MEMORANDO

Al contestar, por favor cite el radicado:
No.:**20231100046783**

Bogotá D.C., 26 de Abril de 2023

PARA: **MIGUEL ANTONIO JIMENEZ PORTELA**
Subdirección Administrativa y Financiera

YESLY ALEXANDRA ROA MENDOZA
Jefe Oficina Asesora de Planeación

FABIÁN HUMBERTO FAJARDO RESTREPO
Subdirector Aprovechamiento (E)

CESAR MAURICIO BELTRAN LOPEZ
Jefe Oficina Tecnologías de la Información y Comunicaciones

DE: Oficina de Control Interno

ASUNTO: Resultado de la evaluación al cumplimiento de la UAESP a la Ley 1581 de 2012 sobre Protección de Datos Personales.

Respetado equipo directivo y gestores:

En cumplimiento del Plan Anual de Auditorías vigencia 2023, la Oficina de Control Interno (OCI) atentamente remite el informe Final de la Auditoria “Evaluación del nivel de cumplimiento de Ley 1581 de 2012 de protección de datos personales por parte de la Unidad Administrativa Especial de Servicios públicos -UAESP”.

El informe presenta la conclusión obtenida con corte a abril de 2023 de la auditoría realizada con base en la Guía de la Superintendencia de Industria y Comercio (SIC). Donde se evidenció un avance general del 60,1% en la implementación de la Protección de Datos Personales según la Ley 1581 de 2012. Frente a la evaluación basada en la guía de la Alta Consejería TIC de controles de seguridad y buenas prácticas, se observó un avance del 70%. En el informe podrán detallar y analizar junto con sus equipos de trabajo las evaluaciones realizadas en los papeles de trabajo anexos.

MEMORANDO

Bogotá D.C., 26 de Abril de 2023

De acuerdo con los resultados y conforme al procedimiento ECM-PC-03 V10 – Planes de Mejoramiento, para el caso de la observación presentada, es necesario que la OTIC formule el Plan de Mejoramiento Interno (PMI) junto con las acciones de mejora, con el objetivo de evitar incumplimientos normativos y minimizar la probabilidad de la materialización de los riesgos asociados. Para el caso de las recomendaciones queda a discreción del responsable del proceso, decidir sobre el tratamiento pertinente, no obstante, se alienta a los responsables en el marco de la mejora continua a también evaluar la suscripción de acciones en un PMI.

Para la suscripción acciones en PMI, se solicita que estas sean enviadas a la OCI dentro del término de diez (10) días hábiles siguientes al recibido de este documento.

Finalmente, desde la OCI agradecemos la atención y colaboración prestada por todos ustedes y los equipos de trabajo designados para el desarrollo de este ejercicio de auditoría. Cualquier información o aclaración al respecto, estaremos dispuestos a atenderla.

Cordialmente,

Sandra Beatriz Alvarado Salcedo

Firmado digitalmente por Sandra Beatriz Alvarado Salcedo
Fecha: 2023.04.26 16:21:10 -05'00'

SANDRA BEATRIZ ALVARADO SALCEDO
Jefe Oficina de Control Interno
Sandra.alvarados@uaesp.gov.co

Anexos: Informe de Auditoría Interna y Papeles de Trabajo (3).
Elaboró: Ligia Marlén Velandia León. PE-222-24-OCI – Osbaldo cortes Lozano P.E (e)-222-24-OCI

