1. INFORMACIÓN GENERAL

1.1. ORGANIZACIÓN

CÁMARA DE COMERCIO DEL ORIENTE ANTIOQUEÑO

1.2. SITIO WEB: https://www.ccoa.org.co/

1.3. LOCALIZACIÓN DEL SITIO PERMANENTE PRINCIPAL: Carrera 47 No. 64 A – 263 Vía Belén Kilómetro 2 Vía Rionegro, Rionegro - Antioquia – Colombia

Si la certificación cubre más de un sitio permanente donde se realicen actividades del sistema de gestión, indicar la localización de cada uno.

ISO/IEC 27001:2013

Dirección del sitio permanente (diferente al sitio principal)	Localización (ciudad - país)	Actividades del sistema de gestión, desarrollados en este sitio, que estén cubiertas en el alcance
Calle 20 No. 22-59	La Ceja, Antioquia - Colombia	Todas las actividades del alcance
Carrera 31 No. 31–28	Guatapé, Antioquia - Colombia	Todas las actividades del alcance
Calle 7 entre carreras 5 y 6, primer piso del palacio municipal	Sonsón, Antioquia - Colombia	Todas las actividades del alcance

ISO 9001:2015

Dirección del sitio permanente (diferente al sitio principal)	Localización (ciudad - país)	Actividades del sistema de gestión, desarrollados en este sitio, que estén cubiertas en el alcance
No Aplica		

1.4. ALCANCE DE LA CERTIFICACIÓN:

ISO/IEC 27001:2013

Prestación de servicios para la gestión de los registros públicos. Declaración de aplicabilidad SI-DA-SE-01 Versión 4 de 2020-08-10.

Provision of services for the management of the public registrations. Statement Applicability SI-DA-SE-01 Version 4 dated 2020-08-10.

ISO 9001:2015

Prestación de servicios de: Afiliación, Registro Público, Información Comercial y Formación Empresarial, en la sede de Rionegro.
No aplica: 8.3 Diseño y desarrollo de productos y servicios.

Services provision of: Affiliation, public records, commercial information and business formation, in the Rionegro City.

1.5. CÓDIGO IAF: SI 7, 39-2

1.6. CATEGORÍA DE ISO/TS 22003: No Aplica

1.7. REQUISITOS DE SISTEMA DE GESTIÓN: ISO/IEC 27001:2013; ISO 9001:2015

1.8. REPRESENTANTE DE LA ORGANIZACIÓN

Nombre:	Maryori Ocampo Ocampo
Cargo:	Líder de Planeación Estratégica y Gestión Organizacional
Correo electrónico	pr.planeacion@ccoa.org.co

1.9. TIPO DE AUDITORÍA:

□ Inicial o de Otorgamiento

X Seguimiento **□ Renovación** **□ Ampliación** **□ Reducción** **□ Reactivación** **□ Extraordinaria** **□ Actualización** **□ Migración (aplica para ISO 45001)**
Aplica toma de muestra por multisitio: Si X No □ para ISO 27001:2013 Si □ No X para ISO 9001:2015
Auditoría combinada: Si □ No X
Auditoría integrada: Si □ No X

1.10. Tiempo de auditoría	FECHA	Días de auditoría)
Etapa 1 (Si aplica)	N.A.	N.A.
Preparación de la auditoría en sitio y elaboración del plan	2021-09-25	1.0
Auditoria remota	2021-10-12,13,14,15	3.5
Auditoría en sitio	N.A.	N.A.

1.11. EQUIPO AUDITOR	
Auditor líder	Jairo Yobany Vargas G.
Auditor	Libardo Chávez Pérez En su etapa de entrenamiento para ser auditor líder ISO/IEC 27001 e ISO 9001, desempeñó el rol de Auditor)
Experto Técnico	Claudia Patricia Serna Gallego - CPS-
Observador – Profesional de Apoyo	No Aplica

1.12. DATOS DEL CERTIFICADO DE SISTEMA DE GESTIÓN		
	ISO/IEC 27001:2013	ISO 9001:2015
Código asignado por ICONTEC	SI CER577303	SC5057-1
Fecha de aprobación inicial	2017-12-22	2007-12-12
Fecha de próximo vencimiento:	2023-12-21	2022-12-11

2. OBJETIVOS DE LA AUDITORIA

2.1 Determinar la conformidad del Sistema de Gestión con los requisitos de la norma de Sistema de Gestión.

2.2 Determinar la capacidad del Sistema de Gestión para asegurar que la Organización cumple los requisitos legales, reglamentarios y contractuales aplicables en el alcance del Sistema de Gestión y a la norma de requisitos de gestión.

2.3 Determinar la eficacia del Sistema de Gestión para asegurar que la Organización puede tener expectativas razonables con relación al cumplimiento de los objetivos especificados.

2.4 Identificar áreas de mejora potencial del Sistema de Gestión

3. ACTIVIDADES DESARROLLADAS

3.1 Los criterios de la auditoría incluyen la norma de requisitos de sistema de gestión, la información documentada del sistema de gestión establecida por la organización para cumplir los requisitos de la norma, otros requisitos aplicables que la organización suscriba y documentos de origen externo aplicables.

3.2 El alcance de la auditoría, las unidades organizacionales o procesos auditados se relacionan en el plan de auditoría que hace parte de este informe.

3.3 La auditoría se realizó por toma de muestra de evidencias de las actividades y resultados de la Organización y por ello tiene asociada la incertidumbre, por no ser posible verificar toda la información documentada.

3.4 Se verificó la capacidad de cumplimiento de los requisitos legales o reglamentarios aplicables en el alcance del Sistema de Gestión, establecidos mediante su identificación, la planificación de su cumplimiento, la implementación y la verificación por parte de la Organización de su cumplimiento.

3.5 El equipo auditor manejó la información documentada suministrada por la Organización en forma confidencial y la retornó a la Organización, en forma física o eliminó la entregada en otro medio, solicitada antes y durante el proceso de auditoría.

3.6 Al haberse ejecutado la auditoría de acuerdo con lo establecido en el plan de auditoría, se cumplieron los objetivos de ésta.

3.7 ¿Se evidenciaron las acciones tomadas por la Organización para solucionar las áreas de preocupación, reportadas en el informe de la Etapa 1? (Se aplica solo para auditorías iniciales o de otorgamiento):
Si ☐ No ☐ N.A ☑

3.8 Si se aplicó toma de muestra de múltiples sitios, indicar cuáles sitios permanentes se auditaron y en que fechas
Si ☑ No ☐ N.A ☐

Sede	Fecha
Carrera 47 No. 64 A – 263 Vía Belén Kilómetro 2 Vía Rionegro, Rionegro - Antioquia – Colombia	2021-10-12 al 2021-10-15
Calle 20 No. 22-59 La Ceja, Antioquia, Colombia	2021-10-13
Guatapé, Antioquia - Colombia	2021-10-13

3.9 ¿En el caso del Sistema de Gestión auditado están justificadas las exclusiones o requisitos no aplicables acorde con lo requerido en el respectivo referencial?
Si ☑ No ☐ N.A ☐

ISO 9001:2015

Numeral	Justificación

3. ACTIVIDADES DESARROLLADAS

8.3 Diseño y desarrollo de productos y servicios	Los servicios prestados incluidos en el alcance están completamente normalizados por la legislación colombiana
7.1.5.2 Trazabilidad de las mediciones	La organización no emplea para la prestación de los servicios equipos que requieran estar sujetos a control metrológico.

ISO/IEC 27001:2013

Numeral	Justificación
A.6.2.2 Teletrabajo	La Cámara de Comercio del Oriente Antioqueño, no ha establecido el Teletrabajo como una modalidad valida, por lo que no aplica y no está implementada.
A.11.1.6 Áreas de despacho y carga	La cámara de comercio no dispone de áreas de despacho y carga
A.12.1.4 Registro y seguimiento	La cámara de comercio no realiza desarrollos de software a nivel interno y cuando surge la necesidad, se surte a través de contrataciones externas.
A.14.2.2 Procedimientos de control de cambios en sistemas	
A.14.2.6 Ambiente de desarrollo seguro	
A.14.2.8 Pruebas de seguridad de sistemas	

3.10 ¿Se auditaron actividades en sitios temporales o fuera del sitio de acuerdo al listado de contratos o proyectos entregados por la Organización?
Si ☐ No ☐ N.A ☑

3.11 ¿Es una auditoría de ampliación o reducción?
Si ☐ No ☑ N.A ☐

3.12 En el caso de los esquemas en los que es aplicable el requisito de diseño y desarrollo del producto o servicio (Por ejemplo, el numeral 8.3 de la norma ISO 9001:2015), este se incluye en el alcance del certificado?
Si ☐ No ☐ N.A. ☑

3.13 ¿Existen requisitos legales para el funcionamiento u operación de la Organización o los proyectos que realiza, por ejemplo, habilitación, registro sanitario, licencia de funcionamiento, licencia de construcción, licencia o permisos ambientales en los que la Organización sea responsable?:
Si ☑ No ☐ N.A ☐

