1. INFORMACIÓN GENERAL

1.1. ORGANIZACIÓN

Cámara de Comercio del Oriente Antioqueño.

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

1.3. LOCALIZACIÓN DEL SITIO PERMANENTE PRINCIPAL: (Aplica para los dos certificados)
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.

Estos sitios adicionales aplican únicamente para el certificado 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	
Calle 7 entre carreras 5 y 6, primer piso del palacio municipal.	Sonsón, Antioquia - Colombia	

1.4. ALCANCE DE LA CERTIFICACION:

ISO 9001:2015

Prestación de servicios de: Afiliación, registro público, información comercial y formación empresarial
Se declara no aplicable el requisito 8.3 Diseño y desarrollo

Services provision of: affiliation, public records, commercial information, and business formation

ISO IEC 27001:2013

Prestación de servicios para la gestión de los registros públicos.
Declaración de aplicabilidad Versión 2.0 de 2017-10-09.

Provision of services for the management of the public registrations.
Statement Applicability Version 2.0 dated 2017-10-09.

1.5. CÓDIGO IAF: 39-2 si 1

1.6. CATEGORIA DE ISO/TS 22003: NA

1.7. REQUISITOS DE SISTEMA DE GESTION: ISO 9001:2015 ISO IEC 27001:2013

1.8. REPRESENTANTE DE LA ORGANIZACIÓN

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

1. INFORMACIÓN GENERAL

1.9. TIPO DE AUDITORIA:

☐ **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 ☐

Auditoría combinada: Si X No ☐ ISO 9001:2015 ISO IEC 27001:2013

Auditoría integrada: Si ☐ No X

1.10. Tiempo de auditoria	FECHA	Días de auditoría)
Etapa 1 (Si aplica)	NA	NA
Preparación de la auditoría en sitio y elaboración del plan	2018-11-03	1
Auditoría en sitio	2018-11-14,15, 16	3

1.11. EQUIPO AUDITOR

Auditor líder	John Jairo Gutiérrez
Auditor	Rodrigo de la Cruz Mejía
Experto Técnico	NA

1.12. DATOS DEL CERTIFICADO DE SISTEMA DE GESTIÓN

	ISO 9001:2015	**ISO IEC 27001:2013**
Código asignado por ICONTEC	SC 5057-1	SI-CER577303
Fecha de aprobación inicial	2007-12-12	2017 12 22
Fecha de próximo vencimiento:	2019-12-11	2020 12 21

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 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 ☐ NAX

3.8. Si se aplicó toma de muestra de múltiples sitios, indicar cuáles sitios permanentes se auditaron y en que fechas:

- El día 14 de Noviembre se visitó la sede ubicada en la Calle 20 No. 22-59 La Ceja, Antioquia
- El día 16 de Noviembre se visitó la sede Ubicada en la Carrera 31 No. 31–28 Guatapé, Antioquia

3.9. ¿En el caso del Sistema de Gestión auditado están justificados los requisitos no aplicables acordes con lo requerido por el respectivo referencial?
Si X No ☐ NA ☐

3. ACTIVIDADES DESARROLLADAS

NORMA	Requisito	Descripción del requisito	Justificación
ISO 9001:2015	8.3	Diseño y desarrollo	Los servicios de la Cámara de Comercio, están reglamentados por la ley, por lo tanto no es posible que se diseñen o desarrollen nuevos productos o servicios en el marco establecido por la misma.
	7.1.5.2	Trazabilidad de las mediciones	por la naturaleza administrativa, los servicios que proporciona la Cámara de Comercio, no requiere de la utilización de equipos de medición para evaluar la conformidad de los servicios.
ISO IEC 27001: 2013	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.12.1.4	Ambiente de desarrollo	LA cámara de comercio no tiene desarrollos internos y en casos de ser necesario se subcontrata la actividad
	A.14.2.2	Control de cambios	
	A.14.2.6	Ambiente de desarrollo seguro	
	A.14.2.8	Pruebas de seguridad en sistemas	

3.10. ¿Se auditaron actividades en sitios temporales o fuera del sitio de acuerdo al listado de contratos o proyectos entregado por la Organización?: Si ☐ No ☐ NA X

3.11. ¿Es una auditoría de ampliación o reducción? Si ☐ No ☐ NA X

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 ☐ NA X

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

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

3. ACTIVIDADES DESARROLLADAS

3.15. ¿Se auditaron actividades en turnos nocturnos? Si ☐ No ☐ NA X

3.16. ¿Se encontraron controlados los procesos de origen externo (out sourcing), cuyo resultado incide en la conformidad del producto y/o servicio que afectan la satisfacción del cliente?
Si X No ☐ NA ☐.

Proceso de origen externo:
Alianzas con universidades y otras para dictar capacitaciones en el proceso de servicios empresariales
AMAZON (Pruebas de contingencia)

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

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

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 ☐ NA X

3.20. ¿Aplica restauración para este servicio? Si ☐ No ☐ NA X

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.

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	A.11.2.1No se evidencia que el cuarto de la planta eléctrica que abastecen la sede principal de la Cámara de Comercio del Oriente Antioqueño, se encuentra protegidas para reducir los riesgos de amenazas y peligros del entorno. En el cuarto de la planta eléctrica se encontraron cajas de cartón, bolsas con cables, repuestos eléctricos y un taller de mantenimiento lo cual representa riesgo de incendio.	Se implementó la acción correctiva implementada para solucionar la no conformidad detectada Se arregló el sitio y los residuos se disponen en sitio apropiado para tal fin.	Si fue eficaz
2	A.15.2.1No se evidencia que la organización audita con regularidad la prestación de servicios de los proveedores. No se encontraron los registros de auditoría de los proveedores: Confecámaras, ASP Solutions S.A, Iron Montain Colombia S.A.S.	Se implementó la acción correctiva implementada para solucionar la no conformidad detectada Se hizo análisis de criticidad de proveedores y se hicieron las visitas respectivas	Si fue eficaz

3. ACTIVIDADES DESARROLLADAS			
3	A.16.1.6No se evidencia el aprendizaje adquirido al analizar y resolver incidentes de seguridad de la información: 2404, 2309 y 2077. Evidencia: Revisión de la gestión de incidentes en el periodo 2016 -2017.	Se implementó la acción correctiva implementada para solucionar la no conformidad detectada En los incidentes se definieron las lecciones aprendidas	Si fue eficaz
4	A.17.1.3No se evidencia que la Organización realizó pruebas de la totalidad de planes de continuidad de negocio y verificación de la eficacia de la implementación de los planes de continuidad de negocio con el fin de asegurar que son válidos durante una crisis o desastre. Al revisar las pruebas de los planes de continuidad de negocio realizadas en las oficinas administrativas de Cámara de Comercio del Oriente Antioqueño, en el periodo 2016 – 2017, se encontraron sin verificación de su eficacia. Así mismo las pruebas de los planes de continuidad de negocio y retorno a la normalidad, correspondientes al ambiente productivo del aplicativo WordManager (Herramienta utilizada para la gestión de documentos digitalizados en la prestación del servicio de Registros Públicos) en un entorno diferente a en las oficinas administrativas, no se encontraron finalizadas en su totalidad.	Se implementó la acción correctiva implementada para solucionar la no conformidad detectada Se hizo prueba de 22 de octubre pero	Si fue eficaz

4. HALLAZGOS DE LA AUDITORÍA

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

- Trabajo en equipo para la realización de los proyectos ya que fortalece el análisis y favorece la toma de decisiones.