ENFOQUE DE LA AUDITORIA INTERNA	GESTIÓN Y RESULTADOS [1]	ANÁLISIS FINANCIERO Y CONTABLE [1]	LEGAL [1]	SISTEMA DE GESTIÓN [2]
	X			
INFORME [3]	Verificar el cumplimiento de la normatividad vigente relacionada con la Protección Datos Personales por parte de los procesos de OAP, OTIC, Atención al Ciudadano y SAPROV.			
PROCESO, PROCEDIMIENTO, O DEPENDENCIA	• OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES – OTIC • OFICINA ASESORA DE PLANEACIÓN - OAP • SUBDIRECCIÓN DE APROVECHAMIENTO – SAPROV y ATENCIÓN AL CIUDADANO			
RESPONSABLE O AUDITADOS	Equipos de Trabajo: OAP, OTIC, Atención al Ciudadano y SAPROV.			
OBJETIVO	Evaluar el nivel de cumplimiento de la Ley 1581 de 2012 de protección de datos personales y su correspondiente normatividad reglamentaria vigente en la UAESP.			
ALCANCE	Evaluar el cumplimiento normativo de la UAESP frente a la Protección de Datos Personales - Ley 1581 de 2012.			
PERIODO DE EJECUCIÓN	Marzo 01 al 28 abril de 2023.			
EQUIPO AUDITOR	Ligia Marlén Velandia León (LMVL) - Osbaldo Cortés Lozano (OCL)			
DOCUMENTACIÓN ANALIZADA [4]	Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales. • Decreto 1727 de 2009: Información titulares. • Decreto 2952 de 2010 Reglamentación 1266 de 2012: Disposiciones generales hábeas data. • Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012. • Decreto 886 de 2014. - Reglamentación RNBD. • Decreto 1074 de 2015 – RNBD. • Guía sobre el tratamiento de datos personales en las entidades estatales. Superintendencia de Industria y Comercio – SIC. • Política de PDP – UAESP. • Procedimientos MIPG vigentes. • GTI-MN-05 V1 Tratamiento de Datos Personales • Política para el Tratamiento de Datos Personales UAESP V3. • Resolución 490-2022 Designación Oficial de Datos Personales.			

(1) Marque con X el enfoque de la Auditoría Interna.
(2) Señale el (los) sistema(s) de gestión evaluado(s).
(3) Establezca el título general del Informe de Auditoría Interna.
(4) Realice una relación de la documentación analizada con base en los criterios de auditoría definidos

1. DESCRIPCIÓN GENERAL DEL DESARROLLO DE LA AUDITORIA

La Oficina de Control Interno – OCI en cumplimiento del Plan Anual de Auditorías de la vigencia 2023, planificó la ejecución de la auditoria con radicado No. 20231100023693 – del 02 de marzo de 2023. El propósito de esta auditoría fue evaluar el nivel de cumplimiento de la Ley 1581 de 2012, sobre protección de datos personales, por parte de la UAESP para los procesos en la OTIC, OAP, SAPROV y ATENCIÓN AL CIUDADANO. Sin embargo, se constató que el proceso de ATENCIÓN AL CIUDADANO no presentó evidencias ni respuestas a los formularios aplicados.

Al consolidar las evidencias, realizar su validación y análisis de los papeles de trabajo, se evidenció que gran parte de las respuestas y soportes entregados aplican mayoritariamente al proceso de la OTIC, por esta razón se utilizó para la definición general de la auditoría, incluyendo las recomendaciones y conclusiones correspondientes. El análisis realizado a los procesos de SAPROV y OAP se tomó en cuenta solo para recomendaciones generales.

Esta auditoría se realizó con base en la guía y formularios de la Superintendencia de Industria y Comercio – SIC, bajo tres perspectivas de evaluación teniendo en cuenta la verificación de los aspectos contenidos en la ***"Guía sobre el tratamiento de datos personales en las entidades estatales"*** construida por la Delegatura para la Protección de Datos Personales de la siguiente manera:

1. ***PRIMERA PERSPECTIVA***: CUESTIONARIO DE DIAGNOSTICO PARA EL CUMPLIMIENTO DE LA LEY 1581 DE 2012 – SIC: 86 criterios organizados en 14 categorías con el fin de establecer el nivel de avance sobre los aspectos relevantes como: Principios para el tratamiento de datos personales, Tratamiento de datos sensibles y de menores de edad, Derechos de los titulares de información, Autorización para el tratamiento de datos personales, Información mínima a los titulares, Suministro de la información personal, Atención de consultas y reclamos de los titulares, Política de tratamiento de datos personales, Aviso de privacidad, Reporte de violaciones a los códigos de seguridad, Gestión de encargados del tratamiento, Transferencia y transmisión internacional de datos personales, Responsabilidad demostrada y Registro nacional de bases de datos.

2. ***SEGUNDA PERSPECTIVA***: VERIFICACIÓN DE AVANCE DE IMPLEMENTACIÓN DE LA LEY 1581 Protección de Datos Personales - PDP: 102 criterios organizados en 13 categorías conformadas de la siguiente manera: Desde la Alta Dirección, Oficial de protección de datos personales, Presentación de informes, Procedimientos operacionales, Inventario de bases de datos con información personal, Políticas, Sistema de administración de riesgos, Formación y educación, Protocolos de respuesta en el manejo de violaciones e incidentes de seguridad, Gestión de los encargados del tratamiento en las transmisiones internacionales de datos personales, Comunicación externa, Plan de supervisión y revisión, Evaluación y revisión de los controles del programa.

