

	GLOBAL COLOMBIA CERTIFICACIÓN S.A.S.		
	INFORME DE AUDITORIA ETAPA II ISO/IEC 27001:2013		
	03.2-F21	VER 5.0	Página 1 de 11

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

Nº CLIENTE: SG-049

ALCANCE EMPRESA: 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 SOA versión 1

TIPO DE AUDITORIA: Primer Seguimiento

FECHA(S) DE LA AUDITORÍA: 19/10/2022 - 21/10/2022

NORMA DE REFERENCIA: NTC ISO/IEC 27001:2013

AUDITOR LÍDER: Jesús David Díaz.

AUDITOR(ES): Andrés Zapata.

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 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.

3 PROCESOS AUDITADOS:

- Seguridad y privacidad de la Información
- Gestión de TI

	GLOBAL COLOMBIA CERTIFICACIÓN S.A.S.		
	INFORME DE AUDITORIA ETAPA II ISO/IEC 27001:2013		
	03.2-F21	VER 5.0	Página 2 de 11

- Direccionamiento Estratégico
- Gestión de Atención a Grupos de Interés
- Fortalecimiento Organizacional
- Gestión de Talento Humano
- Gestión de Compras y Contratación
- Gestión de Recursos Administrativos
- Gestión Jurídica
- Control Interno Disciplinario
- Comunicación Estratégica

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, Última 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 en un lugar 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 recomienda mantener la certificación.

5 REUNIÓN DE APERTURA

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

	GLOBAL COLOMBIA CERTIFICACIÓN S.A.S.		
	INFORME DE AUDITORIA ETAPA II ISO/IEC 27001:2013		
	03.2-F21	VER 5.0	Página 3 de 11

5.1 Representando a Cliente:

Sandra Urrutia – Ministra TIC.
Rosa Lucía Ortega
Julio Enrique Rosero Torres
Angélica Cortés
Sergio Andrés Ramos
Giovanni Espitia
Andrés Díaz Molina

5.2 Representando a Global:

Jesús David Díaz – Auditor Líder de Seguridad de la Información.
Andrés Zapara - Auditor

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 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 en el trabajo del equipo auditor, estos estarán acompañados por personal de la empresa, 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**

	GLOBAL COLOMBIA CERTIFICACIÓN S.A.S.		
	INFORME DE AUDITORIA ETAPA II ISO/IEC 27001:2013		
	03.2-F21	VER 5.0	Página 4 de 11

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 duró **5** días siendo visitado **1** lugar/es. La distribución del tiempo empleado en la evaluación es la siguiente:

0,10 días	Análisis del Sistema Documental y elaboración del Programa.
N.A. días	Etapa 1.
5 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:

N°	Fecha	Sitio
01	19 de Octubre de 2022.	Edificio Murillo Toro Cra. 8ª entre Calles 12ª y 12B, Bogotá D.C.
02	20 de Octubre de 2022.	Edificio Murillo Toro Cra. 8ª entre Calles 12ª y 12B, Bogotá D.C.
03	21 de Octubre de 2022	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.

	GLOBAL COLOMBIA CERTIFICACIÓN S.A.S.	
	INFORME DE AUDITORIA ETAPA II ISO/IEC 27001:2013	
	03.2-F21	VER 5.0

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 0 NCN's menores.

6.3 No Conformidades identificadas

No se presentaron no conformidades

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 auditoría? SI NO
En caso de afirmativo por favor justifique: N.A.

¿Existen cuestiones no resueltas? SI NO
En caso de afirmativo por favor justifique: N.A.

El cliente está controlando de manera eficiente el uso de los documentos y marca de certificación SI NO

Justificación: El cliente controla de manera eficiente los documentos y la marca de certificación, evidenciado durante la realización de la auditoría de Seguimiento. En el PORTAL web del Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC, se muestra la marca de Certificación por parte de GLOBAL COLOMBIA CERTIFICACIÓN y publicado el CERTIFICADO DE CONFORMIDAD del estándar ISO/IEC 27001:2013

Verificación de la eficacia de las acciones correctivas tomadas con relación a no conformidades identificadas previamente, si aplica SI No Aplica
N.A.