- Compromiso directivas y de los líderes de proceso con el sistema de gestión de calidad, puesto que fortalece el mejoramiento continuo en todos los procesos.

- La intención de la gerencia para aplicar la responsabilidad social empresarial, la cual es expresada en las directrices fundamentales y divulgada a toda la organización porque se brinda satisfacción de las necesidades y expectativas de sus miembros, de la sociedad y de quienes se benefician de su actividad comercial, así como también, al cuidado y preservación del entorno.

4. HALLAZGOS DE LA AUDITORÍA

- Trabajos adelantados en la aplicaión de un modelo de excelencia y de innovación en gestión

- Metodologías implementadas para diagnosticar la responsabilidad social empresarial.

4.2 Oportunidades de mejora

- Fortalecer el análisis del contexto organizacional relacionándolo con el análisis DOFA con el fin que facilite la alineación de la identificación de proyectos para desarrollar las oportunidades.

- Dentro de la planeación estratégica de la empresa involucrar componentes de tecnología para fortalecer la posición del gobierno corporativo y consolidar el posicionamiento organizacional (Consultar a manera de orientación ISO 38500:2015 Corporate Governance of Information Technology)

- Establecer una integración de los sistemas de gestión de calidad y seguridad con el fin de optimizar los recursos del sistema, en este orden de ideas es conveniente Fortalecer requisitos comunes a las normas con el fin de facilitar las operaciones y unificar los alcances y sitios certificados

- Mejorar los indicadores de proceso considerando la eficacia, la eficiencia y el impacto que tienen dentro del Sistema de Gestión frente a las diferentes perspectivas de la organización con el fin mantener una relación que brinde un panorama amplio al momento de controlar todos los aspectos de la empresa (consultar a manera de orientación las metodologías de tablero balanceado de control o Balanced Scorecard)

- Fortalecer la medición de indicadores de seguridad de la información y establecer métricas que monitoreen permanentemente el desempeño de los grupos de controles, de los planes de acción, de la evolución del riesgo residual, de la clasificación de incidentes etc., con el ánimo de facilitar la toma de decisiones frente al análisis de datos (Consultar a manera de guía la ISO 27004 Métricas de un sistema de gestión de la seguridad de la información)

4. HALLAZGOS DE LA AUDITORÍA

- Fortalecer el proceso de innovación y desarrollo por medio de las herramientas de evaluación de proyectos y de requisitos de investigación, desarrollo e innovación, consultar a manera de información NTC 5801 ô UNE 166000

- Establecer procesos de Gestión del conocimiento que consolide lecciones aprendidas, preguntas frecuentes, capacitaciones recurrentes etc. con el fin de facilitar el aprendizaje y la recuperación de experiencias aplicadas. Consultar a manera de orientación la norma UNE 412001:2008 guía práctica de gestión del Conocimiento

- Fortalecer los planes de tratamiento del análisis de riesgo por medio del establecimiento de actividades detalladas en la ejecución y así facilitar el seguimiento y la medición de la eficacia de los mismos.

- Fortalecimiento del ciclo PHVA (Planear, hacer, verificar, actuar) en los diversos procesos de modo que facilite la eficacia en el flujo de actividades, la integración de requisitos de otras normas y consolide el enfoque sistémico en especial en las caracterización de servicios empresariales para fortalecer la identificación de actividades enfocadas en diversos servicios.

- Fortalecer la reevaluación de los proveedores con el fin de asegurar una actualización de información

- Mejorar la medición de la eficacia de la formación de modo que esta sea a mediano plazo y que permita recolectar datos tanto de las evaluaciones puntuales por capacitación como de los desempeños generales.

- Fortalecer el plan de continuidad del negocio, realizando pruebas que contemplen escenarios cada vez mas críticos y que involucren a las personas, activos críticos de tecnología e infraestructura, con el fin de contar con un plan que responda a todos los procesos y necesidad de la organización en caso de presentarse eventos adversos o catastróficos. Como ayuda es posible consultar la norma ISO 22313 buenas prácticas en la gestión de la continuidad del negocio.

4. HALLAZGOS DE LA AUDITORÍA

- Fortalecer el plan de continuidad del negocio, realizando pruebas que contemplen escenarios cada vez más críticos y que involucren a las personas, activos críticos de tecnología e infraestructura, con el fin de contar con un plan que responda a todos los procesos y necesidad de la organización en caso de presentarse eventos adversos o catastróficos. Como ayuda es posible consultar la norma ISO 22313 buenas prácticas en la gestión de la continuidad del negocio e ISO 22317:2015 Guías para definir l análisis de impacto del negocio

- De continuar midiendo criterios de “cumplimiento”, comprometer niveles de desempeño deseado del 100.0%, evitando así, el tolerar posibles incumplimientos. Considerar su complementariedad con indicadores de eficacia.

- Eliminar la determinación de frecuencias anuales para la realización de análisis de resultado de los indicadores con el fin de evitar la identificación de incumplimientos al final de los períodos fiscales, que conlleven a la determinación de decisiones reactivas.

- Profundizar en los análisis de causas de los eventos de mayor repetividad asociados a las quejas, reclamos, sugerencias y felicitaciones, que se conviertan en fuente para la toma de decisiones y acciones pertinentes, eliminando dichas causas para asegurar la mejora continua y el aprendizaje organizacional.

- Consolidar las evaluaciones de satisfacción en la atención de las QRSF y llevarlo como un nuevo indicador de eficacia que permita identificar elementos de retroalimentación para el proceso, luego de analizados los resultados.

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. Incluir las reclamaciones o quejas validas del cliente en los sistemas de gestión que aplique durante el último año.

- Procedimiento de incidentes de seguridadSI-PO-SE-01 versión 2 octubre 30
- Se tiene un procedimiento documentado para el registro, establecimiento del tratamiento, seguimiento y evaluación de satisfacción de las quejas – Reclamos – Sugerencias – Felicitaciones, se encuentra en versión 04. Se controla a través del radicado que asigna el aplicativo, la numeración consecutiva. Se atienden los eventos en un 100.0%.

Acciones de mejora: Los comentarios de los usuarios son analizados por el analista de mercadeo, lo que ha motivado la creación de la campaña “Contamos contigo”, en fase de implementación.

Tipo de comentario		
Felicitaciones	55%	Incremento con relación a 2017
Quejas	-29%	
Reclamos	67%	
Sugerencias	-22%	

Principales quejas o reclamaciones recurrentes	Principal causa	Acciones tomadas
2017: Con corte a octubre 30		
38 Quejas	14 por servicio al cliente 7 por servicio de asesoría 4 por programas de visitas 4 Por infraestructura tecnológica 9 Por otros asuntos	Capacitación en el tema de liderazgo Desde el área de Registros Públicos se realizan reuniones de análisis semanal. Se contratan nuevos servidores Se organizan unos instructivos virtuales para los usuarios.
3 Reclamos	Asesoría Fortalecimiento y desarrollo empresarial Beneficios del Registro Público Mercantil	Desde el área de Registros Públicos se realizan reuniones de análisis semanal. Ampliar los temas de capacitación para afiliados. Se capacita a los afiliados

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

23 Sugerencias	9 Por servicio al cliente 3 Por Tramites de registro 2 Por programas de visitas 2 por Fortalecimiento y Desarrollo Empresarial 2 Por infraestructura física.	Se atienden desde las estrategias determinadas para atender las quejas. Además se, amplían los plazos para los trámites específicos.
29 Felicitaciones	16 Por servicio al cliente 6 Por asesorías 2 Por Formación Empresarial 2 Por programas de visitas 2 Por presencia institucional.	
2018: Con corte a octubre 30		
27Quejas	11 Por servicio al cliente 5 Por tiempos de atención 4 Por asesoría 7 Por otros asuntos	Se profundiza a través del ingreso de la analista de mercadeo, en la definición de estrategias más puntuales con relación a los usuarios
Eventos 9	Incumplimientos leves de políticas	
Incidentes 12		

5.1.2. En los casos que aplique verificar que la Organización haya informado a ICONTEC durante los plazos especificados en el Reglamento ES-R-SG-001 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.