Decreto No. 1411 de 1987-07-29, Acto de creación de la Cámara. De la Superintendencia de Industria Comercio, Circular única de la Superintendencia de Industria y Comercio, título 8, Cámaras de Comercio

3. ACTIVIDADES DESARROLLADAS

3.14 ¿Se evidencian cambios significativos en la Organización, desde la anterior auditoría, por ejemplo, relacionados con Alta dirección, estructura organizacional, sitios permanentes bajo el alcance de la certificación, cambios en el alcance de la certificación diferentes a ampliación o reducción, entre otros?
Si ☑ No ☐ N.A ☐

Debido a la emergencia presentada por el COVID-19, las restricciones de movilidad entre ciudades y las disposiciones emitidas por la UT de Certificación de Sistemas de Gestión se realizó el análisis basado en el desempeño de la organización (no conformidades anteriores / recurrentes, quejas / reclamaciones, incidentes de servicio, etc.) y los riesgos tales como (comunicación, tecnología, disponibilidad de información, controles de acceso, etc.). Para los riesgos se confirmó con la empresa tiene la capacidad de utilizar medios de comunicación interactivos (se evidenció que la organización contaba con todas las herramientas tecnológicas de acceso a información, ancho de banda suficiente, información digitalizada y disponía de personas en sitio con cámaras de alta resolución para mostrar espacios físicos, controles de acceso y controles ambientales entre algunos otros), por lo tanto, se podía asegurar el cumplimiento del plan de auditoria y los objetivos establecidos para la misma, razón por la cual se confirmó la viabilidad de poder realizar la auditoria parcialmente remota.

¿Debido a los cambios que ha reportado la Organización, se requiere aumentar el tiempo de auditoría de seguimiento?
Si ☐ No ☑

3.15 ¿Si la Organización realiza actividades del alcance en turnos nocturnos que no pueden ser visitadas en el turno diurno, estas fueron auditadas en esta auditoría?
Si ☐ No ☐ N.A. ☑

3.16 Para sistemas de gestión de calidad; ¿Se subcontratan con proveedores el suministro de productos y servicios que hacen parte del alcance del certificado?
Si ☑ No ☐ N.A ☐
¿En caso afirmativo, se encontraron controlados los proveedores de estos productos y servicios?
Si ☑ No ☐ N.A ☐

Servicios y productos incluidos en el alcance que son proporcionados al cliente por un tercero en nombre de la organización auditada:	Proveedor:
Proceso de Formación Empresarial	Docentes

Se contratan docentes para atender las actividades del proceso de Formación Empresarial, el control lo realiza el líder del proceso y se evidencia dicho control a través de las evaluaciones de desempeño realizadas por estudiantes tanto al programa como al docente y el seguimiento es llevado por el proceso de contratación

3.17 ¿Se presentaron durante la auditoria cambios que hayan impedido cumplir con el plan de auditoría inicialmente acordado con la Organización?
Si ☐ No ☑

3.18 ¿Existen aspectos o resultados significativos de esta auditoría que incidan en el programa de auditoría del ciclo de certificación?
Si ☐ No ☑

3. ACTIVIDADES DESARROLLADAS

3.19 ¿Quedaron puntos no resueltos en los casos en los cuales se presentaron diferencias de opinión sobre las NC identificadas durante la auditoría?
Si ☐ No ☑

3.20 ¿Aplica restauración para este servicio?
Si ☐ No ☑

3.21 Se verificó si la Organización implementó o no, el plan de acción establecido para solucionar las no conformidades menores pendientes de la auditoría anterior de ICONTEC y si fueron eficaces.
Si ☑ No ☐ N.A. ☐

ISO/IEC 27001

NC	Descripción de la no conformidad (se relaciona el numeral de la norma y la evidencia del incumplimiento)	Evidencia obtenida que soporta la solución	¿Fue eficaz la acción? Si/No
1	Numeral 7.5.2.c) Información documentada No han sido apropiadas las actividades de revisión y aprobación con respecto a la conveniencia y adecuación de algunos documentos creados y actualizados al interior de la organización. Evidencia: Se evidencia a fecha del ejercicio de auditoría que el documento Declaración de aplicabilidad no tiene asignado código del sistema de gestión de acuerdo con la nomenclatura definida por la organización. De igual manera el mencionado documento se identifica con un código numérico diferente en el listado maestro de documentos y en el repositorio de gestión documental soportado por la herramienta ISOTOOLS. El documento en mención se encuentra vigente, revisado y aprobado, así como conformante del repositorio de gestión documental de la organización.	Se evidencia la implementación del Patrón Operacional de información documentada GC-PO-MC-01 actualizado en lo que refiere a la estructura documental del sistema de gestión y con controles. Así mismo se evidenció la documentación de procesos actualizada y el informe de los resultados de la de revisión de información documentada de los procesos.	Si

3. ACTIVIDADES DESARROLLADAS

2	Numeral A.14.1.1 Análisis y especificación de requisitos de seguridad de la información. No se han incluido los requisitos de seguridad de la información como mejoras para algunos sistemas de información existentes al interior de la organización. Evidencia: Se evidencia a fecha del ejercicio de auditoria que el aplicativo Seguimiento a las compras GA-FF-CM-14 con fecha de actualización del 15/12/2019, presentó un error en su formulación que fue reportado a la mesa de ayuda como incidente en fecha 18 de junio de 2020. El error sin embargo no se corrigió, razón por la cual se produjo la calificación errónea de uno de los proveedores de la organización, afectando de igual forma el indicador de cumplimiento del proveedor afectado.	Se evidenció la adición de los requisitos de seguridad de la información en el formato de ISOTOOLS, utilizado para la solicitud de mejoras en sistemas de información existentes en la Cámara. Así mismo se evidenció el inventario de activos de información actualizado en línea con los resultados de la revisión que se realizó en los diferentes procesos.	Si

ISO 9001

NC	Descripción de la no conformidad (se relaciona el numeral de la norma y la evidencia del incumplimiento)	Evidencia obtenida que soporta la solución	¿Fue eficaz la acción? Si/No
1	Numeral 8.4.1 Control de los productos y servicios suministrados externamente. Generalidades. La organización no cuenta con información documentada de las actividades que se realizan para el seguimiento del desempeño y la reevaluación de los proveedores externos. Evidencia: En el documento GA-PO-CM-06 “Gestión de Proveedores” se establece que el informe individual de cada proveedor se enviara a través del	Se evidencia la implementación Patrón operacional GA-PO-CM-06 “Gestión de Proveedores, ajustado con los controles de revisión, aprobación y seguimiento necesarios. Así mismo se evidenció el establecimiento de tiempos en el Patrón Operacional para socializar los resultados de la evaluación de proveedores una vez que se finalice con la evaluación.	Si

3. ACTIVIDADES DESARROLLADAS

	correo electrónico para socializar los resultados y conjuntamente generar planes de acción, sin embargo, no se evidencia el envío de los resultados de la evaluación de 2019 y de 2020 para los proveedores Ethical Security y Alo Global.		

2. HALLAZGOS DE LA AUDITORÍA

Como resultado de la auditoría, el equipo auditor declara la conformidad y eficacia del sistema de gestión auditado basados en el muestreo realizado. A continuación, se hace relación de los hallazgos de auditoría.

4.1 Hallazgos que apoyan la conformidad del sistema de gestión con los requisitos.

- ☑ A partir de la elaboración de la planeación estratégica, la Alta Dirección logró visualizar el estado actual de la Cámara de Comercio del Oriente Antioqueño y proyectar mejoramiento en los servicios.
- ☑ Se destacan las diferentes metodologías utilizadas en el ejercicio de planeación estratégica y la manera coherente que le permite su establecimiento hasta el nivel de planes y actividades, porque se alcanzó inmersión completa en cada uno de los procesos del Sistema de Gestión Integral - SGI.
- ☑ La rigurosidad que se evidencia tanto en el patrón operacional de las auditorías internas como en las acciones correctivas, dejan ver el grado de compromiso en todos los niveles de la organización para con el SGI.
- ☑ El resultado superior de las mediciones de los indicadores evidencia el alto grado de madurez del SGI incluyendo procesos de cara al cliente como servicios empresariales y comunicaciones.
- ☑ La ampliación del portafolio en cuatro nuevos servicios (vitrina empresarial, consultorio de comercio exterior, consultorio de desarrollo empresarial y canales de atención), materializa el inicio de la estrategia de diversificación, la cual con seguridad a futuro le garantizará la permanencia a largo plazo a la Cámara de Comercio del Oriente Antioqueño.
- ☑ El nivel de granularidad que tiene en las necesidades y expectativas de las partes interesadas, el cual les permite determinar planes de comunicación y estrategias enfocadas a cada uno de esos grupos de interés, incrementando así la probabilidad de éxito de las mismas.
- ☑ El programa e-mega que busca desarrollar estrategias y buenas prácticas que permiten a las empresas pequeñas, medianas y grandes, incrementar su competitividad y rentabilidad.
- ☑ La integración entre diferentes sistemas de información como el CRM y el SII, permitiendo la centralización y unificación de la información para así lograr una mejora gestión sobre la misma.
- ☑ La nueva estructura digital que presenta el periódico de la Cámara y el aprovechamiento de diferentes canales digitales para la divulgación de la información utilizando técnicas como los textos multimodales.
- ☑ El servicio que presta la intranet para el proceso de Gestión de los Recursos Públicos, permitiéndole a la Cámara centralizar la información relacionada con el que hacer de los procesos, adicionalmente estandariza las formas de dar respuesta de la Cámara a sus usuarios, generando adecuada imagen corporativa y unificando criterios.
- ☑ La base de datos de conocimiento presentada en el proceso de Gestión de Registros Públicos permite tomar acciones preventivas para tratar las salidas no conformes y así evitar que sea el cliente quien detecte o reporte estos eventos.

