

INFORME DE AUDITORÍA DE SISTEMAS DE GESTIÓN



1. INFORMACIÓN GENERAL			
1.1. ORGANIZACIÓN			
CONSEJO SUPERIOR DE LA JUDICATURA - RAMA JUDICIAL DEL PODER PÚBLICO DE COLOMBIA/CONSEJO SUPERIOR DE LA JUDICATURA			
1.2. SITIO WEB: https://www.ramajudicial.gov.co/web/consejo-superior-de-la-judicatura			
1.3. LOCALIZACIÓN DEL SITIO PERMANENTE PRINCIPAL: Carrera 8 No 12B – 82 Bogotá D.C., Colombia.			
1.3.1 LOCALIZACION DE OTROS SITIOS PERMANENTES INCLUIDOS EN EL CERTIFICADO			
# Sitios Permanentes adicionales	Sedes y direcciones de los sitios permanentes (diferentes al sitio principal)	Localización (ciudad - país)	Actividades del alcance del sistema de gestión, desarrollados en este sitio
1	Carrera 7 # 27-18	Bogotá D.C., Colombia	Todas las actividades del alcance
1.4. ALCANCE DE LA CERTIFICACIÓN:			
Gestión tecnológica referente al servicio público de administrar justicia en la rama judicial. Declaración de Aplicabilidad CSJ-SGSI-PDA V1.			
Technological management regarding the public service of administering justice in the judicial branch. Statement of Applicability CSJ-SGSI-PDA V1.			
1.5. CÓDIGO IAF: SI-4			
1.6. REQUISITOS DE SISTEMA DE GESTIÓN: ISO/IEC 27001:2013			
1.7. REPRESENTANTE DE LA ORGANIZACIÓN			
Nombre:	William espinosa Santamaría		
Cargo:	Coordinador Nacional SIGCMA		
Correo electrónico	coornacalidbta@cendoj.ramajudicial.gov.co		
1.8. TIPO DE AUDITORÍA:			
<input type="checkbox"/> Inicial o de Otorgamiento <input checked="" type="checkbox"/> Seguimiento 1 <input type="checkbox"/> Seguimiento 2 <input type="checkbox"/> Renovación <input type="checkbox"/> Renovación (con restauración) <input type="checkbox"/> Renovación (anticipada) <input type="checkbox"/> Renovación (anticipada para unificar ciclos) <input type="checkbox"/> Ampliación <input type="checkbox"/> Reducción <input type="checkbox"/> Auditoria especial (reactivación/extraordinaria) <input type="checkbox"/> Actualización			
Es organización multisitio: Si <input checked="" type="checkbox"/> No <input type="checkbox"/>			

Este informe es propiedad de ICONTEC y se comunicará después de la auditoría únicamente a la Organización y no será divulgado a terceros sin autorización de la Organización

INFORME DE AUDITORÍA DE SISTEMAS DE GESTIÓN



Auditoría combinada: Si <input type="checkbox"/> No <input checked="" type="checkbox"/>		
Auditoría integrada: Si <input type="checkbox"/> No <input checked="" type="checkbox"/>		
1.9. Tiempo de auditoría		
	FECHA	Días de auditoría)
Etapa 1 (Si aplica)	-	-
Preparación de la auditoría y elaboración del plan	2023-08-14	1.0
Auditoría remota	-	-
Auditoría en sitio	2023-09-27/28/29/30	4.0
1.10. EQUIPO AUDITOR		
Auditor Coordinador	-	
Auditor Líder	Diego Camilo Rodríguez	
Auditor	-	
Experto Técnico	-	
Observador	-	
1.11. DATOS DEL CERTIFICADO DE SISTEMA DE GESTIÓN		
Código asignado por ICONTEC		
Fecha de aprobación inicial		
Fecha de próximo vencimiento:		

2. OBJETIVOS DE LA AUDITORÍA
<p>2.1. Determinar la conformidad del sistema de gestión con los requisitos de la norma de sistema de gestión.</p> <p>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 gestión</p> <p>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.</p> <p>2.4. Identificar áreas de mejora potencial del sistema de gestión.</p>

3. ACTIVIDADES DESARROLLADAS
<p>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.</p> <p>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.</p>

Este informe es propiedad de ICONTEC y se comunicará después de la auditoría únicamente a la Organización y no será divulgado a terceros sin autorización de la Organización

- 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
- 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 NA X
- 3.8. Si se aplicó toma de muestra de múltiples sitios, indicar cuáles sitios permanentes se auditaron, en qué fechas: No se realizó toma de muestra se auditaron las dos sedes.
- 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 No NA X
- 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 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 Sin embargo se revisa desde el punto de vista de desarrollo de software, dominio A.14.
- 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 X

Este informe es propiedad de ICONTEC y se comunicará después de la auditoría únicamente a la Organización y no será divulgado a terceros sin autorización de la Organización

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

En caso afirmativo, cuáles:

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 NA

En caso afirmativo descríbalas,

3.16. ¿Se tienen actividades, productos y servicios declarados en el alcance del certificado que han sido tercerizados con proveedores o contratistas?