5.1.3. ¿Existen quejas de usuarios de la certificación recibidas por ICONTEC durante el último periodo evaluado? (Aplica a partir del primer seguimiento)? Si ☐ NoX NA ☐

5.1.4. Se evidencia la capacidad del sistema de gestión para cumplir los requisitos aplicables y lograr los resultados esperados?: Si X No ☐

5.1.5. ¿Se concluye que el alcance del sistema de gestión es apropiado frente a los requisitos que la Organización debe cumplir? (consultar ES-P-SG-02-A-001) Si X No ☐.

5.2. Relación de no conformidades detectadas durante el 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.

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

Auditoria	Número de no conformidades	Requisitos
Otorgamiento / Renovación	ISO 9001: 0 Año 2016	NA
	ISO IEC 27001: 4 Año 2017	A.11.2.1., A.15.2.1., A.16.1.6., A.17.1.3.
1ª de seguimiento del ciclo	ISO 9001:0 Año 2017	NA
	ISO IEC 27001: 8 Año 2018	A.9.1.2, A.11.1.2, A.12.1.3, A.12.3.1, A.12.4.4, A.12.6.1, A.17.2.1,A.18.1.2
2ª de seguimiento del ciclo	ISO 9001: 2 Año 2018	8.4, 6.2
	ISO IEC 27001: Año 2019	NA
Auditorias especiales (Extraordinaria, reactivación, ampliación)		

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

5.3 Análisis del proceso de auditoría interna

Se cuenta con el documento Patrón operacional auditorías internas GC-PO-MC-02 V 5 - 2018-11-09, alineado con ISO 19011

Las auditorias de Seguridad de la información y calidad se hicieron los días 21, 22 y 23 de mayo de 2018 se identifica 1 nc para seguridad de la información y 4 para calidad en todos los casos hay acciones correctivas

La auditorias las realizaron auditores externos calificados

5.4 Análisis de la revisión del sistema por la dirección

La revisión por la dirección se hizo en 24 Octubre y se analizan las entradas y salidas solicitadas por las dos normas.

El documento está enfocado en el mejoramiento continuo

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 X No ☐ NA ☐.

6.2. ¿La publicidad realizada por la Organización está de acuerdo con lo establecido en el reglamento ES-R-SG-001 y el Manual de aplicación ES-P-GM-01-A-011? Si X No ☐ NA ☐.

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 X NA ☐

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 X No ☐.

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? SI ☐ NO X

¿Se presentaron no conformidades menores de la auditoria anterior que no pudieron ser cerradas en esta auditoría? SI ☐ NO X

¿Se presentaron no conformidades menores detectadas en esta auditoría que por solicitud del cliente fueron revisadas durante la complementaria? SI ☐ NO X

8. RECOMENDACIÓN DEL EQUIPO AUDITOR DE ACUERDO CON EL ES-R-SG-001

	SI	NO
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 certificado del 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		
Se recomienda migrar el certificado 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: John Jairo Gutiérrez	Fecha	2018	12	03

9. ANEXOS QUE FORMAN PARTE DEL PRESENTE INFORME

Anexo 1	Plan de auditoría ES-P-SG-02-F-002 (Adjuntar el plan a este formato)	X
Anexo 2	Información específica de esquemas de certificación de sistema de gestión (En caso de que no aplique indicar en el cuadro N/A)	X
Anexo 3	Correcciones, análisis de causa y acciones correctivas Aceptación de la organización firmada.	X

ANEXO 1

PLAN DE AUDITORIA

EMPRESA:	CÁMARA DE COMERCIO DEL ORIENTE ANTIOQUEÑO		
Dirección del sitio :	Carrera 47 No. 64 A - 263 Vía Belén Rionegro 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 27001: Prestación de servicios para la gestión de los registros públicos. Declaración de aplicabilidad Versión 2.0 de 2017-10-09.			
CRITERIOS DE AUDITORÍA	ISO 9001:2015 + ISO IEC 27001:2013+NTC 5906 + la documentación del Sistema de Gestión		
Tipo de auditoría : ☐ INICIAL U OTORGAMIENTO **X SEGUIMIENTO** ☐ RENOVACION ☐ AMPLIACIÓN ☐ REDUCCIÓN ☐ REACTIVACIÓN ☐ EXTRAORDINARIA ☐ ACTUALIZACIÓN			
Aplica toma de muestra por multisitio:	☐ Si X No		
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 Reglamento de certificación de sistemas de gestión R-SG-001.

Auditor Líder:	John Jairo Gutiérrez Ordóñez (JJG) 3176609657	Correo electrónico	jgutierrez@icontec.net
Auditor:	Rodrigo de la Cruz Mejía Gómez (RCM)	Auditor	rmejia@icontec.net
Experto técnico:			

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)
2018-11-14	08:00	08:20	Reunión de apertura	JJG - RCM	Líderes de proceso

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)
	08:20	09:00	Validación de Requisitos no aplicables y justificación de la no aplicabilidad Determinación de requisitos legales aplicables (A.18 ISO 27001 Y 7.5 ISO 9001)	JJG - RCM	Profesional de Planeación y Procesos Maryori Ocampo Ocampo Profesional de Seguridad de la Información Ferney López Dávila
	09:00	11:00	Entendimiento del Contexto organizacional y de las partes interesadas Revisión planeación estratégica Control operacional Análisis de la política del sistema de gestión Análisis de objetivos de calidad y seguridad Revisión por la dirección Requisitos ISO 9001, ISO 27001: 4.1, 4.2, 4, 5, 6.2, 9.3	JJG	Profesional de Planeación y Procesos Maryori Ocampo Ocampo Profesional de Seguridad de la Información Ferney López Dávila
	11:00	12:30	Gestión de riesgos Requisitos ISO 9001: 6.1 Requisitos ISO 27001: 6.1, 8.1, 8.2, 8.3	JJG	Profesional de Planeación y Procesos Maryori Ocampo Ocampo Profesional de Seguridad de la Información Ferney López Dávila Asistente de Gestión y Control del Riesgo Catalina Duque Aparicio
	11:00	12:30	Gestión de quejas y reclamos Requisitos ISO 9001: 8.2	JJG	Profesional de Planeación y Procesos Maryori Ocampo Ocampo Analista de Mercadeo y Servicio al Cliente Juliana Orozco Builes Auxiliar de PEyGO Yuriana Ríos
	12:30	13:30	Receso para el almuerzo	JJG	