GLOBAL COLOMBIA CERTIFICACIÓN S.A.S.

**INFORME DE AUDITORIA ETAPA II
ISO/IEC 27001:2013**

03.2-F21

VER 5.0

Página 6 de 11

¿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:

Se evidencia que la entidad cumple con todos los requisitos estatutarios, reglamentarios y contractuales pertinentes; se verifica el cumplimiento de las leyes 1581 de 2.012, ley 23 de 1982 y otras aplicables a la prestación del servicio.

¿Se declara conformidad respecto a la auditoría interna y proceso de revisión por la dirección?

SI

NO

Resumen de evidencia:

Se declara conformidad de la auditoría interna realizada al Sistema de Gestión de Seguridad y privacidad de la Información del **MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES**, Se pudo validar que dentro del Ministerio durante el año 2022, se realizó el seguimiento sobre auditoría interna, se evidencia organización a través de la definición de documentos como MANUAL DEL MIG, LINEAMIENTOS PREVIOS A LA REALIZACIÓN DEL CICLO DE AUDITORÍAS INTERNAS DEL SISTEMA INTEGRADO DE GESTIÓN, FORMULACIÓN, SEGUIMIENTO Y CIERRE DE ACCIONES DE MEJORA, CICLO DE AUDITORÍAS INTERNAS PARA EL SISTEMA INTEGRADO DE GESTIÓN, PROGRAMA ANUAL DE AUDITORIAS INTERNAS, PLAN DE AUDITORÍA INTERNA DE SISTEMAS DE GESTIÓN, ACTAS DE REUNIÓN DE AUDITORÍA INTERNA E INFORME DE AUDITORÍA INTERNA DEL SISTEMA DE GESTIÓN. Para revisión por dirección se pudo determinar la **CONFORMIDAD**, esta fue realizada y en esta se evidenciaron las consideraciones tales como el estado de las acciones con relación a las revisiones previas por la dirección, cambios en las cuestiones externas e internas, retroalimentación sobre el desempeño de la seguridad de la información incluyendo tendencias relacionadas con las No Conformidades y acciones correctivas, resultado y seguimiento de las mediciones, resultados de auditorías, entre otros

¿Han sido cumplidos los objetivos de la auditoría?

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:

Al comparar los resultados de auditorías de Certificación previas, se puede notar la consistencia que se tiene con la implementación del Sistema de Gestión de Seguridad y Privacidad de la Información.

	GLOBAL COLOMBIA CERTIFICACIÓN S.A.S.	
	INFORME DE AUDITORIA ETAPA II ISO/IEC 27001:2013	
	03.2-F21	VER 5.0

¿La organización realiza la evaluación del tratamiento de quejas? SI NO
 Justifique la respuesta
 Se evidencia que la entidad realiza el tratamiento de los requerimientos sobre las quejas a la entidad

¿Se genera progreso de las actividades planificadas dirigidas a la mejora continua? SI NO
 Justifique la respuesta
 Se evidencia que la entidad realiza actividades enfocadas a la mejora como se encuentra en el registro MIG-TIC-PR-003 Formulación cierre y de acciones de mejora.

¿Se da continuidad en el control operacional por parte de la organización? SI NO
 Justifique la respuesta
 Se verifica que la entidad mantiene el control operacional con los controles establecidos en los procesos

¿Se realizó revisión de cambios que afectan el sistema de gestión de la organización? SI NO
 Justifique la respuesta
 Se ha incluido un nuevo proceso (Arquitectura Empresarial) dentro de los procesos estratégicos del Sistema de Gestión de Seguridad de la información de la entidad.

7 REUNIÓN DE CLAUSURA

La Reunión de Clausura fue presenciada por el siguiente personal:

7.1 Representando a Cliente:

Andrés Diaz Molina.
 Giovanni Espitia Roa.
 Rosa Lucía Ortega Muleth.
 Julio E Rosero Torres.
 Sergio Andrés Ramos.
 Angélica Cortés.

	GLOBAL COLOMBIA CERTIFICACIÓN S.A.S.	
	INFORME DE AUDITORIA ETAPA II ISO/IEC 27001:2013	
	03.2-F21	VER 5.0

7.2 Representando a Global:

Andrés Zapata (Auditor)

Recomendación:

El equipo auditor recomienda **Mantener la certificación**

Justificación: Se evidencia cumplimiento de todos los requisitos de la Norma, legales aplicables y los dispuestos por la organización.

