de gestión conforme la norma de referencia es adecuada y por tanto SI se ha recomendado dar continuidad al certificado vigente con que cuenta el **Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC.**

5 REUNIÓN DE APERTURA

Antes del comienzo de la Auditoría, se mantuvo una reunión de apertura que fue sostenida entre las siguientes personas:

5.1 Representando a Cliente:

Juan Andrés Uscategui
Rosa Lucia Ortega
Yesica Tatiana Vanegas
Andrés David González Murcia
Juddy Amado Sierra
Jhon Caballero Martínez

Angela Cortés
Giovanni Espitia

5.2 Representando a Global:

Edgar Fernando Suarez
Adriana Sandoval

El Auditor Líder se presentó y explicó el Proceso de Auditoría.

El Auditor Líder confirmó que desearía establecer, mediante evidencias objetivas, que ha sido seguido el Sistema de gestión documental. Esto conllevaría a realizar preguntas de prueba y registrar las respuestas dadas. Además mencionó que la Auditoría se llevaría a cabo por muestreo y que sería al azar y no de modo estadístico, aunque si se descubre una No Conformidad, se aumentará el muestreo para establecer el impacto de la No Conformidad. Se explicaron los conceptos de No conformidad mayor y menor

Se confirmó que para evitar situaciones que pongan en riesgo la seguridad y salud en el trabajo del equipo auditor, estos estarán acompañados por personal de la organización, y serán vigilados para salvaguardar su seguridad, además que en caso de emergencia seguirán las instrucciones de su acompañante.

Los criterios utilizados en la auditoría (Norma **NTC ISO/IEC 27001:2013**, procesos y documentación del cliente) han servido como referencia para determinar la conformidad de su sistema de gestión.

El Auditor Líder confirma que toda la información obtenida durante el transcurso de la Auditoría es confidencial entre ambas partes a excepción de la información que puede ser requerida por la Entidad Nacional de Acreditación (ONAC) o mediante requerimiento legal realizado por los organismos de control o judiciales en cuyo caso el suministro de información será notificado a la organización .

Se confirmó la conveniencia del Programa de Auditoría previamente emitido. Se determinó que SI será necesaria la utilización de guías en el proceso de auditoría. El alcance de la Auditoría fue confirmado como, 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.

6 AUDITORÍA

6.1 Análisis de riesgos de seguridad de información de la organización

El análisis de riesgos de seguridad de información de la organización es consistente en el contexto del negocio, y las interrelaciones con otras funciones de negocios, tales como recursos humanos, desarrollo, producción, operaciones, administración, TI, finanzas, entre otros.

6.2 Tiempo empleado y lugares visitados

La auditoría in situ duro 4 días siendo visitado 1 lugar. La distribución del tiempo empleado en la evaluación es la siguiente:

0,10 días	Análisis del Sistema Documental y elaboración del Programa.
0 días	Etapa 1.
4 días	Etapa 2. (Incluye Análisis de Riesgo)
0,10 días	Informe.
0,10 días	Administración

La Auditoría se llevó a cabo en las siguientes fechas y sitios **(forma Presencial o Remota indicar el %)**:

N°	Fecha	Sitio
1	30 de octubre de 2023 - Presencial	Edificio Murillo Toro Cra. 8a entre calles 12A y 12B, Bogotá D.C.
2	31 de octubre de 2023 - Presencial	Edificio Murillo Toro Cra. 8a entre calles 12A y 12B, Bogotá D.C.

Si es evaluación multisitio se debe documentar qué procesos fueron auditados en cada sitio visitado:

N°	Sitio	Procesos evaluados
N/A	N/A	N/A

Los resultados detectados en esta auditoría están basados en los hallazgos y evidencias descritos en el check-list utilizado para su realización. Tras el análisis de todos ellos se han detectado 1 NCN menor.

6.3 No Conformidades identificadas

NCm1: Una vez revisado el Procedimiento de Gestión de incidentes SPI-TIC-PR-001 y los casos registrados en la mesa de gestión de servicios GI626476, GI566230 y GI532250 no fue posible evidenciar la trazabilidad del flujo y uso del Formato Incidente de Seguridad-Privacidad de la Información SPI-TIC-FM-004 con respuesta y evaluación de los incidentes de seguridad de la información presentados dentro del Ministerio, incumpliendo con lo establecido en el control A.16.1.5 del Anexo A de la Norma ISO 27001:2013.