Si No

¿En caso afirmativo, se encontraron controlados los proveedores o contratistas de estas actividades, productos y servicios?

Si No

En el caso en el cual la organización subcontrate el suministro de actividades, productos y servicios que hacen parte del alcance certificado, relaciónelos en la siguiente tabla

Actividades, productos y servicios incluidos en el alcance de certificación que son subcontratados:	Proveedor/Contratista:	Requisito legal para el funcionamiento u operación (en caso de ser aplicable)
NUBE PRIVADA	IFX NETWORKS MICROSOFT AZURE	NA
SERVICIOS DE CIBERSEGURIDAD	ERNST AND YOUNG	NA

3.17. ¿Se presentaron, durante la auditoría, cambios que hayan impedido cumplir con el plan de auditoría inicialmente acordado con la Organización?

Si No En caso afirmativo, cuáles:

3.18. ¿Existen aspectos o resultados significativos de esta auditoría, que incidan en el programa de auditoría del ciclo de certificación?

Si No

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

Este informe es propiedad de ICONTEC y se comunicará después de la auditoría únicamente a la Organización y no será divulgado a terceros sin autorización de la Organización

3.20. ¿Aplica reactivación para este servicio?
 Si No NA

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	No se auditaron los requisitos A.13 y A.14, durante el ejercicio de auditoría interna 2022. Evidencia: Documentos de programa, plan e informe auditoría interna 27001 ejecutada en el 2022. 9.2 a) b)	Programa y plan de auditoría 2023. Informe de auditoría 2023. Hallazgos de auditoría 2023. Se evidencia cumplimiento de auditoría en donde se verificaron todos los requisitos de la norma.	SI
2	El reloj del control biométrico y la cámara de seguridad principal del centro de datos CAN tienen un desfase horario de 10 minutos. Evidencia: Registros de cámara y acceso biométrico del centro de datos CAN. A.12.4.4	Sincronización dispositivos con protocolo NTP Revisión de actualización horaria en proceso de auditoría interna. Se evidencia en auditoría externa según prueba realizada que la sincronización de los dispositivos biométricos y de las cámaras están alineadas a la hora legal colombiana.	SI
3	No se ha realizado auditoría al proveedor NEMO quien presta servicios de SOC, y BEST TECHNOLOGY quien presta servicio de software BEST DOC. Evidencia: Registro de auditoría a proveedores.	Auditoría a proveedores 2023. Se evidencian informes de verificación a proveedores críticos de tecnología.	SI

4. 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.

- La formación de 652 servidores judiciales temas como 27001 y 22301, debido a que aumenta la competencia y conocimiento en estándares de seguridad y la continuidad operativa del sistema judicial.

Este informe es propiedad de ICONTEC y se comunicará después de la auditoría únicamente a la Organización y no será divulgado a terceros sin autorización de la Organización

- Capacitación OWASP Top Ten, ya que aumenta la conciencia de seguridad y reduce las vulnerabilidades en el desarrollo de aplicaciones.
- Azure Sentinel, ya que proporciona visibilidad de amenazas, mejorando la capacidad de detección y respuesta a incidentes.
- Pruebas de ingeniería social, ya que identifican debilidades en la conciencia de seguridad de los empleados y mejoran la resistencia ante ataques de ingeniería social.
- Contratación de profesionales de ciberseguridad, ya que fortalece el equipo interno y mejora la capacidad de respuesta a amenazas.
- Alianza con Ernest and Young, ya que aporta experiencia externa y conocimientos especializados para afinar las estrategias de ciberseguridad.