2. HALLAZGOS DE LA AUDITORÍA

- ☑ Las buenas prácticas evidenciadas en el archivo físico de la sede de la Ceja lo cual permite la conservación en inmejorables condiciones de los registros y documentos de la Cámara.
- ☑ La planificación, control, seguimiento, cierre y lecciones aprendidas que genera la aplicación del patrón operacional (GE.PO.DE.02 Versión: 4) de la Gestión de cambios, permite la permanente mejora del SGI.
- ☑ El resultado de la medición del indicador de "Quejas, reclamos y felicitaciones", en donde la mayor porción de la gráfica corresponde a felicitaciones, lo cual evidencia la excelente gestión realizada por la Cámara.
- ☑ En el firewall se destaca la identificación e implementación del control denominado listas negras, sin duda incrementa la seguridad bloqueando todas las posibles fuentes de ataques.
- ☑ Se destaca la integridad evidenciada entre los cronogramas de mantenimiento (preventivo y correctivo) y los controles implementados en la matriz de riesgo.
- ☑ Se destaca la rigurosidad en el registro y trazabilidad de las compras iniciando con la solicitud, hasta la verificación de la entrega del producto o servicio contratado, evidenciando un excelente control de este proceso.
- ☑ Se destacan los trabajos de monitoreo, mantenimiento y mejora de la capacidad de los equipos ubicados en los datacenters y centros de cableado, porque se implementaron para mejorar la capacidad en almacenamiento de bases de datos y archivos, procesamiento de los servidores principales y la capacidad de los canales de comunicaciones.
- ☑ Se destacan los informes de monitoreo y gestión de cambios de la plataforma tecnológica por el seguimiento a las tareas pendientes registradas en la mesa de ayuda, porque han logrado realizar análisis y aplicar estrategias de mejoramiento, complementando así la metodología de administración de la infraestructura de tecnológica.

4.2 Oportunidades de mejora

- ☑ La redacción de las no conformidades es susceptible de mejorarse mediante una descripción concreta, de tal forma que no de pie a interpretaciones para el caso de las auditorias.
- ☑ Es conveniente que todas las mediciones de los indicadores se realicen y se presenten en la herramienta establecida para este fin, de manera que la información se encuentre centralizada y se facilite su consulta y utilización.
- ☑ Continuar con la revisión del antivirus durante todo el ejercicio de auditoría interna con el fin de validar el nivel de protección para el cual fue implementado.
- ☑ Facilitar el enlace entre la caracterización del proceso y los activos de información del mismo, facilitaría su ubicación y apropiación.
- ☑ La adquisición de tecnologías tipo SIEM (Security Information and Event Management) mediante la integración de dispositivos y configuración de casos de uso o políticas, ayudará al control e incremento de la seguridad de manera significativa, es una herramienta en la que se centraliza la información y se integra con otras herramientas de detección de amenazas.
- ☑ La implementación de tecnologías y servicios tipo SOC (Security Operations Center) ayudará de manera significativa a detectar, analizar y corregir incidentes de ciberseguridad, así mismo permitirá supervisar y analizar la actividad en redes, servidores, terminales, bases de datos, aplicaciones, sitios web y otros sistemas en busca de señales débiles o comportamientos anormales que puedan indicar un incidente de seguridad.
- ☑ Es conveniente la integración entre las aplicaciones que interviene en el proceso de las compras de manera que les permita facilitar la gestión de las mismas y minimizar la probabilidad de errores durante las diferentes etapas.
- ☑ Fortalecer la exigencia en la formalidad de la firma del acuerdo de confidencialidad con los terceros según aplique.
- ☑ En la selección de proveedores, es conveniente aprovechar la coyuntura de integración de las aplicaciones GSP/ y WM de manera que esta selección de proveedores se realice de manera digital completamente y su trazabilidad haga parte de dichas aplicaciones. Así mismo en el informe de la

2. HALLAZGOS DE LA AUDITORÍA

auditoría realizada a los proveedores mejorar las conclusiones y asignar un espacio para las no conformidades.

- ☑ Tomar como insumo el inventario de bases de datos que se le envía a la SIC, como un parámetro que les permita re definir la política de acceso a los correos personales.
- ☑ A modo de consulta revisar:
  - NIST Cybersecurity Framework (El Marco de Ciberseguridad del NIST) y la norma ISO/IEC 27032 "Tecnologías de la información. Técnicas de seguridad - Directrices para la Ciberseguridad", de manera que se utilicen como modelo para implementar sus buenas prácticas en ciberseguridad.
  - ISO/IEC 22317:2015. Sistema de Gestión de Continuidad de Negocio. Directrices para el Análisis de Impacto en el Negocio, para mejorar la matriz BIA (Business Impact Analysis).
  - ISO/IEC 27701: 2019. Técnicas de seguridad - Extensión a ISO / IEC 27001 e ISO / IEC 27002 para la gestión de la información de privacidad - Requisitos y directrices, permitirá contribuir con la mejora continua en la implementación del marco legal Colombiano en materia de protección de datos personales.

5. INFORMACIÓN RELACIONADA CON EL DESEMPEÑO Y LA EFICACIA DEL SISTEMA DE GESTION

5.1. Análisis de la eficacia del Sistema de Gestión certificado

5.1.1. Reclamaciones o Quejas válidas del cliente en el Sistema de Gestión que aplique durante el último año.

Principales quejas o reclamaciones recurrentes	Principal causa	Acciones tomadas
Registros Públicos	Tramites con usuarios	Se evidencia que la organización: ⊕ Habilitó un PAI de apoyo quedando así cinco puntos de atención. ⊕ Habilitó una caja para atender solo el servicio de certificados. ⊕ Realizó campaña por a través de CRM acerca del servicio del certificado virtual dirigido a las personas que han solicitado certificado en las sedes. ⊕ Plan de capacitación y reentrenamiento a la Auxiliar de Servicio al Cliente en: Protocolo de servicio al cliente de CCOA, Servicios, Programas y encadenamientos productivos, y Desarrolle sus habilidades para negociar. ⊕ Establecen controles nuevos en el proceso Registros Públicos, en las actividades de análisis y registros. El Profesional Jurídico realizó revisiones aleatorias de las devoluciones.

5. INFORMACIÓN RELACIONADA CON EL DESEMPEÑO Y LA EFICACIA DEL SISTEMA DE GESTION

		⊕ Establecieron controles nuevos en el proceso de Comunicaciones relacionados con revisiones periódicas de los datos de contacto de todas las sedes que se cargan en Google Maps. (Mínimo cada seis meses). ⊕ Realizaron ajustes en la página web para el trámite de certificados virtuales, con el fin de facilitar este trámite y de que el sitio web sea amigable.

5.1.2 Incluir la ocurrencia de incidentes (accidentes o emergencias) en los sistemas de gestión que aplique y explique brevemente cómo fueron tratados:
Número de Incidentes de seguridad de la información: 13 de bajo impacto en el año 2021. Se evidencia la generación de informes con análisis de causas, corrección y acción correctiva a partir de los incidentes presentados.

5.1.3 En los casos que aplique verificar que la Organización haya informado a ICONTEC durante los plazos especificados en el Reglamento R-PS-007 REGLAMENTO DE LA CERTIFICACIÓN ICONTEC DE SISTEMAS DE GESTIÓN eventos que hayan afectado el desempeño del Sistema de Gestión certificado, relacionados con el alcance de certificación que sean de conocimiento público. El auditor verificará las acciones pertinentes tomadas por la Organización para evitar su recurrencia y describirá brevemente como fueron atendidas.
No se presentan casos.

5.1.4 ¿Existen quejas de usuarios de la certificación recibidas por ICONTEC durante el último periodo evaluado? (Aplica a partir del primer seguimiento)
Si ☐ No ☑ N.A ☐

5.1.5 ¿Se evidencia la capacidad del Sistema de Gestión para cumplir los requisitos aplicables y lograr los resultados esperados?:
Si ☑ No ☐.

5.1.6 ¿Se concluye que el alcance del Sistema de gestión es apropiado frente a los requisitos que la Organización debe cumplir? (consultar E-PS-080 ALCANCE DE CERTIFICACIÓN DEL SISTEMA DE GESTION)
Si ☑ No ☐.

5.2 Relación de no conformidades detectadas en auditorías previas del ciclo de certificación

El ciclo de certificación inicia con una auditoría de otorgamiento o renovación, a partir de esta indicar contra cuáles requisitos se han reportado no conformidades.