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 de que existiesen no conformidades en distintas áreas 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 Empresa 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.

	GLOBAL COLOMBIA CERTIFICACIÓN S.A.S.		
	INFORME DE AUDITORIA ETAPA II ISO/IEC 27001:2013		
	03.2-F21	VER 5.0	Página 9 de 11

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

- La dirección posee gran compromiso en la implementación del sistema de gestión de seguridad de la información, teniendo en cuenta que destina los recursos necesarios para su correcta ejecución y el respectivo seguimiento del Sistema de Gestión de Seguridad y Privacidad de la Información.
- Se evidencia un **alto compromiso de las partes interesadas relevantes**, especialmente en los líderes de los procesos para el logro efectivo de los resultados de la operación del sistema de gestión de seguridad y privacidad de la información.
- Se evidencia un claro **empoderamiento del equipo de trabajo**, todas y cada una de las áreas que tienen relación con el sistema de gestión de seguridad de la información, lo cual fortalece la cultura hacia la mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información.
- La Gestión de riesgos realizada en la compañía establece las bases para la mejora continua del SGSI, Se tienen estimados los riesgos de acuerdo a criterios de Confidencialidad, Disponibilidad, Integridad de la seguridad de la información y prioridades de la organización. Se resalta la identificación de forma clara los riesgos y la manera en que son tratados para lograr mitigarlos y controlarlos.
- Se evidencia un alto conocimiento en las herramientas tecnológicas que se utilizan para la construcción de evidencias dentro del sistema de gestión de seguridad de la información.
- La entidad demuestra que cuenta con los recursos necesarios y suficientes para establecer un avanzado nivel de madurez del sistema de gestión de seguridad de la información
- **Resaltar el compromiso** que se tiene por parte del equipo talento humanos en cada uno de los procesos que se desarrollan relacionados con la **seguridad y privacidad de la información**, a partir que se inicia el proceso de vinculación de un candidato realizando las verificaciones de seguridad pertinentes, hasta todo el proceso de desvinculación que se da en la entidad, así mismo, como se efectúa la formación, educación y capacitación en temas relacionados con seguridad y privacidad de la información. Como evidencia se pudo validar la información a través de la revisión de algunas carpetas físicas y digital de algunos funcionarios de la entidad, contratos por orden de prestación de servicios y funcionarios de planta del ministerio.
- Se incluyen controles seguridad a nivel de red, se validó la efectiva implementación de herramientas de seguridad perimetral con políticas establecidas a nivel de firewall, antivirus, VPNS y directorio activo AD, lo que permite garantizar el

	GLOBAL COLOMBIA CERTIFICACIÓN S.A.S.	
	INFORME DE AUDITORIA ETAPA II ISO/IEC 27001:2013	
	03.2-F21	VER 5.0

funcionamiento adecuado de la infraestructura tecnológica de la organización y la operación continua de los servicios, adicional contener cualquier técnica o amenaza de ciberataque que exista en la actualidad.

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)

N.A.

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

- se sugiere que la organización realice revisión sobre la publicación traslado de acta de legalización segundo y tercer periodo, que corresponde al proceso de Gestión documental, y traslados al archivo general de la nación al validar se pudo evidenciar que no se encontró publicados dentro del portal del **ministerio** el cual afirma que estas fueron asignadas con vigencia del año anterior. Lo cual toma como referencia el control de la norma a.8.3.2 correspondiente a la gestión de medios.

12 EXCLUSIONES Y JUSTIFICACIONES

N.A.

<u>Punto de la Norma</u>	<u>Justificación</u>
N.A.	N.A.

Fecha de Realización del Informe	26 de Octubre de 2022.
Realizado Por	Jesús David Díaz.
Cargo	Auditor Líder.

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



GLOBAL COLOMBIA CERTIFICACIÓN S.A.S.

**INFORME DE AUDITORIA ETAPA II
ISO/IEC 27001:2013**

03.2-F21

VER 5.0

Página 11 de 11