4.2 Oportunidades de mejora

- Implementar 27701, protección datos personales, con el fin de continuar fortaleciendo el cumplimiento de regulaciones y salvaguardar la privacidad de los datos.
- Contratar al profesional universitario grado 20, de acuerdo al acuerdo PCSJA22-12033 del 29/12/2022, para fortalecer el equipo con habilidades específicas y experiencia.
- Definir criterios para un programa de restauración de información, a fin de establecer directrices claras y efectivas.
- Establecer una plantilla para pruebas de restauraciones, con el fin de estandarizar y simplificar el proceso de verificación de recuperación de datos.
- Establecer una metodología única para gestionar los cambios de infraestructura, software y soporte técnico, para mantener la consistencia y el control en el proceso de cambio.
- Definir métricas de gestión de cambios, con el objetivo de medir y evaluar el impacto de las modificaciones en el entorno tecnológico.
- Fortalecer proyecciones de capacidad futura, incluso si es en la nube, para asegurar la escalabilidad y la adaptación a las necesidades cambiantes.
- Definir periodos de revisión de controles de seguridad de forma independiente, para mantener una evaluación continua y efectiva de la seguridad.
- Fortalecer la redacción de hallazgos en el informe de auditoría interna, para comunicar de manera clara y efectiva los resultados y las recomendaciones.

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

5.1. Análisis de la eficacia del sistema de gestión certificado

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

Principales quejas o reclamaciones recurrentes	Principal causa	Acciones tomadas
-	-	-

Este informe es propiedad de ICONTEC y se comunicará después de la auditoría únicamente a la Organización y no será divulgado a terceros sin autorización de la Organización

5.1.2. Incluir la ocurrencia de incidentes (accidentes o emergencias) en los sistemas de gestión que aplique y explique brevemente cómo fueron tratados:

En 2023 se han presentado 2 incidentes de seguridad. El más grave fue presentado a raíz de falla en el proveedor IFX NETWORKS por ataque de ransomware. El día 12 de septiembre de 2023, se presentó este caso, el cual fue abordado a nivel nacional ya que afectó a diversas instituciones publicas y entidades privadas que tenían sus servicios en dicho proveedor. El CSJ decidió activar su plan de contingencia según lo establecido en su plan de continuidad que consistía en llevar procesos manuales e intentar recuperar de forma independiente al proveedor IFX NETWORKS los servicios críticos que el CSJ tenía respaldados de forma externa. Este proceso tardó 10 días sin embargo cuando los servicios se iban a poner en producción por parte del CSJ, el día 21 de septiembre IFX NETWORKSK informó que ya contaba con la disponibilidad de todos los servicios, por lo tanto el CSJ decidió continuar con la operación desde dicho proveedor. En la actualidad el CSJ evalua distintas acciones para mejorar su continuidad de negocio para futuros casos que lleguen a presentarse.

Otro incidente un poco menos grave que el anterior se presentó el 17 de mayo de 2023, en la plataforma Azure y fue la creación de maquinas virtuales masivas para llevar a cabo minería de datos. Este incidente se contuvo de forma exitosa y las acciones se encaminaron a implementar MFA, correlación de eventos con mayor nivel de detalle.

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 cómo fueron atendidas.

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

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 durante el ciclo de certificación

Auditoría	Número de no conformidades	Requisitos
Otorgamiento	3	9.2 a) b), A.12.4.4, A.15.2.1
1ª de seguimiento del ciclo	1	A.17.1.3
2ª de seguimiento del ciclo	-	-
Renovación	-	-
Auditorías especiales (Extraordinaria, reactivación)	-	-
Auditoria de ampliación		

Este informe es propiedad de ICONTEC y se comunicará después de la auditoría únicamente a la Organización y no será divulgado a terceros sin autorización de la Organización

¿Se evidencia recurrencia de no conformidades detectadas en las auditorías de ICONTEC en el último ciclo de certificación? Si <input type="checkbox"/> No <input checked="" type="checkbox"/>	
--	--

5.3 Análisis del proceso de auditoría interna

El equipo auditor fue conformado por 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. La duración de la auditoría interna se considera apropiada a la naturaleza y necesidades del sistema de gestión, se encontró programa, plan, informe de auditoría, análisis de causas y acciones correctivas para las no conformidades detectadas.