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)
	13:30	15:30	Mejoramiento Auditorías internas Acciones correctivas Seguimiento DE las no conformidades año 2017 Requisitos ISO 9001, ISO 27001: 9.2, 10	JJG	Profesional de Planeación y Procesos Maryori Ocampo Ocampo Auxiliar de PEyGO Yuriana Ríos
	15:30	17:00	Servicios empresariales Requisitos ISO 9001: 8.1, 8.2, 8.5.1, 8.5.2, 8.5.3, 8.5.4, 8.5.6, 8.7	JJG	Dir. de Competitividad y Desarrollo Empresarial Analista de Mercadeo y Servicio al Cliente Juliana Orozco Builes Profesional de Planeación y Procesos Maryori Ocampo Ocampo
	17:00		Reunión de auditores	JJG	
2018-11-15	08:00		Balance Día 1	JJG	Profesional de Planeación y Procesos Maryori Ocampo Ocampo Profesional de Seguridad de la Información Ferney López Dávila
	08:15	13:00	Tecnología Configuración técnica de la organización Configuración de sistemas, topologías medios tecnológicos utilizados, tipos de redes segmentos de redes y controles de los diferentes sitios remotos Continuidad DE negocio A.17 Análisis de vulnerabilidad A.12.6.1 Incidentes de seguridad A.16 Mantenimiento de servidores A.11.2.4 Gestión de cambios A.12.1.2 Gestión de capacidad A.12.1.3	JJG	Profesional de Seguridad de la Información Ferney López Dávila Profesional de Planeación y Procesos Maryori Ocampo Ocampo Analista de Tecnología María Luisa Ríos Holguín Asistente de Tecnología Jorge Andrés Sánchez

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)
			Controles códigos maliciosos A.12.2.1 Respaldo de la información A.12.3.1 Registro de eventos A.12.4.1 Sincronización de relojes A.12.4.4. Control de software operacional A.12.5.1, A.12.6.2 Mensajería electrónica A.1.2.3 Mantenimiento de Infraestructura física y tecnológica Visita DATACENTER Requisitos ISO 9001: 7.1.3 Requisitos ISO 27001: A.11.2.1, A.11.2.2, A.11.2.3, A.11.2.4		
	12:00	14:00	**Traslado sede La Ceja** Receso para el almuerzo	JJG	
	14:00	18:00	Gestión de los registros públicos Requisitos ISO 9001: 8.1, 8.2, 8.5.1, 8.5.2, 8.5.3, 8.5.4, 8.5.6, 8.7 Requisitos ISO 27001: 6.1.3, 7.3, A.8.3.1, A.9.2.4, A.9.2.6, A.9.4.2 A.11.1, A.11.2, A.12.1.1, A.12.2.1, A.12.4.4, A.12.5.1, A.12.6.2, A.13.1, A.13.2, A.16.1.3, A.17.1.3 A.18.1.2, A.18.1.4	JJG	Profesional de Seguridad de la Información Ferney López Dávila Jefe de Registros Arelis Álzate Profesional de Planeación y Procesos Maryori Ocampo Ocampo
	14:00	16:30	Gestión Contractual Requisitos ISO 9001: 8.1, 8.2, 8.5.1, 8.5.2, 8.5.3, 8.5.4, 8.5.6, 8.7	JJG	Profesional de Registro y Centro de Conciliación Jimmy Alexis García Tamayo Auxiliar de Dirección Jurídica Mabely Sánchez Profesional de Planeación y Procesos Maryori Ocampo Ocampo
	17:00		Cierre de NTC 5601		
2018-11-16	08:00	08:20	Balance de la auditoria 2 día	JJG	Profesional de Planeación y Procesos

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)
					Maryori Ocampo Ocampo Profesional de Seguridad de la Información Ferney López Dávila
	07:00	09:30	Visita a la sede de Gua tapé Gestión de los registros públicos Requisitos ISO 9001: 8.1, 8.2, 8.5.1, 8.5.2, 8.5.3, 8.5.4, 8.5.6, 8.7 Requisitos ISO 27001: 6.1.3, 7.3, A.8.3.1, A.9.2.4, A.9.2.6, A.9.4.2 A.11.1, A.11.2, A.12.1.1, A.12.2.1, A.12.4.4, A.12.5.1, A.12.6.2, A.13.1, A.13.2, A.16.1.3, A.17.1.3 A.18.1.2, A.18.1.4	JJG	Profesional de Planeación y Procesos Maryori Ocampo Ocampo Profesional de Seguridad de la Información Ferney López Dávila
			Retorno a Rionegro		
	10:30	12:30	Gestión de las Compras y acuerdos con terceros Requisitos ISO 9001: 8.4 Requisitos ISO 27001 A.15:	JJG	Directora Administrativa y Financiera Soraida Tobón Sossa.
	12:00	13:00	Receso para el almuerzo	JJG	
	13:00	14:30	Revisión de la información por parte del auditor	JJG	
	14:30		Reunión de cierre	JJG	Líderes de Proceso

Observaciones:
Se solicita tener disponible tener una memoria para hacer comprobación de políticas de removibles. En cualquier equipo se puede revisar los controles de Navegación en internet.
En cualquier proceso actividad se podrán corroborar temas transversales de concientización de políticas y control de documentos
Para el balance diario de información del equipo auditor le agradecemos disponer de una oficina o sala, así como también de acceso a la documentación del sistema de gestión.
Esta auditoría no es testificada por un Organismo de Acreditación.

Fecha de emisión del plan de auditoría:	2018-10-28

ANEXO 2

INFORMACION ESPECIFICA DE ESQUEMAS DE CERTIFICACIÓN DE SISTEMA DE GESTION

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

Objetivos de la auditoría

Evaluar las implicaciones de los cambios en el SGSI, 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 información mantenimiento, auditorías internas del SGSI, revisión por la dirección y las acciones correctivas;
b) Las comunicaciones de las partes externas como es requerido por el Sistema de Seguridad de la Información la norma ISO / IEC 27001;
c) Los cambios en la documentación del Sistema de Gestión;
d) Las zonas sujetas a cambio;
e) los requisitos de la norma ISO/IEC 27001.

Actividades desarrolladas

- La metodología de la auditoria fue verificación de registros físicos y electrónicos, interacción, observación.
- ¿Se modificó la declaración de aplicabilidad?
  Si ☐ No X

  No se reportan cambios o actualizaciones

VERSIÓN VIGENTE:	JUSTIFICACIÓN DEL CAMBIO
Prestación de servicios para la gestión de los registros públicos. Declaración de aplicabilidad Versión 2.0 de 2017-10-09.	No hay cambios ni actualizaciones .

- Los procedimientos adoptados por el cliente brindan confianza en el SGSI? Si X No ☐
- Describa brevemente los documentos revisados como evidencia de las muestras tomadas para la evaluación del SGSI (Ver ES-P-SG-02-A-007).

  Se revisaron procedimientos concernientes a Políticas de seguridad, Políticas para el talento humano, Perfiles de cargo, contratos, controles de acceso y dispositivos móviles, acceso físico y seguridad física, mantenimiento de equipos, backup, antivirus, control de navegación, correo electrónico, gestión de cambios, gestión de capacidad, ventanas de mantenimiento y procedimientos de funcionamiento de la infraestructura, Políticas de desarrollo seguro, incidentes, declaración de aplicabilidad, la matriz de riesgos y los controles aplicables y su implementación, procedimientos de auditoria interna, control de documentos, registros, acciones correctivas y los documentos contenidos en las caracterización de procesos. Se revisó además el plan de continuidad de negocio y los simulacros realizados

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 ES-P-SG-02-A-007)
  Se cuenta con metodología de riesgos basada en ISO 31000 contenida en el Manual de riesgos de Nov de 2018 Se identificaron 3 riesgos valorados en inherente extremo y en residual quedaría solo 1

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 2018-11-30 y se aprobaron el mismo día.