ISO/IEC 27001:2013

Auditoría	Número de no conformidades		Requisitos
Otorgamiento/Renovación	27001	2	7.5.2.c), A.14.1.1
1ª de seguimiento del ciclo	27001	2	A.9.1.2, A.16.1.4

5. INFORMACIÓN RELACIONADA CON EL DESEMPEÑO Y LA EFICACIA DEL SISTEMA DE GESTION

2ª de seguimiento del ciclo			
Renovación			

¿Se evidencia recurrencia de no conformidades detectadas en las auditorías de ICONTEC en el último ciclo de certificación?
Si □ No X

ISO 9001:2015

Auditoría	Número de no conformidades		Requisitos
Otorgamiento/Renovación	9001	0	N.A.
1ª de seguimiento del ciclo	9001	1	8.4.1
2ª de seguimiento del ciclo	9001	0	N.A
Renovación			

¿Se evidencia recurrencia de no conformidades detectadas en las auditorías de ICONTEC en el último ciclo de certificación?
Si □ No X

5.3 Análisis del proceso de auditoría interna

El equipo auditor fue conformado auditores competentes según los requisitos establecidos por la organización. Se cuenta con procedimiento de auditoría donde se establecen todos los requisitos. La auditoría se orienta de acuerdo con directrices de ISO 19011 y se realizaron de manera independiente para cada sistema de gestión. El ciclo de auditorías se realizó desde el 25 de agosto hasta el 27 agosto de 2021. El alcance se considera apropiada a la naturaleza y necesidades de los sistemas de gestión, se encontró programa de auditoría, plan de auditoría, informe de auditoría y acciones correctivas.

5.4 Análisis de la revisión del Sistema por la dirección

Se realizó un análisis de los requisitos establecidos en el numeral 9.3 y de los resultados de los procesos y de los compromisos establecidos por la dirección. La revisión por la dirección se realizó el 07 de octubre de 2021. Se identificaron tópicos para el mejoramiento de los procesos y se precisaron buenas prácticas para apoyar y cimentar el crecimiento en los procesos.

6 USO DEL CERTIFICADO DE SISTEMA DE GESTION Y DE LA MARCA O LOGO DE LA CERTIFICACION

6.1 El logo o la marca de conformidad de certificación de Sistema de Gestión de ICONTEC se usa en publicidad (¿página web, brochure, papelería, facturas, etc?)
Si ☑ No ☐ N.A ☐

6.2 ¿La publicidad realizada por la Organización está de acuerdo a lo establecido en el reglamento R-PS-007 y el Manual de aplicación E-GM-001 USO DE LA MARCA DE CONFORMIDAD DE LA CERTIFICACIÓN ICONTEC PARA SISTEMAS DE GESTIÓN??
Si ☑ No ☐ N.A ☐

6 USO DEL CERTIFICADO DE SISTEMA DE GESTION Y DE LA MARCA O LOGO DE LA CERTIFICACION

6.3 ¿El logo o la marca de conformidad se usa sobre el producto o sobre el empaque o el envase o el embalaje del producto, o de cualquier otra forma que denote conformidad del producto?
Si ☐ No ☑ N.A ☐

6.4 Se evidencia la adecuación de la información contenida en el certificado (¿vigencia del certificado, logo de organismo de acreditación, razón social registrada en documentos de existencia y representación legal, direcciones de sitios permanentes cubiertos por la certificación, alcance, etc.?
Si ☑ No ☐ N.A

7. RESULTADO DE LA REVISION DE LAS CORRECCIONES Y ACCIONES CORRECTIVAS PARA LAS NO CONFORMIDADES MAYORES DETECTADAS EN ESTA AUDITORIA, MENORES QUE GENERARON COMPLEMENTARIA Y, MENORES DETECTADAS EN ESTA AUDITORIA QUE POR SOLICITUD DEL CLIENTE FUERON REVISADAS

✓ ¿Se presentaron No Conformidades Mayores?
Sí ☐ No ☑ N.A. ☐

✓ ¿Se presentaron No Conformidades menores de la auditoria anterior que no pudieron ser cerradas en esta auditoria?
Sí ☐ No ☐ N.A. ☑

✓ ¿Se presentaron no conformidades menores detectadas en esta auditoría que por solicitud del cliente fueron revisadas durante la complementaria?
Sí ☐ No ☐ N.A. ☑

Fecha de verificación de la complementaria: N.A.

NC	Descripción de la no conformidad (se relaciona el numeral de la norma y la evidencia del incumplimiento)	Evidencia obtenida que soporta la solución	¿Fue eficaz la acción? Si / No
No Conformidades mayores identificadas en esta auditoria			
	N.A.		
No Conformidades pendientes de la auditoria anterior que no se solucionaron			
No conformidades detectadas en esta auditoría que fueron cerradas			
	N.A.		

Si las acciones tomadas no fueron eficaces después de la realización de la verificación complementaria, se debe proceder de acuerdo con lo establecido en el Reglamento ES-R-SG-001.

8. RECOMENDACIÓN DEL EQUIPO AUDITOR DE ACUERDO CON EL ES-R-SG-001				
Se recomienda otorgar la Certificación del Sistema de Gestión				
Se recomienda mantener el alcance del certificado o del Sistema de Gestión				X
Se recomienda renovar el alcance del certificado o del Sistema de Gestión				
Se recomienda renovar anticipadamente el certificado Sistema de Gestión				
Se recomienda ampliar el alcance del certificado del Sistema de Gestión				
Se recomienda reducir el alcance del certificado				
Se recomienda reactivar el certificado				
Se recomienda actualizar el certificado del Sistema de Gestión (a la nueva versión de la norma)				
Se recomienda migrar el alcance del certificado o del Sistema de Gestión				
Se recomienda restaurar el certificado, una vez finalice el proceso de renovación				
Se recomienda suspender el certificado				
Se recomienda cancelar el certificado				
Nombre del auditor líder: Jairo Yobany Vargas Gordillo	Fecha	2021	10	29

9. ANEXOS QUE FORMAN PARTE DEL PRESENTE INFORME		
Anexo 1	Plan de auditoría F-PS-530 PLAN DE AUDITORIA EN SITIO – SISTEMAS DE GESTIÓN (Adjuntar el plan a este formato y el F-PS-654 FORMATO DE PROYECTOS EJECUTADOS Y EN EJECUCIÓN, cuando aplique)	X
Anexo 2	Información específica de esquemas de certificación de Sistema de Gestión	X
Anexo 3	Correcciones, análisis de causa y acciones correctivas Aceptación de la organización firmada. Información de la confirmación del cumplimiento de las condiciones para realizar auditoria con el apoyo de medios tecnológicos	X
Anexo 4	Información específica por condición de emergencia	X
Anexo 5	Declaración de aplicación (solo para ISO 28001)	N.A.

ANEXO 1

Plan de Auditoria

EMPRESA:	CÁMARA DE COMERCIO DEL ORIENTE ANTIOQUEÑO		
Dirección del sitio:	ISO 9001:2015 Cr. 47 # 64 A 263, Vía Belén Kilómetro 2 Rionegro, Antioquia, Colombia ISO IEC 27001:2013 Carrera 47 No. 64 A – 263 Vía Belén Kilómetro 2 Rionegro, Antioquia, Colombia Calle 20 No. 22-59 La Ceja, Antioquia, Colombia Carrera 31 No. 31–28 Guatapé, Antioquia, Colombia Calle 7 entre carreras 5 y 6, primer piso del palacio municipal Sonsón, Antioquia, Colombia.		
Representante de la organización:	Maryori Ocampo Ocampo		
Cargo:	Líder de Planeación Estratégica y Gestión Organizacional	Correo electrónico	pr.planeacion@ccoa.org.co
Alcance ISO 9001: Prestación de servicios de: Afiliación, Registro Público Información Comercial y Formación Empresarial. Alcance ISO/IEC 27001: Prestación de servicios para la gestión de los registros públicos. Declaración de aplicabilidad SI-DA-SE-01 Versión 4 de 2020-08-10.			
Criterios de Auditoría	ISO 9001:2015 + ISO/IEC 27001:2013 + la documentación del Sistema de Gestión		
Tipo de auditoría: □ Inicial u otorgamiento X Seguimiento □ Renovación □ Ampliación □ Reducción □ Reactivación □ Extraordinaria □ Actualización			
Modalidad: □ Auditoría en sitio □ Auditoria parcialmente remota X Auditoría totalmente remota			
Aplica toma de muestra por multisitio:	Si X No □ para ISO 27001:2013 Si □ No X para ISO 9001:2015		
Existen actividades/procesos que requieran ser auditadas en turno nocturno:	□ Si X No		
Con un cordial saludo, enviamos el plan de la auditoría que se realizará al Sistema de Gestión de su organización. Por favor indicar en la columna correspondiente, el nombre y cargo de las personas que atenderán cada entrevista y devolverlo al correo electrónico del auditor líder. Así mismo, para la reunión de apertura de la auditoría le agradezco invitar a las personas del grupo de la alta dirección y de las áreas/procesos/actividades que serán auditadas. Para la reunión de apertura le solicitamos disponer de un proyector para computador y sonido para video, si es necesario, (sólo para auditorías de certificación inicial y actualización). En cuanto a las condiciones de seguridad y salud ocupacional aplicables a su organización, por favor informarlas previamente al inicio de la auditoría y disponer el suministro de los equipos de protección personal necesarios para el equipo auditor.			