6.4 Grado de Confianza asignado a las Auditorías Internas

Las auditorías internas son realizadas según el plan de auditoría que asegura que todos los elementos del sistema son auditados con regularidad.

Los auditores son subcontratados a una entidad externa

Las calificaciones del auditor, datos principales e informes de auditoría dan un Medio grado de confianza en los resultados de la auditoría.

¿Desviaciones del plan de auditoria? En caso de afirmativo por favor justifique: N/A	**SI** ☐	**NO** ☒
¿Existen cuestiones no resueltas? En caso de afirmativo por favor justifique: N/A	**SI** ☐	**NO** ☒
El cliente está controlando de manera eficiente el uso de los documentos y marca de certificación	**SI** ☒	**NO** ☐

Justificación: Se usa dentro de documentos controlados por el SIG y se respetan las condiciones de uso de marca de Global Colombia Certificación.

Verificación de la eficacia de las acciones correctivas tomadas con relación a no conformidades identificadas previamente, si aplica	**SI** ☐	**No Aplica** ☒

No se presentaron no conformidad anteriores por verificar su eficacia

¿Se declara conformidad y eficacia del sistema de gestión respecto a la capacidad del sistema de gestión para cumplir los requisitos legales aplicables y lograr los resultados esperados? **SI ☒** **NO ☐**

Resumen de evidencia:
El cliente presenta las evidencias de la implementación de los controles de seguridad de la información determinados, así mismo, evidencia del mantenimiento de la documentación principal del SGSI como lo son Política General de Seguridad de la Información, Alcance del SGSI, Declaración de Aplicabilidad, Gestión de Riesgos, Auditoría Interna e Indicadores de Desempeño.

¿Se declara conformidad respecto a la auditoría interna y proceso de revisión por la dirección? **SI ☒** **NO ☐**
Resumen de evidencia:
Se revisa auditoría interna y revisión por la dirección del año 2023 y se evidencia cumplimiento de los numerales 9.2 y 9.3 de la Norma ISO 27001:2013.

¿Han sido cumplidos los objetivos de la auditoria? **SI ☒** **NO ☐**
En caso de respuesta negativa por favor justifique la respuesta:
N/A

¿Es una evaluación de seguimiento? **SI ☒** **NO ☐**
En caso de afirmativo indique la comparación con los resultados de auditorías de certificación previas:
La Organización ha implementado riesgos de interrupción del servicio dentro de la gestión de riesgos de seguridad de la información. Se evidencia un alto compromiso por parte de la Alta Dirección, competencia y conocimiento por parte de los responsables del SGSI

¿La organización realiza la evaluación del tratamiento de quejas? **SI ☒** **NO ☐**
Justifique la respuesta
Por medio de la gestión de las PQRSD se tramitan las quejas y solicitudes en seguridad de la información en la entidad cumpliendo con los términos de ley.

¿Se genera progreso de las actividades planificadas dirigidas a la mejora continua? **SI ☒** **NO ☐**

Justifique la respuesta
Se amplió y fortaleció el equipo de trabajo de seguridad de la información dando cobertura y apoyo a todos los procesos del SGSI. Fortalecimiento en el ámbito de privacidad de la información y protección de datos personales. Los cambios no afectan el desempeño del sistema de gestión de seguridad de la información.

¿Se da continuidad en el control operacional por parte de la organización? **SI ☒** **NO ☐**
Justifique la respuesta
Se evidencian controles operacionales actualizados dentro de los procesos que hacen parte del SIG y que apoyan al SGSI

¿Se realizó revisión de cambios que afectan el sistema de gestión de la organización? **SI ☒** **NO ☐**
Justifique la respuesta
Se amplió y fortaleció el equipo de trabajo de seguridad de la información dando cobertura y apoyo a todos los procesos del SGSI. Fortalecimiento en el ámbito de privacidad de la información y protección de datos personales. Los cambios no afectan el desempeño del sistema de gestión de seguridad de la información.

7 REUNIÓN DE CLAUSURA

La Reunión de Clausura fue presenciada por el siguiente personal:

7.1 Representando a Cliente:

Rosa Lucia Ortega
Yesica Tatiana Vanegas
Julios Enrique Rosero
Nicol Velandia
Angela Cortes
Giovanni Espitia
Andrés David González

7.2 Representando a Global:

Edgar Fernando Suarez
Adriana Sandoval

Recomendación:

El equipo auditor recomienda **Mantener la certificación**
Justificación: Se evidencia el correcto funcionamiento del Sistema de Gestión de Seguridad de la información, la Organización controla del SGSI y documenta correctamente cualquier modificación que pueda causar un cambio significativo. Se evidencia compromiso de todos los colaboradores y se cuenta con una correcta implementación de los controles de seguridad a nivel corporativo.