SOLICITUD DE ACCIÓN CORRECTIVA		**No.** 1 de 10
[ ] No - Conformidad Mayor [X] No - Conformidad Menor	Norma(s): ISO 9001:2015 ISO IEC 27001:2013	Requisito(s): 6.2

Descripción de la no conformidad:

No se hace un tratamiento adecuado de los riesgos

Evidencia:

NO se puede verificar la eficacia de los planes de tratamiento de los riesgos de calidad en el proceso estratégico.
Los riesgos de seguridad no están alineados con los controles de seguridad de la información.

Corrección	**Evidencia de Implementación**	**Fecha**
En la matriz de riesgos, establecer la relación directa del riesgo vs los numerales de los controles implementados.	Matriz de riesgos actualizada	18-12-2018

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

¿POR QUÉ?	**MOTIVO**
Los riesgos de seguridad no están alineados con los controles de seguridad de la información.	Cuando se implementa el SGSI los riesgos de seguridad fueron registrados en la matriz de riesgos de la organización y los controles de seguridad se registraron en la declaración de aplicabilidad de acuerdo con el literal D del numeral *6.1.3 Tratamiento de riesgos*
Cuando se implementa el SGSI los riesgos de seguridad fueron registrados en la matriz de riesgos de la organización y los controles de seguridad se registraron en la declaración de aplicabilidad de acuerdo con el literal D del numeral 6.1.3 Tratamiento de riesgos	La norma ISO 27001: 2013 en su numeral *6.1.3 Tratamiento de riesgos*, no contempla que se deba establecer la relación directa del riesgo vs los numerales de los controles en un mismo documento.

La norma ISO 27001: 2013 en su numeral 6.1.3 Tratamiento de riesgos, no contempla que se deba establecer la relación directa del riesgo vs los numerales de los controles en un mismo documento.	Al adoptarse la metodología del sistema de gestión de riesgos de la organización (ISO 31000), para el tratamiento de riesgos de seguridad de la información, riesgos y controles se establecieron en cada documento y no en la matriz de riesgos.
CAUSA RAÍZ	**Al adoptarse la metodología del sistema de gestión de riesgos de la organización (ISO 31000), para el tratamiento de riesgos de seguridad de la información, riesgos y controles se establecieron en cada documento y no en la matriz de riesgos.**

¿POR QUÉ?	**MOTIVO**
No se puede verificar la eficacia de los planes de tratamiento de los riesgos de calidad en el proceso estratégico.	La eficacia a los planes de tratamiento se verifica desde el proceso de Control Interno, quedando evidenciado en el software ISOTools, donde se encuentra toda la trazabilidad de los riesgos.
La eficacia a los planes de tratamiento se verifica desde el proceso de Control Interno, quedando evidenciado en el software ISOTools, donde se encuentra toda la trazabilidad de los riesgos.	La verificación de la efectividad de los planes de tratamiento se valida a través de la evaluación de los controles establecidos en el riesgo de manera general, lo cual se identifica como una de las causas raíz de la NC.
CAUSA RAÍZ	**La verificación de la efectividad de los planes de tratamiento se valida a través de la evaluación de los controles establecidos en el riesgo de manera general, lo cual se identifica como una de las causas raíz de la NC.**

Acción correctiva	**Evidencia de Implementación**	**Fecha**
En la actualización de matriz de riesgos para la vigencia 2019, relacionar de manera explícita los controles que aplican para cada riesgo tratado.	Matriz de riesgos actualizada.	30-05-19
Revisar y ajustar la metodología de riesgos	Documento metodológico ajustado	30-06-19
Realizar la medición de la efectividad de los controles implementados para la movilización del riesgo alineado con la metodología adoptada por la organización.	Matriz de riesgos actualizada.	30-09-19
Implementar en la metodología de gestión de riesgos la medición de la eficacia de cada uno de los controles.	Patrón operacional	30-6-19
Verificar la eficacia de las acciones implementadas.	Medición de la eficacia en la herramienta ISOTools	30-10-19

Diligenciar tantos cuadros como sea necesario para cada no conformidad.

Nota: Es importante que la organización realice un buen análisis de causa para evitar que la no conformidad se repita y el plan de acción sea devuelto por el equipo auditor, por lo cual les sugerimos consultar la guía para la solución de no conformidades, disponible en la página web de Icontec.

Ruta: www.icontec.org – Documentos servicios ICONTEC ó a través del link: http://www.icontec.org/Paginas/Documentos-servicios-icontec.aspx

SOLICITUD DE ACCIÓN CORRECTIVA	No. 2 de 10

[ ] No - Conformidad Mayor [X] No - Conformidad Menor	Norma(s): ISO 9001:2015	Requisito(s): 8.4

Descripción de la no conformidad:

No se encuentra la evaluación y selección de proveedores nuevos ni se ha hecho reevaluación de proveedores.

Evidencia:

No se enceuntra la evaluación de proveedores nuevos de tecnología Tamdem (mantenimiento de scaner) Andean trade (DRP)

NO hay Reevaluación de proveedores

Corrección	Evidencia de Implementación	Fecha
Realizar la evaluación inicial de selección de los proveedores mencionados: Tamdem (mantenimiento de scaner) y Andean trade (DRP)	Evaluaciones documentadas	14-12-18

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

¿POR QUÉ?	MOTIVO
No se enceuntra la evaluación de proveedores nuevos de tecnología Tamdem (mantenimiento de scaner) Andean trade (CRM) NO hay Reevaluación de proveedores	Se tiene establecido un procedimiento formal para la selección y evaluación de nuevos proveedores a partir de 35 SMMLV. No se ha establecido de manera formal un procedimiento para seleccionar y evaluar proveedores de bienes y servicios por montos inferiores a este. En el patrón operacional de Gestión de proveedores, no se tiene diferenciado los criterios de evaluación y reevaluación de proveedores.

CAUSA RAÍZ	**Se tiene establecido un procedimiento formal para la selección y evaluación de nuevos proveedores a partir de 35 SMMLV. No se ha establecido de manera formal un procedimiento para seleccionar y evaluar proveedores de bienes y servicios por montos inferiores a este.** **En el patrón operacional de Gestión de proveedores, no se tiene diferenciado los criterios de evaluación y reevaluación de proveedores.**

Acción correctiva	**Evidencia de Implementación**	**Fecha**
Ajustar el Patrón de Gestión de proveedores con criterios claros para identificar proveedores críticos y no críticos. Como también conceptos de selección, evaluación y reevaluación	Patrón operacional ajustado	30-5-19
Diseñar e implementar formato para la selección y evaluación de nuevos proveedores.	Formato publicado y socializado	30-5-19
Implementar reevaluación de proveedores	Informe de reevaluación	30-8-19
Verificar la eficacia de las acciones implementadas	Medición de la eficacia en la herramienta ISOTools	30-10-19

Diligenciar tantos cuadros como sea necesario para cada no conformidad.

Nota: Es importante que la organización realice un buen análisis de causa para evitar que la no conformidad se repita y el plan de acción sea devuelto por el equipo auditor, por lo cual les sugerimos consultar la guía para la solución de no conformidades, disponible en la página web de Icontec.

Ruta: www.icontec.org – Documentos servicios ICONTEC ó a través del link: http://www.icontec.org/Paginas/Documentos-servicios-icontec.aspx

SOLICITUD DE ACCIÓN CORRECTIVA	No. 3 de 10

[ ] No - Conformidad Mayor [X] No - Conformidad Menor	Norma(s): ISO IEC 27001:2013	Requisito(s): A.9.1.2

Descripción de la no conformidad:

Se encuentra que es posible acceder a redes diferentes a las autorizadas.