La información que se conozca por la ejecución de esta auditoría será tratada confidencialmente, por parte del equipo auditor de ICONTEC.

El idioma de la auditoría y su informe será el español.

Los objetivos de la auditoría son:

- Determinar la conformidad del sistema de gestión con los requisitos de la norma de sistema de gestión.
- Determinar la capacidad del sistema de gestión para asegurar que la organización cumple los requisitos legales, reglamentarios y contractuales aplicables al alcance del sistema de gestión y a la norma de requisitos de gestión.
- Determinar la eficacia del sistema de gestión para asegurar que la organización puede tener expectativas razonables con relación al cumplimiento de los objetivos especificados.
- Identificar áreas de mejora potencial del sistema de gestión.

Las condiciones de este servicio se encuentran indicadas en el R-PS-007 REGLAMENTO PARA LA CERTIFICACION DE SISTEMAS DE GESTIÓN.

Auditor Líder:	Yobany Vargas G.- YVG/LCP	Correo electrónico	jvargas@icontec.net
Auditor:	Libardo Chávez Pérez - LCP En su etapa de entrenamiento para ser auditor líder ISO/IEC 27001 e ISO 9001, desempeñó el rol de Auditor)	Auditor	N.A.
Experto técnico:	Claudia Patricia Serna Gallego - CPS- clausernagallego@gmail.com		
Esta auditoría se realizará totalmente remota utilizando medios tecnológicos - MT			

Fecha/ Sitio (si hay más de uno)	**Hora de inicio de la actividad de auditoría**	**Hora de finalización de la actividad de auditoría**	**PROCESO / REQUISITOS POR AUDITAR**	**EQUIPO AUDITOR**	**CARGO Y NOMBRE (Todas las personas que serán entrevistadas en la auditoría)**
Día 1 2021-10-12 Carrera 47 No. 64 A – 263 Vía Belén Kilómetro 2 Rionegro, Antioquia, Colombia	07:45	08:00	MT-Prueba de conectividad	YVG/LCP /CPS	
Día 1 2021-10-12	08:00	08:30	MT-Reunión de Apertura	YVG/LCP /CPS	Presidente Ejecutivo Director Administrativo y Financiero Director Jurídico Director de Operaciones Director de Competitividad y Desarrollo Empresarial Responsables de procesos
Día 1 2021-10-12	08:30	10:00	**MT- Gestión del conocimiento y la**	YVG/LCP /CPS	Maryori Ocampo, Analista 1 de Planeación y Procesos

			innovación organizacional - **Mejora Continua** Requisitos ISO/IEC 27001: 5.1, 6.1, 7.1, 7.4, 7.5, 9.1, 9.2, 10.1, 10.2 ISO 9001: 4.4.1, 5.1.1, 5.3, 6.1, 6.2, 7.1.2, 7.2, 7.3, 7.4, 7.5, 8.1, 8.2.1, 8.2.2, 9.1.1, 9.1.2, 9.1.3.		Jorge Andrés Sánchez Villa, Analista 2 de Seguridad de la Información María Luisa Ríos, Analista 2 de tecnología Yuriana Ríos, Asistente 1 de Planeación Estratégica y Gestión Organizacional
Día 1 2021-10-12	10:00	11:00	**MT- Gestión estratégica** - **Formulación estratégica** Requisitos ISO 27001: 4, 5, 6.2, 7.5, 9.1, 9.2, 9.3, 10, A.5, A.6, A.8 Requisitos ISO 9001: 4.1, 4.2, 5.1, 5.1.2, 6.1, 9.3.1, 9.3.2, 9.3.3, 10.3	YVG/LCP /CPS	Maryori Ocampo, Analista 1 de Planeación y Procesos Zoraida Ríos, Líder 1 de Relacionamiento Jorge Andrés Sánchez Villa, Analista 2 de Seguridad de la Información María Luisa Ríos, Analista 2 de tecnología Yuriana Ríos, Asistente 1 de Planeación Estratégica y Gestión Organizacional
Día 1 2021-10-12	11:00	12:00	**MT- Gestión estratégica** - Despliegue y seguimiento a la estrategia Requisitos ISO 27001: 4, 5, 6.2, 7.5, 9.1, 9.2, 9.3, 10, A.5, A.6, A.8	YVG/LCP /CPS	Maryori Ocampo, Analista 1 de Planeación y Procesos Zoraida Ríos, Líder 1 de Relacionamiento Jorge Andrés Sánchez Villa, Analista 2 de Seguridad de la Información María Luisa Ríos, Analista 2 de tecnología Yuriana Ríos, Asistente 1 de Planeación Estratégica y Gestión Organizacional
Día 1 2021-10-12	12:00	13:30	**MT- Receso**	YVG/LCP /CPS	
Día 1 2021-10-12	13:30	15:00	**MT- Fortalecimiento y Desarrollo Empresarial**	YVG/LCP /CPS	Alexandra Villada, Analista 1 de Servicios Empresariales

			- Servicios Empresariales Requisitos ISO 9001: ISO 9001: :5.1.1, 5.3, 6.1, 6.2, 6.3, 7.1, 7.1.4, 7.2, 7.3, 7.4, 7.5, 8.1, 8.2.1, 8.2.2, 8.2.3, 8.2.4, 8.5, 8.6, 8.7, 9.1		Zaida Pérez, Asistente 3 de Servicios Empresariales Wilmer López, Director de Competitividad y Desarrollo Empresarial. Carolina Noreña, Profesional Senior de Competitividad y Desarrollo Empresarial. Jorge Andrés Sánchez Villa, Analista 2 de Seguridad de la Información. Yuriana Ríos, Asistente 1 de Planeación Estratégica y Gestión Organizacional
Día 1 2021-10-12	15:00	16:30	**MT- Relacionamiento institucional** **- Gestión de comunicaciones** Requisitos ISO 27001: 7, A.9, A.11, A.12. ISO 9001: 5.1.1, 5.3, 6.1, 6.2, 6.3, 7.1, 7.1.4, 7.2, 7.3, 7.4, 7.5, 8.1, 8.2.1, 8.2.2, 8.2.3, 8.2.4, 8.5, 8.6, 8.7, 9.1	YVG/LCP /CPS	Zoraida Ríos, Líder 1 de Relacionamiento Paulina Restrepo, Analista 1 de Comunicaciones Jorge Andrés Sánchez Villa, Analista 2 de Seguridad de la Información María Luisa Ríos, Analista 2 de tecnología Yuriana Ríos, Asistente 1 de Planeación Estratégica y Gestión Organizacional
Día 1 2021-10-12	16:30	17:30	**MT- Balance diario**	YVG/LCP /CPS	
Día 2 2021-10-13 Carrera 31 No. 31–28 Guatapé, Antioquia, Colombia	08:00	09:30	**MT- Sede Guatapé** Gestión de los registros públicos Requisitos ISO 27001: 6.1.3, 7.3, A.8, A.9, A.11, A.12, A.13, A.16, A.17, A.18	YVG/LCP	Arelis Álzate, Líder 1 de Registros Diana Ramírez, Asistente 3 de Servicio al Cliente Jorge Andrés Sánchez Villa, Analista 2 de Seguridad de la Información María Luisa Ríos, Analista 2 de tecnología Yuriana Ríos, Asistente 1 de Planeación Estratégica y Gestión Organizacional
Día 2 2021-10-13	09:30	11:00	**MT- Sede La Ceja**		Arelis Álzate, Líder 1 de Registros

Calle 20 No. 22-59 La Ceja, Antioquia, Colombia			Gestión de los registros públicos Requisitos ISO 27001: 6.1.3, 7.3, A.8, A.9, A.11, A.12, A.13, A.16, A.17, A.18		Asistente 3 de Servicio al Cliente Jorge Andrés Sánchez Villa, Analista 2 de Seguridad de la Información María Luisa Ríos, Analista 2 de tecnología Yuriana Ríos, Asistente 1 de Planeación Estratégica y Gestión Organizacional
Día 2 2021-10-13	11:00	12:00	**MT- Registros públicos** **- Gestión de los registros públicos** Requisitos ISO 27001: 7, A.9, A.11, A.12. ISO 9001: :5.1.1, 5.3, 6.1, 6.2, 6.3, 7.1, 7.1.4, 7.2, 7.3, 7.4, 7.5, 8.1, 8.2.1, 8.2.2, 8.2.3, 8.2.4, 8.5, 8.6, 8.7, 9.1	YVG/LCP	Arelis Álzate, Líder 1 de Registro Jorge Andrés Sánchez Villa, Analista 2 de Seguridad de la Información. María Luisa Ríos, Analista 2 de tecnología Yuriana Ríos, Asistente 1 de Planeación Estratégica y Gestión Organizacional.
Día 2 2021-10-13	12:00	13:30	**MT- Receso**	YVG/LCP	
Día 2 2021-10-13	13:30	16:30	**MT- Seguridad de la Información** Gestión de seguridad de la información Requisitos ISO 27001: A.5, A.6,	YVG/LCP	María Luisa Ríos, Analista 2 de tecnología Jorge Andrés Sánchez Villa, Analista 2 de Seguridad de la Información Yuriana Ríos, Asistente 1 de Planeación Estratégica y Gestión Organizacional
Día 2 2021-10-13	16:30	17:30	**MT- Balance diario**	YVG/LCP	
Día 3 2021-10-14	08:00	10:00	**MT- Seguridad de la Información** Gestión de seguridad de la información Requisitos ISO 27001: A.5, A.6,	YVG/LCP	María Luisa Ríos, Analista 2 de tecnología Jorge Andrés Sánchez Villa, Analista 2 de Seguridad de la Información María Luisa Ríos, Analista 2 de tecnología