5.4 Análisis de la revisión del sistema por la dirección

Se realizó un análisis de los requisitos establecidos en el numeral 9.3, de los resultados de los procesos y de los compromisos establecidos por la dirección. 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 GESTIÓN Y DE LA MARCA O LOGO DE LA CERTIFICACIÓN

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

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

¿Se presentaron no conformidades mayores? SI NO

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

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

Este informe es propiedad de ICONTEC y se comunicará después de la auditoría únicamente a la Organización y no será divulgado a terceros sin autorización de la Organización

INFORME DE AUDITORÍA DE SISTEMAS DE GESTIÓN



En caso afirmativo diligencie el siguiente cuadro:

Fecha de la verificación complementaria: NA

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 auditoría			
No conformidades pendientes de la auditoría anterior que no se solucionaron			
No conformidades detectadas en esta auditoría que fueron cerradas			

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 R-PS-007.

8. RECOMENDACIÓN DEL EQUIPO AUDITOR DE ACUERDO CON EL R-PS-007

	SI	NO
Se recomienda otorgar la Certificación del Sistema de Gestión		
Se recomienda mantener el alcance del certificado del Sistema de Gestión		
Se recomienda renovar el certificado del Sistema de Gestión		
Se recomienda renovar anticipadamente 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 restaurar el certificado, una vez finalice el proceso de renovación		
Se recomienda suspender el certificado		
Se recomienda cancelar el certificado		
Nombre del auditor líder: Diego Camilo Rodríguez	Fecha	2023
	10	16

9. ANEXOS QUE FORMAN PARTE DEL PRESENTE INFORME

Anexo 1	Correcciones, análisis de causa y acciones correctivas		
			X

Este informe es propiedad de ICONTEC y se comunicará después de la auditoría únicamente a la Organización y no será divulgado a terceros sin autorización de la Organización

INFORME DE AUDITORÍA DE SISTEMAS DE GESTIÓN

Anexo 2	Información específica de esquemas de certificación de sistema de gestión	X
Anexo 3	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 4	Aceptación de los resultados de la auditoría firmada por la organización.	X
Anexo 5	F-PS-946 ANEXO 5 ANÁLISIS DE RIESGOS DE AUDITORÍAS DE SISTEMAS DE GESTIÓN	NA
Anexo 6	Confirmación de cumplimiento de los objetivos de la auditoría con el uso de las TIC	NA
Anexo 7	Declaración de aplicación (solo para ISO 28001)	NA
Anexo 8	Verificación de riesgos y requisitos para realizar auditorías con la participación de Expertos Técnicos	NA

ANEXO 1 CORRECCIONES, CAUSAS Y ACCIONES CORRECTIVAS.

- Se recibió la propuesta de correcciones, análisis de causas y acciones correctivas para la solución de no conformidades el AAAA-MM-DD 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 AAAA-MM-DD.

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.

Consulte la *Guía para la solución de no conformidades* en la [página web de Icontec www.icontec.org](http://www.icontec.org), en la ruta Nuestra Compañía – Documentos servicios – Evaluación de la Conformidad

ANEXO 2

Este informe es propiedad de ICONTEC y se comunicará después de la auditoría únicamente a la Organización y no será divulgado a terceros sin autorización de la Organización

INFORMACIÓN ESPECÍFICA DE ESQUEMAS DE CERTIFICACIÓN DE SISTEMA DE GESTIÓN

Esta sección se completa solo para los siguientes casos:

**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
-	-

- ¿Los procedimientos adoptados por el cliente brindan confianza en el SGSI/ SGPI?
Si X No
- Describa brevemente los documentos revisados como evidencia de las muestras tomadas para la evaluación del SGSI/ SGPI (Ver PE-PS-079 PROCEDIMIENTO ESPECIFICO PARA

Este informe es propiedad de ICONTEC y se comunicará después de la auditoría únicamente a la Organización y no será divulgado a terceros sin autorización de la Organización

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: Registro de incidentes o eventos de seguridad, Registro de vulnerabilidades, revisión de equipos políticas en equipos de cómputo, capacitación de seguridad de la información, declaración de aplicabilidad, Contexto, , identificación y análisis de riesgos, pruebas de continuidad (DRP), selección, evaluación y auditoría a proveedores, auditoría interna y revisión por la dirección entre otros.

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).

18 riesgos Inherentes: 4 EXTREMOS, 6 MODERADO y 8 ALTOS.

18 riesgos Residuales: 2 ALTOS, 8 MODERADOS Y 8 BAJOS.

Los planes de tratamiento están encaminados en fortalecer la infraestructura tecnológica y la ciberseguridad.

ANEXO 3 PLAN DE AUDITORÍA

ANEXO 4 FIRMA DE RESULTADOS

Este informe es propiedad de ICONTEC y se comunicará después de la auditoría únicamente a la Organización y no será divulgado a terceros sin autorización de la Organización