El Alcance de la Certificación ha sido confirmado como: **"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"**

Fue explicado el procedimiento de cómo responder al informe.

El Auditor Líder volvió a confirmar la confidencialidad.

El Auditor Líder señaló el hecho de que como una Auditoría se lleva a cabo por muestreo era posible que existiesen no conformidades en distintos procesos no encontradas. El Cliente ha sido informado de que unas Auditorías Internas efectivas son fundamentales para el futuro del Sistema de Gestión.

El Auditor Líder ha agradecido a la organización la cooperación y hospitalidad mostrada durante el proceso de Auditoría global.

8 NOTAS GENERALES

Se debe hacer notar que se levantará una NCN Mayor si cualquiera de las NCN levantadas durante la auditoría no ha sido cerrada para la próxima visita que realizará el Auditor Líder.

Por consiguiente, es importante que la acción correctiva haya sido llevada a cabo e implantada eficazmente antes de la próxima visita.

Los cambios en la ubicación o en la plantilla (Director y representantes de gestión) deberían ser informados a Global Colombia Certificación tan pronto como sean prácticos después de que haya tenido lugar el cambio.

9 FORTALEZAS REFERENTES A LA IMPLEMENTACIÓN Y EFECTIVIDAD DE LOS REQUISITOS Y CONTROLES DEL SGSI

- 6.1.1. La Organización ha implementado riesgos de interrupción del servicio dentro de la gestión de riesgos de seguridad de la información, lo que permite gestionar y dar continuidad a la operación critica del Ministerio mediante la implementación de controles tecnológicos y organizacionales que se gestionan desde el ámbito de Continuidad del Negocio y Recuperación de Desastres.

10 OBSERVACIONES - REFERENTES A LA IMPLEMENTACIÓN Y EFECTIVIDAD DE LOS REQUISITOS Y CONTROLES DEL SGSI (puede llegar a ser una no conformidad si no se da tratamiento)

- 9.3: Fortalecer la fecha Retroalimentación sobre el desempeño del SGI que incluya tendencia relativa de no conformidades y acciones correctivas
- A.14.2.2: Los cambios a los sistemas dentro del ciclo de vida de desarrollo especificar como se controlan dando alcance dentro del procedimientos de CAMBIOS NORMALES GTI-TIC-PR-011 V 4

11 OPORTUNIDADES DE MEJORA REFERENTES A LA IMPLEMENTACIÓN Y EFECTIVIDAD DE LOS REQUISITOS Y CONTROLES DEL SGSI

- 6.1.2. Teniendo en cuenta que la Metodología de Gestión de Riesgos de Seguridad de la Información implementada por el Ministerio se lleva a cabo bajo la asociación activo-riesgo, convendría que la organización identificará y valorará riesgos teniendo en cuenta la criticidad estimada por cada uno de los atributos de seguridad de la información calificados para cada uno de los activos, con el fin de controlar la posible pérdida de integridad, confidencialidad y disponibilidad de los activos críticos de los procesos del SIG.
- 7.3: Generar mediciones objetivas para las encuestas del SGI que den resultados frente a cumplimiento para generar planes de acción efectivos frente a cada sistema de gestión. La actual forma de medición en la mayoría de las preguntas es abierta, y no apunta a medir requisitos exactos de validación de cumplimiento.
- A.17.1.2: De acuerdo con los requisitos de continuidad de la seguridad de la información, MINTIC debería establecer, documentar, implementar y mantener los controles de compensación para los controles de seguridad de la información que no se pueden mantener durante una situación adversa en, al momento de toma de evidencia no se encuentra dentro del documento: BIA ANALISIS DE IMPACTO A LAS OPERACIONES: SPI-TIC-MA-003. V 2, 21/11/2022. lo ideal es tenerlo dentro del plan de mejora que están realizando con el proveedor externo.

12 NO APLICABILIDAD Y JUSTIFICACIONES

Punto de la Norma	Justificación
N/A	N/A
N/A	N/A

Espacio exclusivo para la Dirección Técnica
¿la información plasmada está acorde a lo evaluado por el auditor Líder?
SI _X_ NO ____

Fecha de Realización del Informe	1 de noviembre de 2023
Realizado Por	Edgar Fernando Suarez M.
Cargo	Auditor Líder

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