Evidencia:

En Guatapé y La ceja se enceuntra que desde los diferentes equipos de Atención integral, es posible acceder a una red wifi de invitados los tienen controles de navegación diferentes a los permitidos facilitando e ingreso a páginas y a descargas no autorizadas

Corrección	Evidencia de Implementación	Fecha
Deshabilitar controlador WIFI de todos los equipos de escritorio de la organización	Imágenes, pruebas de configuración.	10-12-2018

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

¿POR QUÉ?	MOTIVO
En Guatapé y La ceja se encuentra que desde los diferentes equipos de Atención integral, es posible acceder a una red wifi de invitados la cual tiene controles de navegación diferentes a los permitidos facilitando el ingreso a páginas y a descargas no autorizadas	Este tipo de conexiones se autoriza como una alternativa para no afectar la prestación del servicio cuando se presentan fallas técnicas en el servicio de internet.
Este tipo de conexiones se autoriza como una alternativa para no afectar la prestación del servicio cuando se presentan fallas técnicas en el servicio de internet.	**No se han establecido políticas de seguridad que impidan que los equipos del dominio CCOA se conecten a redes no controladas.**
CAUSA RAÍZ	**No se han establecido políticas de seguridad que impidan que los equipos del dominio CCOA se conecten a redes no controladas.**

Acción correctiva	Evidencia de Implementación	Fecha
Configurar adaptadores de red de los equipos de trabajo para restringir la navegación sólo a través de la red CCOA.	Pruebas de navegación.	30-01-19
Habilitar acceso VPN y capacitar a todos los usuarios que usan portátil por fuera de las instalaciones CCOA, en el manejo de este tipo de conexión.	Pruebas de conexión con los usuarios.	30-01-19
En el plan de revisión a estaciones de trabajo que se realiza cada trimestre desde el SGSI, incluir la verificación del cumplimiento de este control.	Registros de verificación trimestral.	30-06-19

Diligenciar tantos cuadros como sea necesario para cada no conformidad.

Nota: Es importante que la organización realice un buen análisis de causa para evitar que la no conformidad se repita y el plan de acción sea devuelto por el equipo auditor, por lo cual les sugerimos consultar la guía para la solución de no conformidades, disponible en la página web de Icontec.

Ruta: www.icontec.org – Documentos servicios ICONTEC ó a través del link: http://www.icontec.org/Paginas/Documentos-servicios-icontec.aspx

SOLICITUD DE ACCIÓN CORRECTIVA	No. 4 de 10

[ ] No - Conformidad Mayor [X] No - Conformidad Menor	Norma(s): ISO IEC 27001:2013	Requisito(s): A.11.1.2

Descripción de la no conformidad:

NO hay apropiados controles físicos de entrada

Evidencia:
El rack de la regional Guatapé no está protegido para evitarla entrada de personal no autorizado, ya que este se encuentra cerca la lavadero de utensilios de aseo.

Corrección	Evidencia de Implementación	Fecha
Ubicar el rack en un espacio que cumpla con los requisitos de seguridad y control de acceso.	Imágenes del rack ubicado adecuadamente	15-12-18

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

¿POR QUÉ?	MOTIVO
El rack de la regional Guatapé no está protegido para evitarla entrada de personal no autorizado, ya que este se encuentra cerca el lavadero de utensilios de aseo.	No se hizo el debido análisis de requerimientos y riesgos para la ubicación de este activo.
No se hizo el debido análisis de requerimientos y riesgos para la ubicación de este activo.	El área de Tecnología contrató la instalación de este elemento, sin embargo, desconocía el procedimiento adecuado a seguir.
El área de Tecnología contrató la instalación de este elemento, sin embargo, desconocía el procedimiento adecuado a seguir.	**No existe un procedimiento documentado que establezca el las acciones que permitan identificar los riesgos y requerimientos para la instalación, movimiento o adecuación de elementos en la infraestructura física.**
CAUSA RAÍZ	**No existe un procedimiento documentado que establezca el las acciones que permitan identificar los riesgos y requerimientos para la instalación,**

	movimiento o adecuación de elementos en la infraestructura física.

Acción correctiva	**Evidencia de Implementación**	**Fecha**
Elaboración e implementación de procedimiento que permita identificar los riesgos y requerimientos para la instalación, movimiento o adecuación de elementos en la infraestructura física.	Procedimiento publicado y socializado con todos los colaboradores	20-2-19
Revisión de la ubicación de los elementos de infraestructura tecnológica en todas las sedes de la organización.	Formato de revisión de sedes	30-1-19
Verificación de la efectividad del procedimiento implementado en nuevos cambios de infraestructura física.	Registro de verificación	30-6-19

Diligenciar tantos cuadros como sea necesario para cada no conformidad.

Nota: Es importante que la organización realice un buen análisis de causa para evitar que la no conformidad se repita y el plan de acción sea devuelto por el equipo auditor, por lo cual les sugerimos consultar la guía para la solución de no conformidades, disponible en la página web de Icontec.

Ruta: www.icontec.org – Documentos servicios ICONTEC ó a través del link: http://www.icontec.org/Paginas/Documentos-servicios-icontec.aspx

SOLICITUD DE ACCIÓN CORRECTIVA	No. 5 de 10

[ ] No - Conformidad Mayor [X] No - Conformidad Menor	Norma(s): ISO IEC 27001:2013	Requisito(s): a.12.1.3

Descripción de la no conformidad:

No se tiene informes de gestión de capacidad futura

Evidencia:

En los informes de capacidad presentados, no se encuentran análisis de capacidad futura

Corrección	Evidencia de Implementación	Fecha
En el informe de capacidad se actualizará con la proyección de capacidad futura.	Informe de proyección de capacidad futura	15-01-2019

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

¿POR QUÉ?	MOTIVO
En los informes de capacidad presentados, no se encuentran análisis de capacidad futura	La medición de la capacidad de la infraestructura tecnológica se realiza con criterios de corto plazo, soportado en informes mensuales de consumo de: Memoria RAM, CPU y almacenamiento.
La medición de la capacidad de la infraestructura tecnológica se realiza con criterios de corto plazo, soportado en informes mensuales de consumo de: Memoria RAM, CPU y almacenamiento.	No se han definido los criterios e instrumentos para normalizar el procedimiento de recolección y análisis de datos que permitan establecer los requisitos de capacidad futura en recursos tecnológicos, físicos y humanos.

CAUSA RAÍZ	**No se han definido los criterios e instrumentos para normalizar el procedimiento de recolección y análisis de datos que permitan establecer los requisitos de capacidad futura en recursos tecnológicos, físicos y humanos.**

Acción correctiva	**Evidencia de Implementación**	**Fecha**
Definir los criterios e instrumentos que permitan medir los requisitos de capacidad y la proyección futura de los recursos tecnológicos, físicos y humanos.	Matriz de gestión de la capacidad.	30-4-19
Realizar el análisis de capacidad futura de acuerdo al procedimiento definido.	Análisis de capacidad	30-5-19
Verificar la eficacia de las acciones implementadas.	Medición de la eficacia en la herramienta ISOTools	30-08-19

Diligenciar tantos cuadros como sea necesario para cada no conformidad.