					Yuriana Ríos, Asistente 1 de Planeación Estratégica y Gestión Organizacional
Día 3 2021-10-14	10:00	12:30	**MT- Gestión de las TICS** - Gestión de la infraestructura tecnológica y sistemas de información Requisitos ISO 27001: 8, A.9, A.10, A.11, A.12, A.13, A.14, A.15, A.16, A.6.1.5, 8.3, A.9, 10	YVG/LCP	María Luisa Ríos, Analista 2 de tecnología Jorge Andrés Sánchez Villa, Analista 2 de Seguridad de la Información María Luisa Ríos, Analista 2 de tecnología Yuriana Ríos, Asistente 1 de Planeación Estratégica y Gestión Organizacional
Día 3 2021-10-14	12:30	14:00	Receso	YVG/LCP	
Día 3 2021-10-14	14:00	16:30	**MT- Gestión de las TICS** - Gestión de servicios de tecnología de información Requisitos ISO 27001: 8, A.9, A.10, A.11, A.12, A.13, A.14, A.15, A.16, A.6.1.5, 8.3, A.9, 10	YVG/LCP	María Luisa Ríos, Analista 2 de tecnología Jorge Andrés Sánchez Villa, Analista 2 de Seguridad de la Información María Luisa Ríos, Analista 2 de tecnología Yuriana Ríos, Asistente 1 de Planeación Estratégica y Gestión Organizacional
Día 3 2021-10-14	16:30	17:30	Balance diario	YVG/LCP	
Día 4 2021-10-15	08:00	09:30	**MT- Gestión Administrativa** - Gestión de Infraestructura Física Requisitos ISO 27001: A.15 ISO 9001: 6.1,6.2, 6.2.1,6.3, 7.1.4, 7.5, 7.5.1,7.5.2, 7.5.3, 8.2.2, 8.2.3, 8.2.4, 8.4, 8.4.1, 8.4.2,8.4.3, 8.5.6, 9.1,9.1.1., 9.1.3, 10	YVG/LCP	Dra. Soraida Tobón, Directora Administrativa y Financiera Leidy Suaza, Asistente 1 Administrativa Jorge Andrés Sánchez Villa, Analista 2 de Seguridad de la Información María Luisa Ríos, Analista 2 de tecnología Yuriana Ríos, Asistente 1 de Planeación Estratégica y Gestión Organizacional
Día 4 2021-10-15	09:30	11:00	**MT- Gestión Administrativa** - Gestión Contractual	YVG/LCP	Dra. Soraida Tobón, Directora Administrativa y Financiera

			Requisitos ISO 27001: 7, A.9, A.11, A.12. ISO 9001:5.1.1, 5.3, 6.1, 6.2, 6.3, 7.1, 7.1.4, 7.2, 7.3, 7.4, 7.5, 8.1, 8.2.1, 8.2.2, 8.2.3, 8.2.4, 8.5, 8.6, 8.7, 9.1		Lina Oquendo, Directora Jurídica Leidy Suaza, Asistente 1 Administrativa Jorge Andrés Sánchez Villa, Analista 2 de Seguridad de la Información María Luisa Ríos, Analista 2 de tecnología Yuriana Ríos, Asistente 1 de Planeación Estratégica y Gestión Organizacional
Día 4 2021-10-15	11:00	12:30	**MT- Preparación informe de auditoría**	YVG/LCP	
Día 4 2021-10-15	12:30	14:00	**MT- Receso**	YVG/LCP	
Día 4 2021-10-15	15:00	16:30	**MT- Preparación informe de auditoría**	YVG/LCP	
Día 4 2021-10-15	16:30	17:30	**MT- Reunión de cierre**	YVG/LCP	Presidente Ejecutivo Director Administrativo y Financiero Director Jurídico Director de Operaciones Director de Competitividad y Desarrollo Empresarial Responsables de procesos

Observaciones:

Requisitos comunes que serán auditados en todos los procesos.

6.1 Acciones para tratar riesgos y oportunidades
7.4 Comunicación
7.5 Información documentada
9.1 Seguimiento, medición, análisis y evaluación
A.9.3 Responsabilidades de los usuarios

Los requisitos comunes que serán auditados en todos los procesos para ISO 9001 son:

6.1 Acciones para abordar riesgos y oportunidades
6.3 Planificación de cambios
7.1.6 Conocimientos de la organización
7.4 Comunicación
7.5 Información documentada
9.1 Seguimiento, medición, análisis y evaluación
10 Mejora

Se sugiere que la auditoría este acompañada por una persona de la organización o guía, con el fin de:

- Establecer contactos y asistir con la ejecución del cronograma de entrevistas.
- Orientar al equipo auditor frente a las reglas relacionadas a la protección personal y de seguridad establecidas por la organización.

- Testificar la auditoria en nombre de la organización y proveer información aclaratoria cuando así sea solicitado por el equipo auditor.
- Identificar y transmitir la información generada a la organización.
- Para cada actividad de auditoría por favor abrir sesiones y salas en Meet, por favor tener en cuenta la dirección de correo electrónico del auditor líder.

Esta auditoría no es objeto de testificación por un Organismo de Acreditación.

Fecha de emisión del plan de auditoría:	2021 09 25

ANEXO 2

Información Específica de Esquemas de Certificación Sistemas de Gestión

INFORMACIÓN ESPECÍFICA DE ESQUEMAS DE CERTIFICACIÓN DE SISTEMA DE GESTIÓN

Sistema de gestión de seguridad de la información ISO/IEC 27001
Sistema de gestión de privacidad de la información ISO/IEC 27701

Marque con una X si el sistema de gestión auditado.

ISO/IEC 27001 X ISO/IEC 27001 + ISO/IEC 27701 □

Objetivos de la auditoría

Evaluar las implicaciones de los cambios en el SGSI/SGPI, iniciadas como consecuencia de cambios en la operación del cliente y cubrir al menos:
a) El sistema de mantenimiento de elementos tales como la evaluación y control de riesgos de seguridad de la información y privacidad, mantenimiento, auditorías internas del SGSI/SGPI, revisión por la dirección y las acciones correctivas;
b) Las comunicaciones de las partes externas como es requerido por la norma ISO/IEC 27001 e ISO/IEC 27701;
c) Los cambios en la documentación del SGSI/SGPI;
d) Las zonas sujetas a cambio;
e) los requisitos de la norma ISO/IEC 27001 e ISO/IEC 27701 cuando sea aplicable.

Actividades desarrolladas

- La metodología de la auditoría fue verificación de registros físicos y electrónicos, interacción, observación.

- ¿Se modificó la declaración de aplicabilidad?
  Si □ No X
  Si aplica, mencionar el cambio y la versión (Asegúrese de colocar la declaración de aplicabilidad vigente en el alcance de la certificación) en la siguiente tabla:

VERSIÓN VIGENTE:	JUSTIFICACIÓN DEL CAMBIO
Declaración de aplicabilidad BNT- DAP-SGSI-01 Versión 2 (2019-09-02).	No aplica

- ¿Los procedimientos adoptados por el cliente brindan confianza en el SGSI/ SGPI?
  Si X No □
  Si la respuesta es NO, se debe justificar porque no brindan confianza o eliminar si no aplica.

- Describa brevemente los documentos revisados como evidencia de las muestras tomadas para la evaluación del SGSI/ SGPI (Ver PE-PS-079 PROCEDIMIENTO ESPECIFICO PARA CERTIFICACION ISO/IEC 27001 y el PE-PS-133 PROCEDIMIENTO ESPECIFICO PARA LA GESTION DE LA PRIVACIDAD DE LA INFORMACION ISO/IEC 27701).