1. DESCRIPCIÓN GENERAL DEL DESARROLLO DE LA AUDITORIA

3. ***TERCERA PERSPECTIVA***: REVISIÓN CONTROLES SEGURIDAD DE DATOS - PROTECCIÓN DE DATOS PERSONALES - PDP: Esta se realizó con la aplicación de instrumento de verificación de controles de seguridad de datos, desarrollado por la Alta Consejería TIC del Distrito Capital, que contiene 33 criterios o controles organizados en 9 categorías así: Sección Gestión de riesgos en seguridad de los datos personales, Gestión de incidentes o incumplimientos en seguridad de los datos personales, Identificación de controles implementados de seguridad en la captura de la información de datos personales, Identificación de las Bases de Datos que tiene datos personales (según el alcance establecido a nivel de procesos y sistemas de información), Revisión del estado actual de los controles para el acceso a las bases de datos con información personal, Revisión del estado actual de controles de seguridad implementados en el almacenamiento de los datos personales (Ejemplo: Cifrado, acceso, entre otros), Revisión del estado actual de controles técnicos cuando se comparte la información de datos personales con terceras partes, Revisión del estado actual de controles técnicos en la eliminación de datos personales o cuando pasan a ser históricos, Revisión de controles de sensibilización y capacitación o formación a los servidores públicos en lo relacionado con protección de datos personales.

De esta manera el ejercicio desarrollado en su totalidad estuvo compuesto por la evaluación de los 221 criterios indicados en la Guía de la SIC.

Cada uno de estos criterios se evaluó con una calificación cuantitativa indicada en la siguiente tabla teniendo en cuenta el incumplimiento (0), y cumplimiento parcial o total (0.5 y 1) respectivamente. Para los casos que no aplica la calificación fue N/A por no tener el área o proceso responsabilidad en el respectivo criterio, como se observa a continuación:

Calificación	Descripción
1	Cumple
0,5	Parcial
0	No cumple
N/A	N/A

Tabla 1 - Criterio de evaluación - Fuente: Elaboración Propia.

Se aplicaron tres papeles de trabajo diseñados para valorar cada perspectiva y la evaluación se generó con base en las evidencias presentadas por los procesos y el desarrollo de los instrumentos respectivos.

Se siguieron las perspectivas para proceder con su evaluación de la siguiente manera:

1. DESCRIPCIÓN GENERAL DEL DESARROLLO DE LA AUDITORIA

1- ***PRIMERA PERSPECTIVA***: CUESTIONARIO DE DIAGNOSTICO PARA EL CUMPLIMIENTO DE LA LEY 1581 DE 2012 – SIC- Se procedió a aplicar el instrumento a los procesos de la OTIC, SAPROV y OAP, sin embargo, el proceso de Servicio al Ciudadano no presentó evaluación ni evidencias por lo que no se realizó la evaluación a este proceso. El resultado preponderante fue generado para la OTIC en todas las 14 categorías y 86 criterios de evaluación respectivamente. Con base en lo anterior la OCI verificó un avance del 68% con respecto a un 86% presentado por el proceso en su autoevaluación, como se observa a continuación tomando en consideración que algunos de los criterios que el proceso manifestó no aplica (N/A), a criterio del equipo evaluador si les aplica. Por esto, a pesar de que la calificación es similar, el resultado porcentual es diferente.

Criterios	Autoevaluación proceso	Evaluación OCI
1. Principios para el tratamiento de datos personales	4,5	3
2. Tratamiento de datos sensibles y de menores de edad	2	2,5
3. Derechos de los titulares de información.	3	1
4. Autorización para el tratamiento de datos personales	5,5	4,5
5. Información mínima a los titulares	3	4
6. Suministro de la información personal	2	2
7. Atención de consultas y reclamos de los titulares	9	9,5
8. Política de tratamiento de datos personales.	8	8
9. Aviso de privacidad	7	6,5
10. Reporte de violaciones a los códigos de seguridad	1	1
11. Gestión de encargados del tratamiento	6,5	6,5
12. Transferencia y transmisión internacional de datos personales.	0,5	3
13. Responsabilidad demostrada.	4	5
14. Registro nacional de bases de datos.	1	1
	57	**57,5**
	86%	**68%**

Tabla 2 - Resultados Evaluación Primera Perspectiva - Fuente Propia

2- ***SEGUNDA PERSPECTIVA***: VERIFICACIÓN DE AVANCE DE IMPLEMENTACIÓN DE LA LEY 1581 DE 2012 – SIC. Se procedió a aplicar el instrumento a los procesos de OTIC, SAPROV, OAP, el proceso de Servicio al Ciudadano no presentó evaluación ni evidencias. El resultado preponderante fue generado para OTIC en todas las 13 categorías y los 102 criterios de evaluación. De acuerdo con lo anterior se evidencia un avance de 53% con respecto a un 59% de la autoevaluación presentada por el proceso como se observa a continuación:

1. DESCRIPCIÓN GENERAL DEL DESARROLLO DE LA AUDITORIA

Criterios	Autoevaluación proceso	Evaluación OCI
1. Desde la Alta Dirección	3	3
2. Oficial de Protección de Datos Personales	10	10,5
3. Presentación de informes	0,5	0,5
4. Procedimientos operacionales	0	0
5. Inventario de bases de datos con información personal	10	8
6. Políticas	5,5	5
7. Sistema de administración de riesgos	5,5	4,5
8. Formación y Educación	4	4
9. Protocolos de respuesta en el manejo de violaciones e incidentes de seguridad	4,5	3,5
10. Gestión de los encargados del tratamiento en las transmisiones internacionales de datos personales	3	3
11. Comunicación externa	4	4
12. Plan de supervisión y revisión	0	0
13. Evaluación y revisión de los controles del programa	5	5
	55	**51**
	59%	**53%**

Tabla 3 - Resultados Evaluación Segunda Perspectiva - Fuente Propia

3- ***TERCERA PERSPECTIVA***: REVISIÓN CONTROLES SEGURIDAD DE DATOS – PROTECCIÓN DE DATOS PERSONALES: Este instrumento se aplicó únicamente a la OTIC, donde se evidencia un cumplimiento del 70% en comparación con la autoevaluación de OTIC que presentó un avance de 80% para las 9 categorías y 33 criterios:

Criterios	Autoevaluación proceso	Evaluación OCI
1. Sección Gestión de riesgos en seguridad de los datos personales	4	3,5
2. Gestión de incidentes o incumplimientos en seguridad de los datos personales	2,5	2,5
3. Identificación de controles implementados de seguridad en la captura de la información de datos personales.	3	3
4. Identificación de las Bases de Datos que tiene datos personales, según el alcance establecido a nivel de procesos y sistemas de información.	3	2,5

1. DESCRIPCIÓN GENERAL DEL DESARROLLO DE LA AUDITORIA

5. Revisión del estado actual de los controles para el acceso a las Bases de datos con información personales	4	3,5
6. Revisión del estado actual de controles de seguridad implementados en el almacenamiento de los datos personales (Ejemplo: Cifrado, acceso, entre otros).	3	2,5
7. Revisión del estado actual de controles técnicos cuando se comparte la información de datos personales con terceras partes.	2,5	1,5
8. Revisión del estado actual de controles técnicos en la eliminación de datos personales o cuando pasan a ser históricos.	2,5	2
9. Revisión de controles de sensibilización, capacitación o formación a los servidores públicos en lo relacionado con protección de datos personales	2	2
	26,5	23,0
	80%	**70%**

Tabla 4 - Resultados Evaluación Tercera Perspectiva - Fuente Propia

Como resultado de la evaluación, se observó un avance general de 60,5% en la implementación de las obligaciones de la entidad respecto a la protección de datos personales establecidas en la Ley 1581 de 2012 y su reglamentación, de acuerdo con la evaluación adelantada con base en la Guía de la Superintendencia de Industria y Comercio, la cual abarca los dos instrumentos aplicados en la primera y segunda perspectiva.

En relación con la evaluación realizada mediante el instrumento proporcionado por la Alta Consejería TIC del Distrito, sobre los controles de seguridad y buenas prácticas, se observó un avance general del 70% para la vigencia de 2023, con respecto a la autoevaluación del proceso que se ubicó en el 80%.

2. CONFORMIDADES Y FORTALEZAS

Una vez evaluados los instrumentos de la Superintendencia de Industria y Comercio aplicados para evaluar el avance de implementación de la Ley 1581 de 2012 de Protección de Datos Personales se presentan a continuación las conformidades y fortalezas encontradas, a saber:

2.1. La entidad cuenta con la Política para el Tratamiento de Datos Personales y el Manual de Tratamiento de Datos Personales, debidamente formalizados y publicados.

2.2. La UAESP, cuenta con el Oficial de Datos Personales, designado mediante la Resolución 490 de 2022.

2. CONFORMIDADES Y FORTALEZAS

2.3. De acuerdo con la evaluación realizada por la OCI, se verificó que la entidad ha logrado un avance del 60,5% en la implementación de la Guía de la SIC (perspectiva 1 y 2), y un avance del 70% en relación con el Instrumento proporcionado por la Alta Consejería TIC.

2.4. La OTIC realizó el reporte de las Bases de Datos de la entidad ante la Superintendencia de Industria y Comercio – SIC. Para esta auditoría se evidenciaron 142 bases de datos reportadas desde el 2018. Para la vigencia 2023 se han reportado cuatro (4) bases de datos, lo que evidencia cumplimiento frente a los requerimientos normativos, evitando así posibles sanciones.

2.5. La UAESP ha realizado varias capacitaciones, inducciones y socializaciones relacionadas con la política y procesos para la protección de datos personales al interior de la Entidad.

2.6. Durante la vigencia 2022, se presentó la materialización de un riesgo de Datos Personales en la entidad, el cual fue gestionado de manera oportuna mediante la aplicación de los protocolos establecidos para enfrentar este tipo de incidentes.

3. OBSERVACIONES

De acuerdo a lo establecido en la guía de la Superintendencia de Industria y Comercio – SIC, se evidenció que la UAESP no cuenta con un Programa Integral de Gestión de Datos Personales, con el objetivo de dar cumplimento a la Ley 1581 de 2012, los lineamientos de la Alta Consejería TIC Distrital y demás normatividad vigente y aplicable[1].

4. SOLICITUD DE CORRECCIÓN Y ACCIONES CORRECTIVAS

N/A

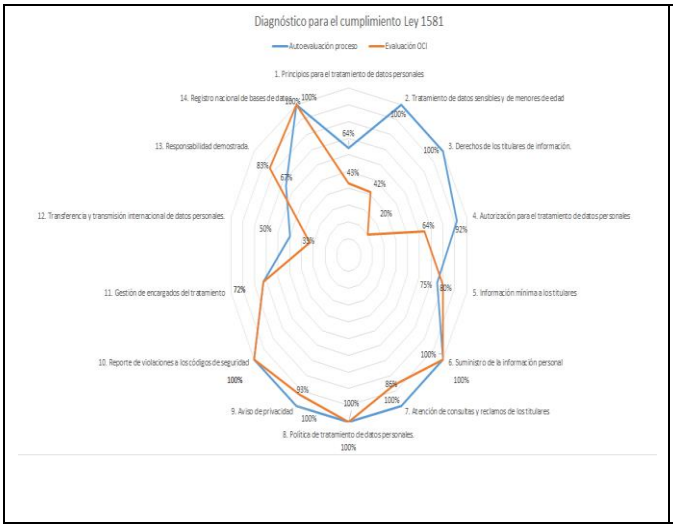
No.	DESCRIPCIÓN DE LA NO CONFORMIDAD	REQUISITO QUE INCUMPLE
-	N/A	

[1] Guia Accountability 26 pág (sic.gov.co)

5. CONCLUSIONES

Una vez realizada la evaluación de protección de datos personales se puede concluir lo siguiente:

5.1. Para el diagnóstico del cumplimiento de la Ley 1581 de 2012, de acuerdo con la valoración de la PRIMERA PERSPECTIVA con base en la Guía de la SIC, se encuentran algunos criterios con avances significativos, como son: *"6. Suministro de Información Personal, 8. Política de tratamiento de datos personales,10. Reporte de violaciones a los códigos de seguridad, 14. Registro nacional de base de datos".* A continuación se listan los criterios que se encuentran con un rezago en su implementación: *4. Derechos de los titulares de Información, 12. Transferencia y transmisión internacional de datos personales, 2. Tratamiento de datos sensibles y de menores de edad, 1. Principios para el tratamiento de datos personales";* por lo cual es importante que tengan en cuenta las recomendaciones emitidas junto con los demás criterios que se encuentran en una calificación promedio como se presenta en la siguiente gráfica y su respectivo cuadro resumen.

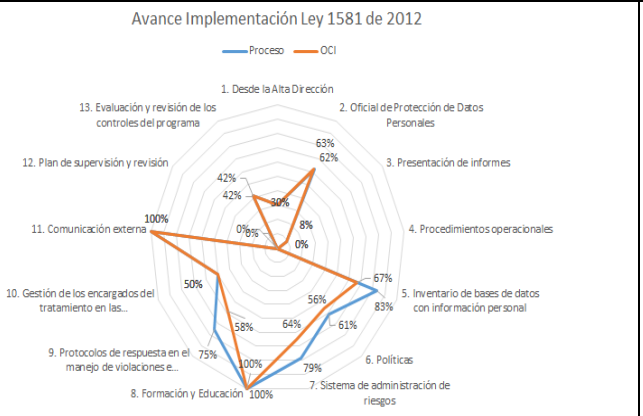


Criterios	Autoevaluación proceso	Evaluación OCI
1. Principios para el tratamiento de datos personales	64%	43%
2. Tratamiento de datos sensibles y de menores de edad	100%	42%
3. Derechos de los titulares de información.	100%	20%
4. Autorización para el tratamiento de datos personales	92%	64%
5. Información mínima a los titulares	75%	80%
6. Suministro de la información personal	100%	100%
7. Atención de consultas y reclamos de los titulares	100%	86%
8. Política de tratamiento de datos personales.	100%	100%
9. Aviso de privacidad	100%	93%
10. Reporte de violaciones a los códigos de seguridad	100%	100%
11. Gestión de encargados del tratamiento	72%	72%
12. Transferencia y transmisión internacional de datos personales.	50%	33%
13. Responsabilidad demostrada.	67%	83%
14. Registro nacional de bases de datos.	100%	100%

Tabla 5 - Diagnóstico cumplimiento 1581 - Fuente Propia

5.2. Para la verificación de avance de implementación de la Ley 1581 de 2012, de acuerdo con la valoración de la SEGUNDA PERSPECTIVA con base en la Guía de la SIC, se encuentran algunos criterios con avances significativos, como son: *"8. Formación y educación, 11. Comunicación externa",* así mismo, los que se encuentran en rezago de implementación: *"12. Plan de supervisión y revisión, 4. Procedimientos operacionales, 3. Presentación de informes, 1. Desde la alta dirección, 13. Evaluación y revisión de los controles del programa"*, por lo cual es importante que se tenga en cuenta las recomendaciones dadas junto con los demás criterios que se encuentran en una calificación promedio como se presenta en la siguiente gráfica y su respectivo cuadro resumen.

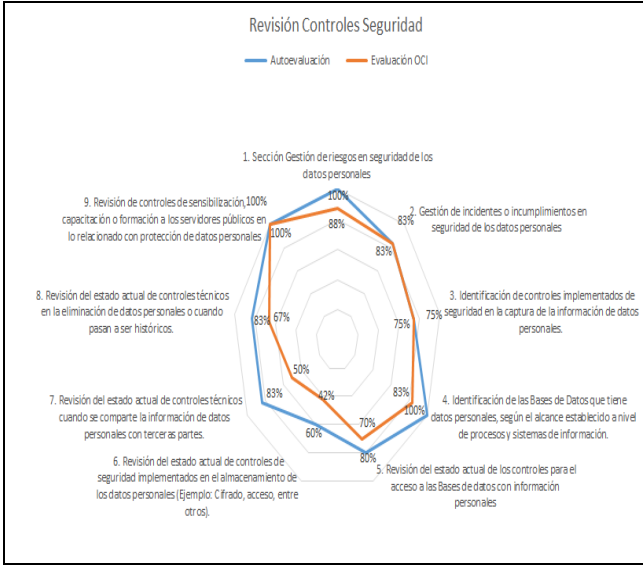
5. CONCLUSIONES



Criterios	Autoevaluación proceso	Evaluación OCI
1. Desde la Alta Dirección	30%	30%
2. Oficial de Protección de Datos Personales	63%	62%
3. Presentación de informes	8%	8%
4. Procedimientos operacionales	0%	0%
5. Inventario de bases de datos con información personal	83%	67%
6. Políticas	61%	56%
7. Sistema de administración de riesgos	79%	64%
8. Formación y Educación	100%	100%
9. Protocolos de respuesta en el manejo de violaciones e incidentes de seguridad	75%	58%
10. Gestión de los encargados del tratamiento en las transmisiones internacionales de datos personales	50%	50%
11. Comunicación externa	100%	100%
12. Plan de supervisión y revisión	N/A	0%
13. Evaluación y revisión de los controles del programa	42%	42%

Tabla 6 - Avance Implementación 1581 - Fuente Propia

5.3. De acuerdo con la verificación de controles de seguridad del instrumento de la Alta Consejería TIC del Distrito, la OCI verificó un avance general del 70%, algunos criterios cuentan con un avance medio, estos criterios son: *"6. Revisión del estado actual de controles de seguridad implementados en almacenamiento de los datos personales, 7. Revisión del estado actual de controles técnicos cuando se comparte la información de datos personales con terceras partes"*, por lo cual es importante que se atiendan las recomendaciones dadas, de acuerdo con la siguiente gráfica y su respectiva tabla base:



Criterios	Autoevaluación	Evaluación OCI
1. Sección Gestión de riesgos en seguridad de los datos personales	100%	88%
2. Gestión de incidentes o incumplimientos en seguridad de los datos personales	83%	83%
3. Identificación de controles implementados de seguridad en la captura de la información de datos personales.	75%	75%
4. Identificación de las Bases de Datos que tiene datos personales, según el alcance establecido a nivel de procesos y sistemas de información.	100%	83%
5. Revisión del estado actual de los controles para el acceso a las Bases de datos con información personales	80%	70%
6. Revisión del estado actual de controles de seguridad implementados en el almacenamiento de los datos personales (Ejemplo: Cifrado, acceso, entre otros).	60%	42%
7. Revisión del estado actual de controles técnicos cuando se comparte la información de datos personales con terceras partes.	83%	50%
8. Revisión del estado actual de controles técnicos en la eliminación de datos personales o cuando pasan a ser históricos.	83%	67%
9. Revisión de controles de sensibilización, capacitación o formación a los servidores públicos en lo relacionado con protección de datos personales	100%	100%

Tabla 7- Tabla 6 - Revisión Controles de Seguridad - Fuente Propia

5. CONCLUSIONES

5.4. Como resultado de la auditoría, la OCI evidenció un avance del 60.5% en la implementación de la Ley 1581 de 2012 con base en la Guía de la SIC.

5.5. En cuanto a los lineamientos de la Alta Consejería TIC del Distrito Capital la UAESP se encontró un avance del 70%.

6. RECOMENDACIONES

Con base en el desarrollo de la auditoría y teniendo en cuenta los diferentes artículos, de la Ley 1581 de 2012 y demás normatividad aplicable, se tuvieron en cuenta las calificaciones con promedio bajo, para los cuales se recomienda tener en cuenta los anexos para que a nivel interno los procesos realicen una evaluación con mayor profundidad.

6.1. PRIMERA PERSPECTIVA: CUESTIONARIO DE DIAGNOSTICO PARA EL CUMPLIMIENTO DE LA LEY 1581 DE 2012 – SIC:

- La OCI, recomienda contar con el consentimiento previo, expreso e informado para el tratamiento de datos de los Titulares de los cuales se recolecta información personal, de manera registrada y trazable.
- Con base en el criterio *"Se conserva información personal veraz, completa, exacta, actualizada, comprobable y comprensible"*, se recomienda complementar el aviso de privacidad incluyendo *"que los datos son reales"*. De otra parte, se recomienda contar con un repositorio institucional para evitar que la información quede en repositorios de las cuentas personales tanto de los servidores como los contratistas.
- Se recomienda para el criterio *"¿Se garantiza la confidencialidad de la información por las personas de la organización que intervienen en el Tratamiento de datos personales, incluso después de que han finalizado su relación?"*: complementar con los controles técnicos como ORFEO y RURO, garantizando la confidencialidad de la información, con el objetivo que ninguna persona sin autorización u otra área la puedan ver.
- Se recomienda contar con autorización explícita, previa e informada de los Titulares para el Tratamiento de sus datos sensibles de los menores de edad.
- Se recomienda contar con la aplicabilidad de este criterio donde se evidencie que se *"obtienen nuevas autorizaciones de los Titulares, cuando la organización realiza cambios sustanciales en las políticas de Tratamiento de información personal"*.
- Se recomienda realizar inventario de la información que se está transfiriendo fuera del país y gestionar su cumplimiento y aplicabilidad (ej.: los servicios que se encuentran en la nube), donde se evidencie cumplimiento de: *"se han implementado medidas apropiadas y efectivas para garantizar el adecuado Tratamiento de los datos personales que se transfieren a otro país y para otorgar seguridad a los registros."*

6. RECOMENDACIONES

6.2. SEGUNDA PERSPECTIVA: VERIFICACIÓN DE AVANCE DE IMPLEMENTACIÓN DE LA LEY 1581 DE 2012 – SIC

- Se recomienda documentar el proceso de generación de reportes como parte del Programa Integral de Gestión de Datos Personales.
- Se recomienda formalizar la estructura para la generación de reportes en la que se establezca: la persona que genera, el tipo de reporte y se asignen responsabilidades claras ante una queja de los Titulares y los Entes de Control.
- Se recomienda contar con procedimientos administrativos consistentes con las políticas generales de protección de datos personales y con las disposiciones legales vigentes. Así como también procedimientos donde se establezcan reglas para la conservación y eliminación de información personal, y procedimientos debidamente documentados e implementados donde se establezcan reglas para la inclusión en todos los medios contractuales de la entidad de una cláusula de confidencialidad.

6.3. TERCERA PERSPECTIVA: REVISIÓN CONTROLES SEGURIDAD DE DATOS - PROTECCIÓN DE DATOS PERSONALES

- Se recomienda contar con procedimientos para garantizar que todos los datos personales recogidos sean exactos, completos y actualizados, y se informe adecuadamente al Titular lo estipulado en el formulario de la SIC: "*El usuario se compromete a suministrar información correcta y veraz. Así mismo, se compromete a que no escalará a través de los formularios web y aplicativos desarrollados por la entidad información maliciosa o que pueda generar afectación a los sistemas de LA ENTIDAD."*.
- Se recomienda para el criterio "*Se asegura por parte de la Entidad que los datos personales no se conservan por más tiempo que el necesario para la finalidad para la que se recogió, obtuvo o trató la información"*, establecer con gestión documental los tiempos de conservación de los datos personales y establecer los mecanismos para destruirlos de manera eficiente.

6.4. RECOMENDACIONES GENERALES:

1. Elaborar, socializar e implementar en la UAESP un plan integral de protección de datos personales.
2. Ajustar el manual de protección de datos personales con lineamientos definidos para garantizar la seguridad de los datos personales en la entidad.
3. Definir un repositorio institucional para que los procesos NO continúen utilizando los repositorios personales, incurriendo en el riesgo de pérdida de información sensible, como es el caso de la información que reposa en la OAP y que corresponde a datos personales de consultas ciudadanas.
4. Elaborar los Mapas de Riesgos Institucionales de seguridad de los datos personales.
5. La OCI recomienda a la OTIC y al Oficial de datos Personales, revisar con la OAP la pertinencia de incluir en la política de gestión de riesgos la administración de riesgos en el tratamiento de datos personales.

6. RECOMENDACIONES

6. Establecer un procedimiento documentado para la formalización, identificación, actualización y reporte de bases de datos con información personal al Registro Nacional de Bases de Datos de la SIC.
7. Incluir en las condiciones generales de los contratos de prestación de servicios las obligaciones que deben cumplir los contratistas respecto al tratamiento de datos personales, como garantizar la seguridad y confidencialidad de los datos personales, no usarlos para fines no autorizados, no apropiarse de ellos y reintegrar a la entidad todos los datos que trataron durante la prestación de sus servicios.
8. Llevar a cabo las acciones necesarias para poner en práctica las políticas y lineamientos establecidos en los que se incluyan herramientas para la implementación, comunicación y programas de educación en materia de protección de datos personales.

APROBACIÓN:

Sandra Beatriz Alvarado Salcedo FIRMA Firmado digitalmente por Sandra Beatriz Alvarado Salcedo Fecha: 2023.04.26 16:47:39 -05'00' **Sandra Beatriz Alvarado Salcedo** **Jefe(a) de Oficina de Control Interno**	**Ligia Marlen Velandia León – Osbaldo Cortes Lozano** **Auditor(es) Interno(s)**

FECHA[4]: **25/04/2023**

DD – MMMM – AAAA

(4) Fecha en la cual el(la) jefe(a) de Oficina y los Auditores Internos designados APROBARON el Informe de Auditoría.