Nota: Es importante que la organización realice un buen análisis de causa para evitar que la no conformidad se repita y el plan de acción sea devuelto por el equipo auditor, por lo cual les sugerimos consultar la guía para la solución de no conformidades, disponible en la página web de Icontec.

Ruta: www.icontec.org – Documentos servicios ICONTEC ó a través del link: http://www.icontec.org/Paginas/Documentos-servicios-icontec.aspx

SOLICITUD DE ACCIÓN CORRECTIVA	No. 6 de 10

[ ] No - Conformidad Mayor [X] No - Conformidad Menor	Norma(s): ISO IEC 27001:2013	Requisito(s): A.12.3.1

Descripción de la no conformidad:

NO se encuentran pruebas de restauración para todas las bases de datos

Evidencia:

NO hay pruebas de restauración para Wm CCOA .
NO se encuentra el Plan de pruebas de restauración según la política de Respaldo

Corrección	Evidencia de Implementación	Fecha
Ajustar Política de Backup y Recuperación, el cual debe contemplar la realización de pruebas de restauración de la totalidad de backups de servidores.	Política de Backup y Recuperación	14-12-17

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

¿POR QUÉ?	MOTIVO
No se encuentran pruebas de restauración para todas las bases de datos	En el plan de pruebas de restauración definido en la mesa de ayuda, se define realizar pruebas de restauración aleatoria a los servidores respaldados.
En el plan de pruebas de restauración definido en la mesa de ayuda, se define realizar pruebas de restauración aleatoria a los servidores respaldados.	No se consideró pertinente realizar pruebas de restauración de cada Backup, se dio relevancia a la recuperación total de los medios de almacenamiento y no a cada imagen contenida en ellos.
No se consideró pertinente realizar pruebas de restauración de cada Backup, se dio relevancia a la recuperación total de los medios de almacenamiento y no a cada imagen contenida en ellos.	En la política de Backup y Recuperación no se tiene establecido la realización de pruebas de restauración del 100% de los Backup.
CAUSA RAÍZ	**En la política de Backup y Recuperación no se tiene establecido la realización de pruebas de restauración del 100% de los Backup.**

Acción correctiva	**Evidencia de Implementación**	**Fecha**
Elaborar un plan de pruebas de restauración que incluya periodicidad, total de servidores respaldados y medios.	Plan de pruebas de respaldo	20-1-19
Ejecución de la totalidad del plan de pruebas	Informe de pruebas realizadas	30-7-19
Verificar la eficacia de las acciones implementadas	Medición de la eficacia en la herramienta ISOTools	30-09-19

Diligenciar tantos cuadros como sea necesario para cada no conformidad.

Nota: Es importante que la organización realice un buen análisis de causa para evitar que la no conformidad se repita y el plan de acción sea devuelto por el equipo auditor, por lo cual les sugerimos consultar la guía para la solución de no conformidades, disponible en la página web de Icontec.

Ruta: www.icontec.org – Documentos servicios ICONTEC ó a través del link: http://www.icontec.org/Paginas/Documentos-servicios-icontec.aspx

SOLICITUD DE ACCIÓN CORRECTIVA	No. 7 de 10

[ ] No - Conformidad Mayor [X] No - Conformidad Menor	Norma(s): ISO IEC 27001:2013	Requisito(s): A.12.4.4

Descripción de la no conformidad:

Los relojes no están sincronizados con una única fuente de referencia de tiempo

Evidencia:

Se encuentra que hay dos cámaras con horas diferentes (11:40 y 11:57).
Se evidenció una diferencia horaria al recuperar una grabación del día de la auditoria (15 Nov 11:52) de más de 7 minutos

Corrección	Evidencia de Implementación	Fecha
Ajustar los parámetros de configuración de fecha y hora en todos los dispositivos de procesamiento de información, cámaras y servidor de videovigilancia.	Procedimiento documentado	30-11-18
Incluir en el patrón operacional *Gestión de Activos de Tecnología*, el procedimiento para la instalación y configuración de los dispositivos de procesamiento de información y de videovigilancia.	Procedimiento documentado	15-12-18

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

¿POR QUÉ?	MOTIVO
Se encuentra que hay dos cámaras con horas diferentes (11:40 y 11:57). Se evidenció una diferencia horaria al recuperar una grabación del día de la auditoria (15 Nov 11:52) de más de 7 minutos	La configuración de fecha y hora de cada cámara se realizó de forma manual en cada dispositivo y se dejó para mostrarse en pantalla junto con la fecha y hora del servidor de cámaras. Con lo cual, se evidenció la no correspondencia entre estos datos.
La configuración de fecha y hora de cada cámara se realizó de forma manual en cada dispositivo y se dejó para mostrarse en pantalla junto con la fecha y hora del servidor de cámaras. Con lo cual, se evidenció la no correspondencia entre estos datos.	Para el seguimiento y revisión de los videos almacenados, siempre se toma en cuenta la hora del servidor de video, el cual se encuentra sincronizado con el servidor de dominio.
Para el seguimiento y revisión de los videos almacenados, siempre se toma en cuenta la hora del servidor de video, el cual se encuentra sincronizado con el servidor de dominio.	No existe un procedimiento documentado para la configuración, sincronización y revisión de la fecha y hora en los dispositivos de procesamiento de información y de seguridad.

CAUSA RAÍZ	**No existe un procedimiento documentado para la configuración, sincronización y revisión de la fecha y hora en los dispositivos de procesamiento de información y de seguridad.**

Acción correctiva	**Evidencia de Implementación**	**Fecha**
Documentar en el patrón operacional Revisión del estado y funcionamiento de la infraestructura tecnológica, el procedimiento para el seguimiento de los recursos de videovigilancia y otros dispositivos.	Procedimiento documentado	30-1-19
Verificar la eficacia de las acciones implementadas.	Medición de la eficacia en la herramienta ISOTools	30-04-19

Diligenciar tantos cuadros como sea necesario para cada no conformidad.

Nota: Es importante que la organización realice un buen análisis de causa para evitar que la no conformidad se repita y el plan de acción sea devuelto por el equipo auditor, por lo cual les sugerimos consultar la guía para la solución de no conformidades, disponible en la página web de Icontec.

Ruta: www.icontec.org – Documentos servicios ICONTEC ó a través del link: http://www.icontec.org/Paginas/Documentos-servicios-icontec.aspx

SOLICITUD DE ACCIÓN CORRECTIVA	No. 8 de 10

[ ] No - Conformidad Mayor [X] No - Conformidad Menor	Norma(s): ISO IEC 27001:2013	Requisito(s): A.12.6.1

Descripción de la no conformidad:

No se tienen oportunidad en el análisis de vulnerabilidades

Evidencia:

No se ha realizado el análisis de vulnerabilidades del año 2018

Corrección	Evidencia de Implementación	Fecha
Planear la realización de las pruebas de vulnerabilidades para el segundo trimestre del año, plan de remediación para el tercer trimestre y reanálisis en el cuarto trimestre.	Cronograma de actividades 2019 SGSI	15-12-18

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

No se ha realizado el análisis de vulnerabilidades del año 2018	Las pruebas de vulnerabilidades 2018 fueron planeadas para desarrollarse en el mes de noviembre.
Las pruebas de vulnerabilidades 2018 fueron planeadas para desarrollarse en el mes de noviembre.	Esta actividad se definió en el cronograma del SGSI para realizarse durante el último trimestre del año y el plan de acción resultante, desarrollarlo durante el primer semestre del año siguiente.
Esta actividad se definió en el cronograma del SGSI para realizarse durante el último trimestre del año y el plan de acción resultante, desarrollarlo durante el primer semestre del año siguiente.	La norma no exige periodicidad ni fechas específicas para la realización de dichas pruebas.
CAUSA RAÍZ	**Esta actividad se definió en el cronograma del SGSI para realizarse durante el último trimestre del año y el plan de acción resultante, desarrollarlo durante el primer semestre del año siguiente.**

Acción correctiva	Evidencia de Implementación	Fecha
Realización de pruebas de vulnerabilidades	Informe de pruebas	15 -6-19
Retest a las pruebas de vulnerabilidades	Informe de reanálisis	30 -9-19
Verificar la eficacia de las acciones implementadas	Medición de la eficacia en la herramienta ISOTools	30-10-19

Diligenciar tantos cuadros como sea necesario para cada no conformidad.