Se revisaron los documentos concernientes a: Políticas de seguridad de la información, Registro de incidentes o eventos de seguridad, Registro de revisiones de perfiles a colaboradores, Registro de vulnerabilidades, Revisión de cuentas desactivadas de usuarios retirados, Revisión física de equipos de cómputo, Roles de seguridad de la información, Manual de gestión de seguridad de la información, Capacitación de seguridad de la información, Declaración de aplicabilidad, Formato identificación de perfiles a colaboradores, Gestión de vulnerabilidades, Identificación y análisis de riesgos, Identificación, clasificación y valoración de activos de información, Incidentes de seguridad, Inventario de activos de información, Manual identificación, clasificación y valoración de activos de información, Manual plan de continuidad del negocio, Prueba de plan de continuidad del negocio, Informe de auditoría interna, Informe ethical hacking, Políticas de seguridad de la información, Registro de incidentes o eventos de seguridad, Registro de revisiones de perfiles a colaboradores, Registro de vulnerabilidades, Revisión de cuentas desactivadas de usuarios retirados, Revisión física de equipos de cómputo y Roles de seguridad de la información.

Análisis de la eficacia del sistema de gestión certificado

- Describa brevemente el análisis de riesgos, de la revisión de los planes de tratamiento y del riesgo residual (Ver PE-PS-079 y PE-PS-133).

    - En el periodo 2020 - 2021 se registraron 125 riesgos y planes de tratamiento del riesgo. calificados de la siguiente manera: Críticos 3, Altos 15, Medios 22, Bajo 85
    - Los dueños del riesgo identifican los riesgos y registran la aprobación de los riesgos inherentes y el riesgo residual de manera estandarizada.
    - La metodología de análisis de riesgos se destaca por su alcance, cobertura y por la constante participación de todos los líderes de los procesos. Los dueños del riesgo identifican los riesgos y registran la aprobación de los riesgos inherentes y el riesgo residual de manera estandarizada.
    - En el riesgo residual, la gestión del plan de tratamiento se realiza a través de planes de acciones claramente definidos, responsables y recursos asociados.

ANEXO 3 - CORRECCIONES, CAUSAS Y ACCIONES CORRECTIVAS

- Se recibió la propuesta de correcciones, análisis de causas y acciones correctivas para la solución de no conformidades el 2021-10-28 y recibieron observaciones por parte del auditor líder.

- Las correcciones, análisis de causas y acciones correctivas propuestas por la organización, fueron aceptadas por el auditor líder el 2021-10-29.

SOLICITUD DE ACCIÓN CORRECTIVA		**No.** 1 de 2
☐ No - Conformidad Mayor ☒ No - Conformidad Menor	Norma(s): ISO/IEC 27001:2013	Requisito(s): A.9.1.2 Acceso a redes y a servicios en red

Descripción de la no conformidad:

No se evidenció restricción de acceso a los servicios de red (Acceso a correos personales en internet y páginas de almacenamiento de archivos en la nube), en los equipos de las sedes de Guatapé y La Ceja y Líder 1 de Registro.

Evidencia:

Al inspeccionar los privilegios de acceso a los servicios de red, desde los computadores asignados a:

- Diana Patricia Ramírez - Auxiliar de Servicio al Cliente en la sede Guatapé y Yasmin Osorio - Asesor de Servicio al Cliente en la sede La Ceja, se encontró libre acceso a: correo personal (Gmail.com).
- Arelis Álzate Líder 1 de Registro, se encontró libre acceso a: sitios web de almacenamiento de archivos en la nube (Mega.com).

Contraviniendo la Declaración de Aplicabilidad, SI-DA-SE-01 Versión 4 en el control A.9.1.2

Corrección	**Evidencia de Implementación**	**Fecha**
1. Restricción de acceso a páginas de almacenamiento de archivos en la nube (mega.com, Winzip, Winrar)	Restricción de acceso a sitios de almacenamiento (Pruebas e imágenes)	19/10/2021
2. Actualizar la política de control de acceso sobre el acceso y uso de correo personal	Política de control de acceso actualizada en el documento SI-MM-SE-01 Manual de Seguridad de la Información.	05/10/2021

Descripción de la (s) causas (s)

(Por favor use este espacio para realizar el análisis de causa. Por ejemplo: porqués, espina de pescado, etc…).

Causas

¿Por qué?	**Motivo**

No se evidenció restricción de acceso a los servicios de red (Acceso a correos personales en internet y páginas de almacenamiento de archivos en la nube), en los equipos de las sedes de Guatapé y La Ceja y Líder 1 de Registro.	Al inspeccionar los privilegios de acceso a los servicios de red, desde los computadores asignados a: Diana Patricia Ramírez - Auxiliar de Servicio al Cliente en la sede Guatapé y Yasmin Osorio - Asesor de Servicio al Cliente en la sede La Ceja, se encontró libre acceso a: correo personal (Gmail.com). Arelis Álzate Líder 1 de Registro, se encontró libre acceso a: sitios web de almacenamiento de archivos en la nube (Mega.com).
Al inspeccionar los privilegios de acceso a los servicios de red, desde los computadores asignados a: Diana Patricia Ramírez - Auxiliar de Servicio al Cliente en la sede Guatapé y Yasmin Osorio - Asesor de Servicio al Cliente en la sede La Ceja, se encontró libre acceso a: correo personal (Gmail.com). Arelis Álzate Líder 1 de Registro, se encontró libre acceso a: sitios web de almacenamiento de archivos en la nube (Mega.com).	No se tenía bloqueado el acceso a correo personal (Asesores de servicio al cliente) y a sitios de almacenamiento en la nube (Líder 1 de Registro)
No se tenía bloqueado el acceso a correo personal y a sitios de almacenamiento en la nube (Líder de Registro)	La organización determinó en vigencias anteriores no realizar el bloqueo de acceso al correo personal. Adicionalmente, si bien se cuenta con un documento de referencia sobre el acceso y los perfiles que se asignan a los colaboradores, la documentación no es clara en cuanto a los perfiles y privilegios de acuerdo al nivel del cargo del colaborador.
La organización determinó en vigencias anteriores no realizar el bloqueo de acceso al correo personal. Adicionalmente, si bien se cuenta con un documento de referencia sobre el acceso y los perfiles que se asignan a los colaboradores, la documentación no es clara en cuanto a los perfiles y privilegios de acuerdo al nivel del cargo del colaborador.	Aunque la organización determinó no realizar el bloqueo del correo personal para los colaboradores, no se dejó evidencia de esta decisión. En cuanto al documento de acceso y perfiles del proceso de infraestructura tecnológica y servicios de información no referencia el acceso y los permisos de acuerdo a los diferentes niveles de cargo en la organización.

Causa Raíz:	1. No se tiene claridad sobre la política de control de acceso en lo que refiere al acceso al correo personal. 2. En el documento de referencia de accesos y perfiles no se documenta claramente los perfiles y privilegios de acuerdo a los niveles de cargo de la organización

Acción correctiva	Evidencia de Implementación	Fecha
1. Analizar la pertinencia de realizar el bloqueo del correo personal de los colaboradores y actualizar la política de control de acceso, según la decisión tomada.	Socialización en el comité de gestión del análisis realizado frente a la política de control de	15/01/2022

	accesos definida por la organización.	
2. Definir los criterios de acceso a los sistemas y aplicaciones en el manual de políticas de seguridad de la información y el documento de referencia de accesos y perfiles, donde se establezcan los accesos de acuerdo al cargo del colaborador.	SI-MM-SE-01 Manual de Seguridad de la Información actualizado de acuerdo a los criterios de acceso a los sistemas y aplicaciones	30/01/2022
3. Revisar los controles de acceso de los colaboradores y realizar las correcciones de acuerdo a los hallazgos.	Informe de revisión de controles y acciones implementadas	30/01/2022
4. Realizar sensibilización a los colaboradores sobre el uso del correo electrónico.	Registro de asistencia a evento de sensibilización	15/02/2022
5. Medir la eficacia de las acciones abordadas para el tratamiento de la no conformidad	Registro de eficacia en ISOTools.	15/02/2022

SOLICITUD DE ACCIÓN CORRECTIVA		**No.** 2 de 2
☐ No - Conformidad Mayor		Requisito(s):
☒ No - Conformidad Menor	Norma(s): ISO/IEC 27001:2013	A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos.

Descripción de la no conformidad:

No se evidencia la clasificación de incidentes de seguridad de la información, según lo definido en el SI-PO-SE-02 Patrón Operacional Sistema de Gestión de Seguridad de la Información.

Evidencia:
El incidente de seguridad No. 27990, el cual generó una indisponibilidad del datacenter, por espacio de 25 minutos, el día 19 de abril de 2021 y fue clasificado como incidente de tecnología de la información.

Corrección	**Evidencia de Implementación**	**Fecha**
1. Reclasificar el incidente de seguridad No. 27990, el cual generó una indisponibilidad del datacenter, por espacio de 25 minutos, el día 19 de abril de 2021 y fue clasificado como incidente de tecnología de la información.	Ticket No. 27990 reclasificado en la plataforma de gestión tecnológica.	25/10/2021

Descripción de la (s) causas (s)
(Por favor use este espacio para realizar el análisis de causa. Por ejemplo: porqués, espina de pescado, etc…).

Causas

¿Por qué?	**Motivo**

No se evidencia la clasificación de incidentes de seguridad de la información, según lo definido en el SI-PO-SE-02 Patrón Operacional Sistema de Gestión de Seguridad de la Información.	El incidente de seguridad No. 27990, el cual generó una indisponibilidad del datacenter, por espacio de 25 minutos, el día 19 de abril de 2021 y fue clasificado como incidente de tecnología de la información.
El incidente de seguridad No. 27990, el cual generó una indisponibilidad del datacenter, por espacio de 25 minutos, el día 19 de abril de 2021 y fue clasificado como incidente de tecnología de la información	El incidente se clasifica como incidente de tecnología de la información a partir del reporte inicial del usuario, sin embargo una vez gestionado este no se re clasifica como incidente de seguridad de la información, por desconocimiento del asistente de tecnología.
No se re clasifica como incidente de seguridad de la información	Si bien desde el proceso de gestión de servicios de información (TI) y gestión de seguridad de la información se realiza la gestión de este incidente en conjunto, y el incidente se tiene en cuenta en el indicador de incidentes de seguridad de la información del proceso, al momento de realizar el cierre de este, no se reclasifica en la herramienta de gestión de tickets.
Al momento de realizar el cierre del ticket no se reclasifica en la herramienta de gestión de tickets.	No se cuenta con un paso de análisis y reclasificación de tickets en el patrón operacional de GT-PO-GS-03 Gestión de eventos e incidentes.

Causa Raíz:	1. Desde el proceso de gestión de servicios de tecnología de la información (TI) no se tiene claridad sobre la clasificación, la gestión y el cierre de incidentes de seguridad.

Acción correctiva	Evidencia de Implementación	Fecha
1.Actualización del patrón operacional de GT-PO-GS-03 Gestión de eventos e incidentes y niveles de servicio, y en el documento GT-PR-GS-01 Niveles de Servicio en lo que se considere pertinente sobre la identificación, gestión y cierre de incidentes de seguridad de la información.	Patrón operacional de GT-PO-GS-03 Gestión de eventos e incidentes y niveles de servicio, y en el documento GT-PR-GS-01 Niveles de Servicio, actualizados de acuerdo a identificación, gestión y cierre de incidentes de seguridad de la información.	30/11/2021
2. Socialización con el equipo de TI los documentos actualizados.	Registro de asistencia de socialización de documentos actualizados.	30/01/2022
3. Reinducción a los asistentes de tecnología sobre la clasificación y la asignación de tickets a través de la plataforma de servicios de tecnología.	Registro de asistencia a reinducción “Clasificación de Tickets”	30/01/2022

5. Medir la eficacia de las acciones abordadas para el tratamiento de la no conformidad	Registro de eficacia en ISOTools	15/03/2022

RESULTADOS DE AUDITORÍA:

Número de no conformidades ISO/IEC 27001 detectadas en esta auditoría: (0) mayores (2) menores
Número de no conformidades ISO 9001 detectadas en esta auditoría: (0) mayores (0) menores

Número de no conformidades pendientes que no se cerraron en esta auditoría: ( ) menores (X) N.A.

Plazo para la entrega de propuesta de corrección y acción correctiva (de acuerdo con lo establecido en el ES-R-SG-01) hasta: 2021-10-29

Fecha tentativa de verificación complementaria, cuando aplique: N.A.

ACEPTACIÓN DE LA ORGANIZACIÓN:

Declaro que los servicios previstos fueron integralmente ejecutados y soy consciente de los resultados obtenidos.

La organización acepta la (s) no conformidad (es) reportada (s) en el presente informe y se compromete a presentar los planes de acción en los tiempos establecidos en el reglamento de certificación ES-R-SG-001.

En caso de no aceptarse alguna no conformidad relacione él número de la no conformidad _N.A._ y el requisito al que fue reportada _N.A._. En este caso la organización deberá solicitar una reposición dirigida al Gerente de Certificación.

Nombre del Representante de la Organización: Maryori Ocampo Ocampo	Firma: 

ANEXO 4 - INFORMACIÓN ESPECÍFICA POR CONDICIÓN DE EMERGENCIA

Tipo de emergencia: COVID-19

VERIFICACIÓN DE RIESGOS Y REQUISITOS MÍNIMOS PARA EL DESARROLLO DE LA AUDITORIA CON EL APOYO DE MEDIOS TECNOLOGICOS		SI	NO
1	¿Se cuenta con los requisitos mínimos de conexión y herramienta tecnológica para el desarrollo de la auditoría con el apoyo de medios tecnológicos?	X	
2	¿La calidad de la comunicación con el apoyo de medios tecnológicos permite una comunicación eficaz y continua?	X	
3	¿El uso de medios tecnológicos permite el mantenimiento de la confidencialidad y seguridad de la información? Nota: confirmar con la empresa si está de acuerdo en compartir información a través de la herramienta tecnológica.	X	
4	¿Se cuenta con los requisitos mínimos de información (acceso a la información de los procesos en medio digital o electrónico o escaneado en el momento que el auditor lo solicite durante el ejercicio en vivo)?	X	
5	¿Las actividades Core del negocio incluidas en el alcance de la certificación, pueden ser verificadas por medio remoto?	X	
6	¿La organización está en funcionamiento, es decir que las actividades CORE del negocio, a incluir en el alcance de la certificación se están desarrollando conforme los requisitos establecidos en la norma de referencia del sistema de gestión a auditar? Nota. En el caso que la respuesta sea NO, informar al Coordinador de programación y al Ejecutivo de Cuenta, que se debe reprogramar la auditoría etapa II.	X	
7	¿La auditoría con el apoyo de medios tecnológicos a las actividades Core del negocio incluidas en el alcance de la certificación puede afectar la calidad o seguridad del producto o servicio? Nota: confirmar con la empresa si se puede hacer uso de herramientas tecnológicos durante la auditoría a las actividades de prestación del servicio, ej: usar cámaras en un banco o durante la atención en salud, etc.		X
8	¿Si las actividades del Core del negocio son prestadas fuera de las instalaciones de la organización, ¿estas pueden ser verificadas por medios remotos?	X	
9	¿El personal de la organización cuenta con la disposición y competencia para el atender la auditoría con el apoyo de medios tecnológicos? Nota: se espera que la empresa confirme que las personas que van a recibir la auditoría están capacitadas en el uso de la herramienta.	X	
10	¿Se detectaron otros riesgos de alto impacto que no permiten el desarrollo de la auditoría? Por favor relacione los otros riesgos identificados: Ninguno En caso de auditorías de seguimiento o renovación revise también el desempeño del sistema de gestión (no conformidades de auditorías externas e internas, comunicaciones de partes interesadas, incidentes, accidentes, emergencias, eventos adversos, entre otros). Nota: en caso de que su respuesta sea SI comuníquese con la UT para establecer el proceso a seguir).		X
11	De encontrar situaciones que generen riesgos en relación con las preguntas 1 a 10, ¿consideran que éstos pueden ser mitigados o eliminados para la realización de la auditoría etapa 2 con la utilización de herramientas tecnológicas? Explique su respuesta, incluyendo los métodos que se utilizarán para mitigar los riesgos Nota. Recuerde que se generan riesgos si la respuesta a las preguntas 1 a 5, 6, 8 y 9 es NO, y las correspondientes a las preguntas 7 y 10 es SI.	X	

12	En los casos en que se haya autorizado por parte de la UT realizar cambio de modalidad de parcialmente remoto a totalmente remoto con la participación de un profesional de apoyo, ¿se comunicó a la organización el rol del profesional de apoyo? Si ☐ No ☐ N.A ☑ ¿Se cuenta con el consentimiento de la organización, incluyendo el compromiso con el suministro de los medios tecnológicos requeridos para asegurar la conectividad? Si ☑ No ☐ N.A ☐		
13	De acuerdo con el análisis de riesgos realizado y teniendo en cuenta los objetivos de la auditoria se concluye que se puede realizar la auditoría (Marcar con una X en frente de la metodología seleccionada):		
	Totalmente remota	X	
	Parcialmente remota		
	Totalmente en sitio		

CONFIRMACIÓN DEL CUMPLIMIENTO DE LAS CONDICIONES PARA REALIZAR AUDITORIA CON EL APOYO DE MEDIOS TECNOLÓGICOS		
1	Medio(s) tecnológico(s) empleado(s):	☑ TEAMS ☐ OTRA Cuál? _____
2	¿Cuáles actividades de la auditoria o procesos del SG fueron realizados en forma remota?	La totalidad de los procesos incluidos en el plan de auditoría.
3	¿El tamaño del muestreo fue suficiente y la organización estaba preparada para suministrar las evidencias solicitadas por este medio?	☑ SI ☐ NO
4	¿Cuáles herramientas fueron empleadas para la verificación de los procesos de realización o prestación del servicio de manera remota?	☑ Teams Cámaras de video de alta resolución, para ver controles de acceso físico y zonas seguras, entrevistas, verificación de información digitalizada, uso de herramienta MS TEAMS para compartir información y realizar video conferencia
5	¿El tiempo fue suficiente para abarcar todo lo planificado?	☑ SI ☐ NO
6	¿La conexión por medio de la herramienta tecnológica permitió dar inicio y desarrollar la auditoria de acuerdo con los tiempos previstos en el plan de auditoria?	☑ SI ☐ NO