Nota: Es importante que la organización realice un buen análisis de causa para evitar que la no conformidad se repita y el plan de acción sea devuelto por el equipo auditor, por lo cual les sugerimos consultar la guía para la solución de no conformidades, disponible en la página web de Icontec.

Ruta: www.icontec.org – Documentos servicios ICONTEC ó a través del link: http://www.icontec.org/Paginas/Documentos-servicios-icontec.aspx

SOLICITUD DE ACCIÓN CORRECTIVA	No. 9 de 10

[ ] No - Conformidad Mayor [X] No - Conformidad Menor	Norma(s): ISO IEC 27001:2013	Requisito(s): A.17.2.1

Descripción de la no conformidad:

No se encuentra redundancia en el sitio de procesamiento alterno

Evidencia:

No se han definido los requisitos de redundancia tecnológica ni de requisitos de seguridad de la información en el sitio alterno de la Ceja

Corrección	Evidencia de Implementación	Fecha
Definir los requisitos de redundancia tecnológica y de seguridad de la información en el sitio de recuperación alterno La Ceja	Lista de verificación de requerimientos	15-12-18

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

¿POR QUÉ?	MOTIVO
No se han definido los requisitos de redundancia tecnológica ni de requisitos de seguridad de la información en el sitio alterno de la Ceja	El plan de continuidad para la prestación del servicio CORE (Registros públicos) y procesos básicos de apoyo, fue aprobado recientemente por la alta dirección como primera fase del plan de continuidad de negocio.
El plan de continuidad para la prestación del servicio CORE (Registros públicos) y procesos básicos de apoyo, fue aprobado recientemente por la alta dirección como primera fase del plan de continuidad de negocio.	El plan de continuidad de negocio se ha establecido por fases, para el 2019, se ha presupuestado la adecuación de los requerimientos tecnológicos del sitio de recuperación La Ceja.
CAUSA RAÍZ	**El plan de continuidad de negocio se ha establecido por fases, para el 2019, se ha presupuestado la adecuación de los requerimientos tecnológicos del sitio de recuperación La Ceja.**

Acción correctiva	Evidencia de Implementación	Fecha
Implementar los servicios de redundancia identificados para asegurar la prestación del servicio en contingencia en la sede La Ceja.	Informe de pruebas realizadas	30-5-19
Verificar la eficacia de las acciones implementadas	Medición de la eficacia en la herramienta ISOTools	30-07-19

Diligenciar tantos cuadros como sea necesario para cada no conformidad.

Nota: Es importante que la organización realice un buen análisis de causa para evitar que la no conformidad se repita y el plan de acción sea devuelto por el equipo auditor, por lo cual les sugerimos consultar la guía para la solución de no conformidades, disponible en la página web de Icontec.

Ruta: www.icontec.org – Documentos servicios ICONTEC ó a través del link: http://www.icontec.org/Paginas/Documentos-servicios-icontec.aspx

SOLICITUD DE ACCIÓN CORRECTIVA	No. 10 de 10

[ ] No - Conformidad Mayor [X] No - Conformidad Menor	Norma(s): ISO IEC 27001:2013	Requisito(s):

Descripción de la no conformidad:

No se encuentra eficacia en la implementación de procedimientos para asegurar el cumplimento de software patentado

Evidencia:

Se encuentra en uso en los computadores de sucursales de LA CEJA y GUATAPÉ el software Team Viewer de uso gratuito y de utilización no comercial

Corrección	Evidencia de Implementación	Fecha
Desinstalar de los equipos reportados el Software no autorizado, así mismo realizar auditoría a todos los equipos del dominio.	Reporte de auditoría de equipos del dominio.	15-12-18
Incluir en el patrón operacional Gestión de Activos de Tecnología, el procedimiento para el seguimiento y control de software instalado para análisis por parte del usuario o en su versión de prueba.	Patrón operacional Gestión de Activos de Tecnología actualizado	15-12-18
Diseñar flujo de tareas en la mesa de servicios TI para requerimientos de instalación software de prueba.	Proceso creado en módulo de servicios TI	15-12-18

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

Se encuentra en uso en los computadores de sucursales de LA CEJA y GUATAPÉ el software Team Viewer de uso gratuito y de utilización no comercial.	El área de Tecnología empleó la versión de prueba del software Team Viewer con el fin de prestar soporte remoto a los asesores de las oficinas receptoras. Sin embargo, al finalizar el periodo de prueba, no se procedió con la desinstalación.
El área de Tecnología empleó la versión de prueba del software Team Viewer con el fin de prestar soporte remoto a los asesores de las oficinas receptoras. Sin embargo, al finalizar el periodo de prueba, no se procedió con la desinstalación.	No se cuenta con un procedimiento documentado para el seguimiento y control de software instalado para análisis por parte del usuario o en su versión de prueba.
No se cuenta con un procedimiento documentado para el seguimiento y control de software instalado para análisis por parte del usuario o en su versión de prueba.	El procedimiento actual está establecido para sólo una revisión anual de las estaciones de trabajo del dominio.

CAUSA RAÍZ	**El procedimiento actual está establecido para sólo una revisión anual de las estaciones de trabajo del dominio.**

Acción correctiva	**Evidencia de Implementación**	**Fecha**
Realizar la programación de seguimiento y verificación de software instalado con periodicidad semestral desde la plataforma de servicios TI	Registrada en la plataforma de servicios TI	**31/01/2019**
Verificar la eficacia de las acciones implementadas	Medición de la eficacia en la herramienta ISOTools	30-06-2019

Diligenciar tantos cuadros como sea necesario para cada no conformidad.

Nota: Es importante que la organización realice un buen análisis de causa para evitar que la no conformidad se repita y el plan de acción sea devuelto por el equipo auditor, por lo cual les sugerimos consultar la guía para la solución de no conformidades, disponible en la página web de Icontec.

Ruta: www.icontec.org – Documentos servicios ICONTEC ó a través del link: http://www.icontec.org/Paginas/Documentos-servicios-icontec.aspx

RESULTADOS DE AUDITORÍA:	
Número de no conformidades detectadas en esta auditoría: (0) Mayores (10) menores: 1 ISO 9001, 1 compartida en las normas y 8 de ISO IEC 27001 Número de no conformidades pendientes que no se cerraron en esta auditoría: (0) 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 : 2018-11-30 Fecha tentativa de verificación complementaria, cuando aplique NO APLICA	
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 _____ y el requisito al que fue reportada _____. En este caso la organización deberá solicitar una reposición dirigida al Jefe de Certificación.	
Nombre del Representante de la Organización: Maryori Ocampo Ocampo Líder de Planeación Estratégica y Gestión Organizacional	Firma: