MEMORANDO

Al contestar, por favor cite el radicado:
No.:**20241100036183**

Bogotá D.C., 29 de Abril de 2024

PARA: **MARY LILIANA RODRÍGUEZ CÉSPEDES**
Subdirección de Asuntos Legales

MIGUEL ANTONIO JIMÉNEZ PORTELA
Subdirección Administrativa y Financiera

ALBEIRO ANTONIO PORRAS ALVAREZ
Subdirección de Recolección Barrido y Limpieza

YIRA BOLAÑOS ENRÍQUEZ
Subdirección de Servicios Funerarios y Alumbrado Público (E)

MARILEN ARIADNA RODRÍGUEZ VERDUGO
Subdirección de Aprovechamiento

VICTOR JULIO MORENO MONSALVE
Subdirección de Disposición Final

MARÍA JOSE BARRERA RANGEL
Oficina Asesora de planeación

CESAR MAURICIO BELTRAN LOPEZ
Oficina de Tecnologías de la Información y las 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, para el periodo abril 2023 a marzo 2024.

Respetado equipo directivo y gestores:

En cumplimiento del Plan Anual de Auditorías con vigencia 2024, la Oficina de Control Interno - OCI atentamente remite el informe final de la auditoria *"Evaluación del nivel de cumplimiento de la Ley 1581*

Bogotá D.C., 29 de Abril de 2024

de 2012 de protección de datos personales de la Unidad Administrativa Especial de Servicios públicos - UAESP" para el periodo comprendido entre marzo del 2023 – abril 2024.

La auditoría se realizó con base en la Guía de la Superintendencia de Industria y Comercio (SIC). Donde se evidenció un avance general del 87,9% 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 78%. En el informe anexo, podrán detallar y analizar junto con sus equipos de trabajo las evaluaciones realizadas.

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 Oficina de Tecnologías de la Información y las Comunicaciones - OTIC y la Subdirección Administrativa y Financiera – Talento Humano SAF-TH formulen los Planes 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 de los responsables de los procesos decidir sobre el tratamiento pertinente, no obstante, se alienta a los responsables en el marco de la mejora continua evaluar la suscripción de acciones en el PMI.

Para la suscripción acciones en el PMI, se solicita que estas sean enviadas a la OCI dentro de un 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: 2024.04.29 15:51:35 -05'00'

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

Anexos: Informe de Auditoría Interna y Anexos 1 y 2.
Elaboró: Ligia Marlén Velandia León. PE-222-24-OCI – Osbaldo cortes Lozano P.E (e)-222-24-OCI

CONTENIDO

Lista de Tablas

1. INFORMACIÓN GENERAL DE LA AUDITORIA

Tabla 1- Información de la auditoria

ENFOQUE DE LA AUDITORIA INTERNA	Gestión y Resultados - Legal
INFORME	Verificar el cumplimiento de la normatividad vigente relacionada con la Ley 1581 de 2012 de protección de datos personales por parte de los procesos auditados.
PROCESO, PROCEDIMIENTO	• Oficina de tecnologías de la información y las comunicaciones - OTIC • Subdirección administrativa y financiera, Atención al ciudadano y Talento humano SAF/AC/TH • Oficina asesora de planeación - OAP • Subdirección de aprovechamiento - SAPROV • Subdirección Recolección barrido y limpieza - SRBL • Subdirección de Disposición final - SDF • Subdirección de servicios funerarios y alumbrado público – SF/AP • Subdirección de asuntos legales - SAL
RESPONSABLE O AUDITADOS	Equipos de Trabajo: OTIC, SAF/AC/TH, OAP, SAPROV, RBL, SDF, SF/AP y SAL
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 frente a la Protección de Datos Personales - Ley 1581 de 2012 en los procesos auditados, correspondiente al periodo de abril 2023 a marzo 2024.
PERIODO DE EJECUCIÓN	01 de marzo al 30 de abril del 2024.
EQUIPO AUDITOR	Ligia Marlén Velandia León (LMVL) y Osbaldo Cortés Lozano (OCL)

DOCUMENTACIÓN ANALIZADA	• Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales (PDP). • Decreto 1727 de 2009: Información titulares. • Decreto 2952 de 2010 Reglamentación 1266 de 2012: Disposiciones 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. • Política de PDP – UAESP. • Procedimientos MIPG. • Perspectiva con base en la guía de la Superintendencia de Industria y Comercio - SIC • Verificación de controles de seguridad del instrumento de la Alta Consejería TIC del Distrito

2. DESARROLLO DE LA AUDITORIA

La Auditoría de Cumplimiento de la Ley 1581 de 2012 sobre Protección de Datos Personales - PDP, llevada a cabo en la Unidad Administrativa Especial de Servicios Públicos - UAESP durante los meses de marzo y abril, representa una actividad de control que permite a la entidad garantizar el adecuado tratamiento de los datos personales. Esta auditoría inició con la revisión a las recomendaciones formuladas en el informe de auditoría del año 2023, en el cual se identificaron oportunidades de mejora en la gestión de datos personales. Posteriormente se continuó con la revisión del cumplimiento frente al desarrollo de las dos perspectivas: Perspectiva con base en la guía de la SIC y verificación de controles de seguridad del instrumento de la Alta Consejería TIC del Distrito. Finalmente, la OCI emitió las respectivas conclusiones y recomendaciones.

La Ley 1581 de 2012 establece los principios y directrices que regulan el tratamiento de datos personales en Colombia, con el objetivo de proteger los derechos fundamentales de las personas respecto a la privacidad y el control sobre sus datos personales. Dentro de los aspectos abordados en esta auditoría se encuentran el tratamiento de datos de menores de edad, la obtención de autorización para el tratamiento de datos personales, así como la gestión de riesgos e incidentes relacionados con la seguridad de la información en lo que respecta a PDP, entre otros.

Es fundamental destacar que el tratamiento de datos personales es una responsabilidad compartida entre la UAESP y todos sus colaboradores, quienes debemos cumplir con los lineamientos de seguridad y confidencialidad en el manejo de la información. Esta auditoría tuvo como objetivo evaluar el grado de cumplimiento de la UAESP en relación con las disposiciones establecidas en la Ley 1581, así como identificar oportunidades de mejora que permitan fortalecer las mejores prácticas para la protección de datos en la entidad.

A continuación, se detallan los pasos seguidos en este proceso, teniendo en cuenta los riesgos asociados:

2.1 Planificación

La Oficina de Control Interno – OCI en cumplimiento del Plan Anual de Auditorías de la vigencia 2024, planificó la ejecución de la auditoria con radicado No. :20241100018563 – del 01 de marzo de 2024.

Para el diagnóstico de este ejercicio de auditoria el equipo auditor tuvo en cuenta dos perspectivas a evaluar cómo fueron: 1. Perspectiva con base en la guía de la SIC. 2. Perspectiva con base en la verificación de controles de seguridad del instrumento de la Alta Consejería TIC del Distrito.

Durante esta fase se desarrollaron las siguientes actividades:

- Establecer los objetivos y alcance de la auditoría, definiendo el marco normativo y los criterios de evaluación
- Preparación de los papeles de trabajo y los formularios para que los procesos diligenciaran con las evidencias correspondientes.

2.2 Seguimiento a las recomendaciones auditoría 2023

Con base en el informe de auditoría de 2023 con radicado 20231100046783 de fecha 26 de abril de 2023 se formularon recomendaciones y una observación, de los cuales se verifica seguimiento en el marco de esta auditoría así:

Tabla 2 *Seguimiento a la Observación sobre diagnóstico y avance de las perspectivas del cumplimiento de la SIC y Controles de PDP.*

Observación - 2023	Acciones tomadas por el proceso OTIC	Verificación OCI
De acuerdo con 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.	Se elaboró, fue aprobado por el CIGD y se encuentra publicado en el Sistema Integrado de Gestión	La OCI evidenció que la UAESP ya cuenta con el Programa Integral de Gestión de Datos Personales, el cual se encuentra en el siguiente: Enlace

De lo anterior, se concluye que el proceso sí emprendió acciones para subsanar la observación y mitigar los riesgos, al realizar y documentar el Programa Integral de Gestión de Datos Personales; evidenciando así un compromiso activo por parte de la entidad en garantizar la protección y gestión

adecuada de la información personal. Este programa demuestra la adopción de medidas estructuradas y sistemáticas para asegurar el cumplimiento de la normatividad vigente en materia de protección de datos, fortaleciendo así la confianza y transparencia en el manejo de la información por parte de la UAESP.

En la siguiente tabla, se ofrece un análisis detallado de las recomendaciones asociadas a las perspectivas evaluadas. En él, se incluyen las estrategias y acciones específicas que el proceso implementó, así como el seguimiento realizado por la OCI para asegurar su efectiva ejecución.

***Tabla** 3. Seguimiento a Recomendaciones sobre diagnóstico y avance de las perspectivas del cumplimiento de la SIC y Controles de PDP.*

No.	Recomendaciones formuladas sobre evaluación de las perspectivas para el año 2023	Oportunidad de mejora que realizó el proceso OTIC - 2023	Seguimiento OCI
1	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.	Se cuenta consentimiento previo en los formularios Web mediante una lista de comprobación que están disponibles para la ciudadanía cuando se solicita datos personales y en formatos físicos las listas de asistencia con la firma de autorización, a su vez se solicita que la información sea exacta comprobable y comprensible	Con base en las evidencias allegadas por el proceso se corrobora su cumplimiento, toda vez que el proceso emprendió oportunidades de mejora duranta la vigencia 2023.
2	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 crea un repositorio institucional mediante SharePoint para cada proceso con el fin de almacenar datos personales y sean compartidos a las personas del proceso que lo requieran sin que esta información quede atada a una cuenta personal. -Se ajusto los avisos de privacidad de acuerdo con recomendación dadas.	De acuerdo con las evidencias aportadas por el proceso, la OCI evidenció un avance inicial para esta recomendación, ese decir, el proceso realizó acciones teniendo en cuenta la recomendación dada.
3	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	-Se cuenta con un documento de Reserva y Confidencialidad de la Información donde el contratista se compromete a guardar reserva de la información después de finalizar el respectivo contrato. -En el Aplicativo ORFEO se configura el nivel de seguridad y privacidad en la creación y visualización de radicados internos con los parámetros de Publico, Confidencial y Privado para la reserva y confidencialidad de la información.	Una vez validadas las evidencias se observó que el proceso realizó acciones que aportaron al cumplimiento de la recomendación.

No.	Recomendaciones formuladas sobre evaluación de las perspectivas para el año 2023	Oportunidad de mejora que realizó el proceso OTIC - 2023	Seguimiento OCI
	sin autorización u otra área la puedan ver	-Se realiza el cifrado de la firma en el aplicativo SIRA	
4	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 cuenta con la Carta de Compromiso sobre actividades de bienestar institucional donde se solicita autorización a padres de familia para realizar actividades a los menores de edad. -Se cuenta con la encuesta sobre la Calidad de la Información Estadística y Necesidades de Información donde se solicita información sensible.	Se evidenció la carta de compromiso de bienestar institucional, donde se expresa autorización para tratamiento de datos de menores de edad, es decir se emprendieron acciones para mitigar este riesgo y se dio cumplimiento a la recomendación.
5	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".	No se han realizado cambios sustanciales a la Política Tratamiento Datos Personales de la versión anterior a la actual.	En la Política de Tratamiento de Datos Personales, no se han realizado cambios sustanciales que ameriten cambios.
6	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.	Se cuenta con clausulas para la privacidad y protección de la información que se encuentra custodiada por un tercero en la nube en este caso con Microsoft Azure se tiene la Declaración de privacidad de Microsoft, las especificaciones en la Minuta del Acuerdo Marco de Servicios de Nube donde se definen las especificaciones y obligaciones del Proveedor.	Se evidenció documento de Declaración de Privacidad de Microsoft, para el tema de Datos Personales, es decir se cuenta con cláusulas que dan fe de su cumplimiento en especial con los contratos de terceros para servicios en la Nube como Microsoft.
7	Se recomienda documentar el proceso de generación de reportes como parte del Programa Integral de Gestión de Datos Personales.	Se hace relación en el Programa Integral Datos Personales se especifica en el numeral 9.	En el numeral 9 del Programa Integral de Datos Personales, se hace referencia a la generación de reportes.
8	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 hace relación parcial en el Programa Integral Datos Personales se especifica en los siguientes numerales:9. Presentación de Informes,13. Evaluación y Revisión. Para las responsabilidades claras ante una queja de los Titulares se especifica en el	Se evidenciaron acciones que dieron fe de su cumplimiento.

No.	Recomendaciones formuladas sobre evaluación de las perspectivas para el año 2023	Oportunidad de mejora que realizó el proceso OTIC - 2023	Seguimiento OCI
		documento GTI-MN-05 V2 Tratamiento de Datos Personales en el numeral: 11.2 Lineamientos para los reclamos	
9	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.	-Borrador Procedimiento Solicitud Autorización del Titular. -Borrador Procedimiento Consultas y Reclamos Datos personales -Formato Consultas y Reclamos Datos Personales -Borrador Procedimiento Reporte Base de Datos Personales en el RNBD.	De acuerdo, con las evidencias presentadas por el proceso, se observó un progreso importante en la elaboración de procedimientos, los cuales se encuentran actualmente en etapa de borrador.
10	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 cuenta con avisos de privacidad donde se solicita al usuario brindar la información de manera exacta, real comprensible, comprobable. También se configuran en los sistemas de información la parametrización de campos donde se valida el tipo de dato dando mensajes al usuario si se comprueba alguna inconsistencia.	Tras validar las evidencias, se constató que el proceso llevó a cabo acciones que contribuyeron al cumplimiento de la recomendación.
11	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.	-Se estipula en la Política Tratamiento Datos Personales V4 en el numeral 20 la conservación de las bases de datos personales. -Para el borrado seguro de la información se cuenta con el instructivo de soporte Técnico.	Al revisar las evidencias aportadas por el proceso, se confirmó que se adoptaron acciones para llevar a cabo la implementación de la recomendación dada por la OCI.

En el presente análisis, también se abordaron las recomendaciones generales que se sugirieron en la auditoría anterior, esto con el propósito de evaluar su adopción y la efectividad de las acciones tomadas en respuesta a dichas sugerencias de la siguiente manera:

Tabla *4. Seguimiento a Recomendaciones Generales*

No.	Recomendaciones formuladas sobre evaluación de las perspectivas para el año 2023	Oportunidad de mejora que realizó el proceso OTIC - 2023	Seguimiento OCI
1	Elaborar, socializar e implementar en la UAESP un plan integral de protección de datos personales.	-Se elabora el documento Programa Integral Datos Personales -Se envía pieza comunicativa sobre el Programa Integral Datos Personales.	Al verificar las evidencias presentadas por el proceso, se constató el desarrollo de acciones que llevaron a un cumplimiento efectivo en la implementación de la recomendación proporcionada. El programa se encuentra publicado en la página de la entidad.
2	Ajustar el manual de protección de datos personales con lineamientos definidos para garantizar la seguridad de los datos personales en la entidad.	-Se realiza actualización del documento GTI-MN-05 V2 Tratamiento de Datos Personales.	De acuerdo con las evidencias analizada, se pudo constatar que el proceso realizó actualización del manual con fecha de enero de 2024.
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.	Se crea un repositorio institucional mediante SharePoint para cada proceso con el fin de almacenar datos personales y sean compartidos a las personas del proceso que lo requieran sin que esta información quede atada a una cuenta personal.	Se observó que la OTIC emprendió medidas iniciales para cumplir con la recomendación formulada.
4	Elaborar los Mapas de Riesgos Institucionales de seguridad de los datos personales.	Se contemplan riesgos de Datos Personales en los Mapa de Riesgos de los Procesos de Atención al Ciudadano y OTIC.	Se observó la existencia de mapas de riesgos de la OTIC, y servicio al ciudadano.
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	En la política Gestión Riesgos se contempla la privacidad de la información lo cual se relaciona a Datos Personales, no obstante, la OTIC se encuentra realizando la propuesta de ajuste a la política para que se exprese de manera explícita.	La OCI evidenció avances iniciales con el borrador de la política de administración del riesgo.

No.	Recomendaciones formuladas sobre evaluación de las perspectivas para el año 2023	Oportunidad de mejora que realizó el proceso OTIC - 2023	Seguimiento OCI
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.	-En elaboración procedimiento Borrador Reporte Base de Datos Personales en el RNBD.	La OCI, evidenció la elaboración del borrador del procedimiento Reporte Base de Datos Personales en el Registro Nacional de Bases de Datos.
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.	-Se incluye en condiciones generales de los contratos por prestación de servicios numerales 26, 27, 28 lo relacionado con seguridad de la información y datos personales -Se cuenta con documento Reserva y Confidencialidad de la Información. -Se contempla en la Propuesta Contratista lo relacionado con la Protección de Datos Personales.	De acuerdo, con las evidencias proporcionadas por el proceso, se verificó un progreso significativo en la inclusión de cláusulas de Protección de Datos Personales en el contrato de prestación de servicios. Esto indica que se han tomado medidas para cumplir con la recomendación sugerida.
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.	Se han realizado sensibilizaciones y envío de piezas comunicativas sobre Protección de Datos Personales en la Entidad de acuerdo con el Plan de Capacitaciones de Seguridad de la Información y el Plan Institucional de Capacitaciones.	Se observó la implementación de acciones orientadas a sensibilizar al personal al interior de la UAESP sobre la importancia de la protección de datos personales, en línea con el plan anual de capacitación.

La OCI, verificó que se cumplieron las recomendaciones emitidas en el marco de la auditoría del 2023. Este cumplimiento refleja el compromiso por parte del proceso para abordar y solucionar las oportunidades de mejora identificadas.

2.3 Primera Perspectiva con base en la guía de la Superintendencia de Industria y Comercio SIC.

En esta fase, el equipo auditor envió por correo electrónico el formulario "Perspectiva con base en la guía de la Superintendencia de Industria y Comercio - SIC", adaptado a las necesidades específicas de la entidad. Además, se proporcionó acceso al repositorio para el cargue de las evidencias para cada uno de los 9 procesos seleccionados. Es preciso aclarar que la Subdirección de Servicios Funerarios y Alumbrado Público diligenció un solo formulario para los dos procesos.

Cada una de las preguntas del cuestionario se evaluó mediante una calificación cuantitativa indicada en la siguiente tabla, teniendo en cuenta que para; el incumplimiento (0) y cumplimiento parcial o total (0.5 y 1) respectivamente. Para los casos que no aplica el criterio de evaluación fue N/A por no tener el proceso responsabilidad en el respectivo criterio, como se observa a continuación:

***Tabla 5** - Criterios de evaluación*

#	Calificación	Descripción
1	1	Cumple
2	0,5	Parcial
3	0	No cumple
4	N/A	No Aplica

En tabla No. 6, se detallan los resultados generales del cuestionario de diagnóstico para el cumplimiento de la ley 1581 de 2012 de la SIC, el cual está compuesto por 15 categorías y 90 preguntas las cuales buscan establecer el nivel de avance sobre la implementación de la Ley 1581 de 2012.

Tabla 6 *- Diagnóstico para el Cumplimiento de la Ley 1581 - Primera Perspectiva con Base en la Guía de la SIC.*

	OAP		RBL		SAPROV		SDF		SFAP		TH		OTIC		SAL		SAF - SC	
Criterio	**Proceso**	**OCI**	**Proceso**	**OCI**	**Proceso**	**OCI**	**Proceso**	**OCI**	**Proceso**	**OCI**	**Proceso**	**OCI**	**Proceso**	**OCI**	**Proceso**	**OCI**	**Proceso**	**OCI**
1. Principios para el tratamiento de datos personales	10,0	8,8	N/A	N/A	10,0	8,0	10,0	8,8	8,3	8,3	10,0	9,0	10,0	9,3	10	10	10	10
2. Tratamiento de datos sensibles y de menores de edad	10,0	10,0	N/A	N/A	N/A	N/A	10,0	10,0	N/A	N/A	10,0	10,0	10,0	10,0	10	10	N/A	N/A
3. Derechos de los titulares de información.	10,0	10,0	N/A	N/A	10,0	7,5	10,0	10,0	5,0	5,0	8,3	8,3	10,0	10,0	10	10	10	10
4. Autorización para el tratamiento de datos personales	10,0	8,8	N/A	N/A	10,0	8,3	10,0	10,0	6,7	6,7	8,8	7,5	10,0	10,0	10	10	10,0	10,0
5. Información mínima a los titulares	10,0	9,0	N/A	N/A	5,0	5,0	10,0	4,0	7,0	7,0	10,0	6,0	10,0	9,0	10	6,25	8,8	6,3
6. Suministro de la información personal	N/A	N/A	N/A	N/A	N/A	N/A	10,0	5,0	10,0	5,0	10,0	7,5	10,0	10,0	10	10	10,0	10,0
7. Atención de consultas y reclamos de los titulares	10,0	10,0	10,0	10,0	10,0	10,0	N/A	N/A	5,0	5,0	10,0	10,0	10,0	10,0	10	10	10,0	9,0
8. Política de tratamiento de datos personales.	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	10,0	10,0	N/A	N/A	10,0	10,0
9. Aviso de privacidad	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	10,0	10,0	N/A	N/A	10,0	10,0

	OAP		RBL		SAPROV		SDF		SFAP		TH		OTIC		SAL		SAF - SC	
Criterio	**Proceso**	**OCI**	**Proceso**	**OCI**	**Proceso**	**OCI**	**Proceso**	**OCI**	**Proceso**	**OCI**	**Proceso**	**OCI**	**Proceso**	**OCI**	**Proceso**	**OCI**	**Proceso**	**OCI**
10. Reporte de violaciones a los códigos de seguridad	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	10,0	10,0	N/A	N/A	N/A	N/A
11. Gestión de encargados del tratamiento Encargado del Tratamiento	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	10,0	8,3	8,1	5,0	7,8	4,4	N/A	N/A	N/A	N/a
12. Transferencia y transmisión internacional de datos personales.	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	10,0	10,0	N/A	N/A	N/A	N/A
13. Responsabilidad demostrada.	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	5,8	5,8	10	10	10,0	10,0
14. Registro nacional de bases de datos.	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	10,0	10,0	N/A	N/A	N/A	N/A
15. Incidentes	10,0	10,0	10,0	10,0	10,0	10,0	10,0	10,0	10,0	10,0	10,0	8,3	10,0	10,0	10	10	10,0	10,0
Calificación	**10,0**	**9,5**	**10,0**	**10,0**	**9,2**	**8,1**	**10,0**	**8,3**	**7,8**	**6,9**	**9,5**	**8,0**	**9,6**	**9,2**	**10,0**	**9,6**	**9,9**	**9,5**

En la tabla No. 7, el equipo auditor consolidó los datos generados por los procesos, donde se presenta un valor de ejecución porcentual para la calificación del proceso y la de la OCI, junto con la diferencia entre las dos evaluaciones, como se observa a continuación:

***Tabla 7** - Resumen Diagnóstico para el Cumplimiento de la Ley 1581 - Primera Perspectiva con Base en la Guía de la SIC.*

#	Proceso	Calificación proceso	Calificación OCI	Diferencia
1	OAP	10,0	9,5	0,5
2	RBL	10,0	10,0	0,0
3	SAPROV	9,2	8,1	1,0
4	SDF	10,0	8,3	1,8
5	SFAP	7,8	6,9	0,8
6	SAF - TH	9,5	8,0	1,5
7	OTIC	9,6	9,2	0,3
8	SAL	10,0	9,6	0,4
9	SAF - SC	9,9	9,5	0,4
	Consolidado	**86**	**79**	**7**
	Porcentaje	**95.37%**	**87.90%**	**7.47%**

Como resultado de la evaluación, la OCI observó un porcentaje elevado en la implementación y apropiación de la política de tratamiento de datos personales presentando un consolidado del 95.3 % vs una evaluación de la OCI que representa el 87,9% de evaluación con una diferencia del 7,4%. A continuación, se presenta un análisis general por proceso. Para consultar el detalle del análisis para cada uno de los procesos la OCI presenta el Anexo 1 Consolidado Perspectivas 1 y 2.

SDF: presentó una diferencia de 1.8 puntos debido al cumplimiento parcial de lo solicitado en los numerales 5. Información mínima a los titulares y 6. Suministro de la información personal que presentan cumplimiento parcial.

SAF-TH: Presentó una diferencia de 1.5 puntos, esto debido a no cumplir con los dos criterios de los numerales: No. 5 Información mínima de los titulares, No. 6 Suministro de información personal, tanto que las evidencias presentadas no corresponden a lo solicitado en el punto de estudio, y No 11. Gestión de encargados del tratamiento, el proceso no tiene establecido contratos con terceros que recolectan información personal en las reuniones a cargo de la subdirección.

SAPROV: Presentó diferencia de 1 punto, motivada por cumplimiento parcial en los numerales: No. 1 Principios para el tratamiento de datos personales en los apartados 1.1 y 1.4, No. 3 Derechos de los

titulares de información, apartado 3.3 y No. 4 Autorización para el tratamiento de datos personales apartado 4.1.

SFAP: Presentó una baja ejecución debido cumplimiento parcial de los numerales: No. 1. Principios para el tratamiento de datos personales, No. 4. Autorización para el tratamiento de datos personales, No. 5. Información mínima a los titulares, No. 7. Atención de consultas y reclamos de los titulares y al no cumplimiento del numeral No. 3. Derechos de los titulares de información aparatado 3.3.

OAP: Se presentó una diferencia de 0,5 punto debido al cumplimiento parcial de los numerales: No. 1. Principios para el tratamiento de datos personales, apartado 1.7, No. 4. Autorización para el tratamiento de datos personales, apartado 4.1 y No. 5. Información mínima a los titulares, apartado 5.4

SAL: La diferencia de 0,4 punto se presentó en el cumplimiento parcial del numeral No. 5. Información mínima a los titulares, apartados 5.3, 5.4 y 5.5.

SAF-SC: La diferencia de 0,4 punto se presentó por no cumplir con lo señalado en el numeral No. 5. Información mínima a los titulares, apartado 5.4

OTIC: La diferencia de 0,3% punto, se presentó por el cumplimiento parcial de los numerales: No. 1. Principios para el tratamiento de datos personales – apartado 1.6, No. 5 5. Información mínima a los titulares – apartado 5.5 y No. 11 Gestión de encargados del tratamiento.

Las recomendaciones que se desprenden del presente análisis son desarrolladas en el numeral 7 del presente documento.

2.4 Segunda Perspectiva Verificación de controles de seguridad del instrumento de la Alta Consejería TIC del Distrito

Para esta fase, el equipo auditor envió por correo electrónico a la OTIC acceso al repositorio de evidencias y el formulario "Verificación de controles de seguridad del instrumento de la Alta Consejería TIC del Distrito", el cual contiene 33 controles organizados en 9 categorías.

Cada una de las preguntas del cuestionario se evaluó mediante una calificación cuantitativa indicada en la siguiente tabla, teniendo en cuenta que para; el incumplimiento (0) y cumplimiento parcial o total (0.5 y 1) respectivamente. Para los casos que no aplica el criterio de evaluación fue N/A. A continuación, se presenta el consolidado basado en la autoevaluación del proceso y la verificación de la OCI:

Tabla 8 *- Revisión controles seguridad de datos - Segunda Perspectiva con base en la Guía de la Alta Consejería TIC*

Criterios de evaluación	Evaluación 2023			Evaluación 2024		
	Proceso	OCI	Diferencia	Proceso	OCI	Diferencia
1. Sección Gestión de riesgos en seguridad de los datos personales	10	8,8	1,2	10	8.75	1,25
2. Gestión de incidentes o incumplimientos en seguridad de los datos personales	8,3	8,3	0	10	10	0,0
3. Identificación de controles implementados de seguridad en la captura de la información de datos personales.	7,5	7,5	0	8,75	7,5	1,3
4. Identificación de las Bases de Datos que tiene datos personales, según el alcance establecido a nivel de procesos y sistemas de información.	10	8,3	1,7	10	8,3	1,7
5. Revisión del estado actual de los controles para el acceso a las Bases de datos con información personales	8	7	1	8	8	0,0
6. Revisión del estado actual de controles de seguridad implementados en el almacenamiento de los datos personales (Ejemplo: Cifrado, acceso, entre otros).	5	4,2	0,8	8,3	5,8	2,5
7. Revisión del estado actual de controles técnicos cuando se comparte la información de datos personales con terceras partes.	8,3	5	3,3	10,0	6,7	3,3
8. Revisión del estado actual de controles técnicos en la eliminación de datos personales o cuando pasan a ser históricos.	8,3	6,7	1,6	8,3	6,7	1,7
9. Revisión de controles de sensibilización, capacitación o formación a los servidores públicos en lo relacionado con protección de datos personales	10	10	0	10	10	0,0
	80%	**70%**	**10%**	**93%**	**78%**	**13%**

Con base en los resultados de la tabla No. 8, la OCI evidenció un incremento sobre la autoevaluación de la OTIC del 13 %, al pasar del 80% en el año 2023 al 93% para el 2024, mientras que tomando como base la evaluación de la OCI el incremento es del 8% pasando del 70% al 78%.

El detalle para cada uno de los criterios evaluados, se encuentran en el Anexo No. 1, pestaña (PDP - OTIC). A continuación, se presenta el resumen para cada uno de los ítems evaluados:

Tabla 9 - *Evaluación OCI Segundo Criterio*

Criterios de evaluación	Dif.	Evaluación OCI
1. Sección Gestión de riesgos en seguridad de los datos personales	1,3	1.1 ¿Se cuenta con metodología de gestión de riesgos para protección de datos personales? Con base en la revisión de las evidencias, la OCI verifica el cumplimiento parcial de lo solicitado en el punto, toda vez que el documento entregado como evidencia se encuentra en borrador.
2. Gestión de incidentes o incumplimientos en seguridad de los datos personales	0,0	Presenta una ejecución del 100%.
3. Identificación de controles implementados de seguridad en la captura de la información de datos personales.	1,3	3.1 ¿Se cuenta con el aviso de aceptación de tratamiento de datos personales? El equipo auditor evidenció formularios de captura de datos personales realizados por terceros que no cumplen con lo solicitado en el punto. 3.4 ¿Cuenta con procedimientos para garantizar que todos los datos personales recogidos son exactos, completos y actualizados? De acuerdo con la revisión realizada por la OCI, no se puede evidenciar que la entidad garanticé que todos los datos personales recogidos son exactos, completos y actualizados.
4. Identificación de las Bases de Datos que tiene datos personales, según el alcance establecido a nivel de procesos y sistemas de información.	1,7	4.1 ¿Se tienen identificada las Bases de datos con información personal en los sistemas de información de los procesos? La OCI no evidenció que el alcance del inventario de bases de datos incluyera los operadores y empresas externas que pueden capturar información personal.
5. Revisión del estado actual de los controles para el acceso a las Bases de datos con información personales	0,0	5.4. ¿Se realiza revisión periódica de los privilegios de accesos otorgados a la información personal? La OCI, no evidenció la realización periódica de los privilegios de accesos otorgados a las bases de datos que contienen información personal.
6. Revisión del estado actual de controles de seguridad implementados en el almacenamiento de los datos personales (Ejemplo: Cifrado, acceso, entre otros).	2,5	6.1. ¿Se tiene cifrada la Base de datos para proteger la información de datos personales? Se evidenció acceso a información sensible en ORFEO, la cual debería estar protegida contra acceso no autorizado. Por otra parte, no se evidenció mecanismos para proteger los datos almacenadas en OneDrive o en los equipos de los funcionarios de la entidad. 6.2. ¿Se tiene anonimización sobre la información personal almacenada en las bases de datos? La OCI evidenció documentos que tratan el tema de anonimización de datos personales, sin embargo, no fue posible verificar el cumplimiento en la totalidad de bases de datos. 6.3.¿Se tiene activación de registros de auditoría de las acciones realizadas por los usuarios en las Bases de datos con información personal? El proceso no presentó evidencias sobre auditoría para la totalidad de bases de datos ni de un sistema unificado que pueda verificar las acciones realizadas por usuarios. 6.5. Cuando se hace un campo en los datos personales de la BD, ¿Se replica o actualiza el cambio al resto de BD's? La OCI no puede verificar el cumplimiento de los solicitado en las bases

Criterios de evaluación	Dif.	Evaluación OCI
		de datos en Excel, que están replicadas en diferentes repositorios o equipos.
7. Revisión del estado actual de controles técnicos cuando se comparte la información de datos personales con terceras partes.	3,3	7.2. ¿Se tiene establecido una política o control documental para establecer acuerdos de confidencialidad o de no divulgación cuando se comparte información de datos personales con terceras partes? La auditoría evidenció que terceros capturan datos personales sin el debido cumplimiento de la ley 1581 de 2021 y la Política de Datos Personales. 7.3. ¿Se cuenta con mecanismos de control para cifrar la información punto a punto durante la transferencia? La OCI evidenció el cumplimiento parcial toda vez que tanto la uaesp.gov.co, gdocumental.uaesp.gov.co, intranet.uaesp.gov.co/wp-login.php, tienen habilitados el puerto 80 (http) protocolo que no cifra la información punto a punto.
8. Revisión del estado actual de controles técnicos en la eliminación de datos personales o cuando pasan a ser históricos.	1,7	8.3. ¿Se encuentra documentado en el aviso de privacidad la vigencia de los datos personales? La OCI evidenció que el aviso de privacidad no incluye la vigencia de los datos personales.
9. Revisión de controles de sensibilización, capacitación o formación a los servidores públicos en lo relacionado con protección de datos personales	0,0	Presenta una ejecución del 100%.

Las recomendaciones que se desprenden del análisis son desarrolladas en el numeral 7 del presente documento.

2.5 Análisis riesgos

En el marco de la auditoría de protección de datos personales, se llevó a cabo una evaluación detallada de los riesgos asociados con la gestión y tratamiento de la información personal en la entidad. Basándonos en el análisis efectuado, se identificaron los siguientes riesgos significativos que podrían afectar el cumplimiento del criterio ***"****Conservar información personal veraz, completa, exacta, actualizada, comprobable y comprensible*":

- Posible incumplimiento de la normativa vigente en protección de datos personales.
- Uso indebido de la información personal por parte de personal no autorizado.
- Riesgo de acceso y manipulación no autorizada de la información personal.
- Vulnerabilidades por falta de un el sistema de almacenamiento centralizado, comprometiendo la integridad y confidencialidad de los datos.

Los riesgos listados resaltan la importancia de implementar medidas de control y seguridad robustas para garantizar el manejo adecuado y seguro de la información personal, así como el cumplimiento de las regulaciones y estándares en materia de protección de datos personales.

Lo anterior podría tener repercusiones adversas en la entidad en caso de que alguno de estos riesgos se materialice, conllevando posibles sanciones financieras o daños a la reputación, entre otros. Por ello, es crucial establecer un mapa de riesgos específico para la Protección de Datos Personales -PDP, que incluya la implementación de controles adecuados, así como un sistema de monitoreo y seguimiento efectivo.

Además, es esencial continuar fortaleciendo las políticas y procedimientos existentes, y reforzar las actividades de sensibilización, capacitación y acompañamiento dirigidas tanto a los procesos internos como a los terceros que prestan servicios en la UAESP. De esta manera, se promueve una cultura de seguridad de la información, garantizando un enfoque integral en la gestión y protección de los datos personales.

Adicionalmente se realizó la evaluación de los riesgos potenciales en relación con el manejo de los datos personales por parte de los procesos, incluyendo posibles brechas de seguridad, vulnerabilidades en el sistema de gestión documental (ORFEO) y oportunidades de mejora en las políticas internas.

3. CONFORMIDADES Y FORTALEZAS, O ASPECTOS POSITIVOS ENCONTRADOS

Estas conformidades y fortalezas reflejan un avance hacia el cumplimiento de la Ley 1581 de 2012 sobre PDP, así como un compromiso firme con la implementación de mejores prácticas y el cumplimiento de las normativas vigentes. A continuación, se presentan los aspectos más destacables que surgieron durante el ejercicio de auditoría:

- La UAESP cuenta un Programa Integral de Protección de Datos personales publicada en la página web. Enlace
- La entidad cuenta con una política definida para la protección de datos personales en su versión No. 4, la cual fue actualizada el 25/08/2023. Sobre esta política la OCI evidenció avances en su implementación y socialización a los procesos. Enlace
- Se evidenció la inclusión de cláusulas específicas de protección de datos en los contratos de prestación de servicios, cumpliendo con las regulaciones y estándares vigentes.
- Se emprendieron acciones orientadas a sensibilizar al personal sobre la importancia de la protección de datos personales, en línea con el plan anual de capacitación, promoviendo así la apropiación de la Ley 1581 de 2012. Enlace
- Se consideraron las diversas recomendaciones formuladas en la auditoría anterior, implementando acciones específicas orientadas a mitigar riesgos y potenciar mejoras en los procesos relacionados con la protección de datos personales.
- La entrega puntual de evidencias e información por parte de los procesos fue importante por lo cual se destacada como un aspecto positivo en la auditoría.
- La entidad realiza la actualización del inventario de activos de información donde se identifican los datos personales por cada proceso. Enlace
- La entidad cuenta con el rol de “Oficial de Protección de Datos Personales”, designado mediante Resolución 490 de 2022. En cumplimiento con los lineamientos establecidos en la “Guía para la implementación del Principio de Responsabilidad Demostrada (Accountability).

- La entidad realiza de manera periódica el registro de las bases de datos con información personal en el "Registro Nacional de Bases de Datos (RNBD)", administrado por la SIC Enlace.

4. OBSERVACIONES

De acuerdo, con el análisis y evaluación de los instrumentos aplicados junto con las evidencias aportadas por los procesos, la OCI formula la siguiente observación, con el objetivo de fortalecer la protección de los datos personales de la UAESP y evitar la materialización del riesgo:

Tabla 10 - Observaciones de la auditoría

No.	PROCESO	DESCRIPCIÓN DE LA OBSERVACIÓN
1	**OTIC – TH**	**Diagnóstico para el Cumplimiento de la Ley 1581 - Primera Perspectiva con Base en la Guía de la SIC.** **11. Gestión de encargados del tratamiento** Al revisar las reuniones llevadas a cabo por TH y actividades realizadas por terceros, esta oficina evidenció que algunas empresas están recopilando datos personales sin cumplir con los requisitos legales necesarios para actuar como encargados del tratamiento de datos personales, ver Anexo 2 - Evidencias. En los siguientes enlaces se puede acceder a algunos de los formularios para la captura de datos personales enviados por terceros: - Charla Dime en qué inviertes y te diré si puedes 25/10/2023: enlace - formulario - Charla de selección, uso y reposición de elementos de protección personal, 20/10/2023: enlace-formulario

5. SOLICITUD DE CORRECCCIÓN O ACCIONES CORRECTIVAS

Tabla 11 – Solicitud de Correcciones o Acciones Correctivas

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

6. CONCLUSIONES

Tras evaluar los instrumentos: 1. Perspectiva con base en la guía de la Superintendencia de Industria y Comercio – SIC y 2. Verificación de controles de seguridad del instrumento de la Alta Consejería TIC del Distrito, a continuación, se presentan las diferentes conclusiones derivadas de dicho análisis:

- Como resultado del ejercicio de auditoría se evidenció una calificación general del 87.9% en la implementación del régimen de PDP según Ley 1581 de 2012 con respecto a la guía de la SIC, es decir se evidenció un avance del 27,4% frente al 60.5% obtenido en el 2023.
- Frente a la evaluación del instrumento de la alta consejería TIC de controles de seguridad y buenas prácticas se evidenció un avance general del 78% para el 2024 frente 70% obtenido en la evaluación de 2023.
- Este avance representa una mejora notable respecto a la evaluación registrada en el anterior año 2023, reflejando los esfuerzos y el compromiso continuo de la entidad en fortalecer la protección de datos personales y cumplir con las normativas.
- En cuanto a la primera perspectiva de la SIC se encuentran algunos criterios con avances significativos como son**: 2.** Tratamiento de datos sensibles y de menores de edad**, 8**. Política de tratamiento de datos personales, **9**. Aviso de privacidad, **10**. Reporte de violaciones a los códigos de seguridad, **12**. Transferencia y transmisión internacional de datos personales.
- Así mismo se encuentran algunos criterios con rezago en la implementación como son los siguientes: **11.** Gestión de encargados del tratamiento Encargado del Tratamiento, **5.** Información mínima a los titulares.
- En cuanto a la segunda perspectiva de la Alta consejería se encuentran algunos criterios con avances significativos como son: **2.** Gestión de incidentes o incumplimientos en seguridad de los datos personales y **9**. Revisión de controles de sensibilización, capacitación o formación a los servidores públicos en lo relacionado con protección de datos personales.
- La OCI, evidenció algunos criterios con bajo porcentaje de calificación como fueron: **7.** Revisión del estado actual de controles técnicos cuando se comparte la información de datos personales con terceras partes, **8**. Revisión del estado actual de controles técnicos en la eliminación de datos personales o cuando pasan a ser históricos respectivamente.
- Es fundamental fortalecer la gestión de protección de datos personales, para impulsar acciones en toda la entidad, como también involucrar a todos los funcionarios en esta iniciativa, así crear

un ambiente de responsabilidad compartida que garantice una implementación efectiva de la Ley 1581 de 2012.

- Se debe continuar con establecer no sólo el programa, la política y procedimientos, sino también promover una cultura organizacional orientada hacia la protección de la información personal en la UAESP.
- Es esencial continuar impulsando y capacitando a todos los procesos y equipos de trabajo, asegurando que comprendan la importancia de cumplir con las normas y prácticas en materia de protección de datos personales.

7. RECOMENDACIONES

Recomendaciones por proceso

En el desarrollo de la auditoría se evidenciaron algunas recomendaciones que dan lugar para que cada uno de los procesos las revisen y apropien los diferentes planes de acción para minimizar los riesgos asociados y evitar que pasen a observaciones en una posterior evaluación.

Tabla 12 - Recomendaciones por proceso

No.	PROCESO	RECOMENDACIÓN
1	OAP	Validar que la captura de datos personales realizada durante los ejercicios de rendición de cuentas y los espacios ciudadanos, cumplan con lo establecido en la ley 1581 de 2012.
2	SRBL	Responder a la totalidad de los criterios solicitados por esta oficina y los que no aplican justificarlos, dado que el proceso es el administrador funcional de la aplicación SIGAB, que realiza el tratamiento de datos personales. En esta dinámica, SIGAB desempeñaría el rol de encargado del tratamiento de datos, mientras que la UAESP asumiría la responsabilidad de supervisar y asegurar la protección integral de dicha información, en estricto cumplimiento con las normativas y regulaciones aplicables.
3	SDF	Realizar seguimiento para ajuste del formato que dé cumplimiento con el criterio "***5.4 Se informa de manera clara y expresa a los Titulares, al momento de solicitar la autorización para el Tratamiento de datos personales, la identificación, dirección física y electrónica y teléfono del responsable del Tratamiento***" y así lograr su implementación a través del SIG.
4	SAPROV	Importante por parte del proceso emprender acciones para implementar los criterios "***5.3. Se informa de manera clara y expresa a los Titulares, al momento de solicitar la autorización para el Tratamiento de datos personales, los derechos que les asisten y 5.4. Se informa de manera clara y expresa a los Titulares, al momento de solicitar la autorización para el Tratamiento de datos personales, la identificación, dirección física y electrónica y teléfono del***

No.	PROCESO	RECOMENDACIÓN
		responsable del Tratamiento". Respectivamente y su implementación a través del SIG.
5	**SSFAP**	Realizar una evaluación independiente del cumplimiento de la Ley 1581 de 2012, llevando a cabo un análisis específico para el proceso de alumbrado público y otro para el proceso de funerario, con el ánimo de ver oportunidades de mejora de cada uno.
6	**SAF-TH**	***1.1. Se recolecta información personal para finalidades legítimas y se informa al Titular esas finalidades (TODOS LOS PROCESOS)*** Considerar la pertinencia de ajustar los formularios de asistencia, en virtud del propósito declarado de la recopilación de estos datos, el cual se limita a "***Serán utilizados exclusivamente como insumo para verificar la asistencia***". Desde la perspectiva de protección de datos personales, la OCI no ha identificado una conexión directa entre la recopilación de un listado de asistencia y la inclusión de preguntas que puedan considerarse de naturaleza sensible. Esta falta de coherencia entre la finalidad declarada y la naturaleza de los datos recopilados podría interpretarse como una contradicción con el principio de especificidad establecido en la Ley 1581 de 2012. Este principio, según lo manifestado por la Superintendencia de Industria y Comercio (SIC), dictamina que la finalidad del tratamiento de datos debe ser claramente definida, explícita y legítima desde el momento de su recolección, como se observa a continuación: ***El principio de la finalidad debe tenerse en cuenta para el tratamiento de cualquier tipo de datos personales***. Concepto Radicado No. 16-459471 del 27 de enero de 2017, fuente: Principio de la finalidad **9. Revisión de controles de sensibilización, capacitación o formación a los servidores públicos en lo relacionado con protección de datos personales** Aplicar y reforzar la socialización del plan integral de protección de datos personales, así como la política, manual y procedimientos respectivos; es decir, validar su aplicabilidad, garantizando así una gestión coherente y alineada con las mejores prácticas en protección de datos. ***11.1. Se han establecido procedimientos internos para asegurar que los Encargados del Tratamiento garanticen la protección de los datos personales que le son entregados y que su Tratamiento se haga acorde con los principios y deberes establecidos en la ley.***

No.	PROCESO	RECOMENDACIÓN
		Contar con acuerdo de confidencialidad para encargados de tratamiento de datos personales, esto para los diferentes proveedores que prestan algún servicio en la entidad (ejemplos: capacitaciones, ferias, servicios, entre otros).
7	SAF-SC	**5.5. Se conserva prueba de haber informado a los Titulares lo mencionado anteriormente** La OCI recomienda coordinar con la OTIC los mecanismos que permitan cumplir con lo solicitado en el punto. **7.9. Se da a conocer a los Titulares los procedimientos dispuestos por la organización para el acceso, actualización, supresión y rectificación de datos personales y de revocatoria de la autorización, y los mismos son fácilmente accesibles.** La OCI recomienda validar los controles que permitan obtener el permiso a las peticiones recibidas vía telefónica
8	SAL	**5.3. Se informa de manera clara y expresa a los Titulares, al momento de solicitar la autorización para el Tratamiento de datos personales, los derechos que les asisten.** La OCI recomienda revisar la viabilidad de incluir en los documentos de contratación un apartado sobre el derecho que asiste a los titulares de los datos. **5.4. Se informa de manera clara y expresa a los Titulares, al momento de solicitar la autorización para el Tratamiento de datos personales, la identificación, dirección física y electrónica y teléfono del responsable del Tratamiento.** La OCI recomienda tanto a la OTIC como a la SAL, verificar la viabilidad de actualizar la política y demás documentos relacionados dando cumplimiento a lo solicitado en el punto de estudio. **5.5. Se conserva prueba de haber informado a los Titulares lo mencionado anteriormente** La OCI recomienda cumplir con los puntos anteriores permitiendo alcanzar lo solicitado en el numeral 5.5.

No.	PROCESO	RECOMENDACIÓN
		Nota: A pesar de que se carguen los datos en SECOP la UAESP mantiene archivo de los mismos por lo cual es importante verificar con gestión documental y OTIC el cumplimiento normativo.
9	OTIC	**Revisión primera Perspectiva con base en la guía de la Superintendencia de Industria y Comercio - SIC** **1.6. ¿Se cuenta con medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a la información personal para evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento?:** Con base en las evidencias presentadas por el proceso y de acuerdo con ejercicios realizados en el aplicativo de gestión documental ORFEO, donde el equipo auditor pudo consultar información de tipo confidencial y sensible. La OCI recomienda continuar con las tareas de fortalecimiento del etiquetado de la información confidencial asegurando el acceso solo a las partes interesadas, ver Anexo 2 - Evidencias. **5.4. ¿Se informa de manera clara y expresa a los Titulares, al momento de solicitar la autorización para el Tratamiento de datos personales, la identificación, dirección física y electrónica y teléfono del responsable del Tratamiento?** Ajustar el "Aviso de privacidad" tanto en los formatos dispuestos en los canales virtuales y formatos físicos, incluyendo "la identificación, dirección física y electrónica y teléfono del responsable del Tratamiento (UAESP)" ver Anexo 2 - Evidencias. **5.5. ¿Se conserva prueba de haber informado a los Titulares lo mencionado en los criterios (5,1 – 5,4)?** Evaluar la viabilidad de implementar un repositorio consolidado donde se puedan consultar las: "prueba de haber informado a los Titulares" de manera unificada. **11.6. ¿Se cuenta con medidas necesarias para que la información suministrada al Encargado se mantenga actualizada?** Realizar levantamiento de información, para determinar sí los concesionarios que suscriben contrato con la UAESP realizan tratamiento de datos personales a nombre de la entidad **13. Responsabilidad demostrada (Accountability)** Demostrar ante cualquier organismo de control, que la UAESP adopta las medidas necesarias para cumplir con las reglas sobre el tratamiento de datos personales. Es indispensable tener presente que "***los responsables del tratamiento de datos***

No.	PROCESO	RECOMENDACIÓN
		personales deben ser capaces de demostrar, a petición de la SIC, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 (47) y en el Decreto 1377 de 2013" **Revisión Segunda Perspectiva - verificación de controles de seguridad del instrumento de la Alta Consejería TIC del Distrito** **1.2. ¿Se realiza identificación y gestión de riesgos a los datos personales?** Fortalecer la identificación y gestión de riesgos relacionados con datos personales gestionados por los concesionarios y terceros. **1.3. ¿Se cuenta con plan de tratamiento de riesgos de datos personales documentado?** Incluir en los planes presentados como evidencia, una sección exclusiva para el tratamiento de riesgos asociados a los datos personales. **3.1. ¿Se cuenta con el aviso de aceptación de tratamiento de datos personales?** Ampliar la implementación del aviso de aceptación a la totalidad de los mecanismos que recolectan datos personales. **3.4. ¿Cuenta con procedimientos para garantizar que todos los datos personales recogidos son exactos, completos y actualizados?** Adelantar las actividades necesarias para ampliar el alcance de los controles y procedimientos existentes, implementar nuevos y demostrar su efectividad, permitiendo cumplir lo solicitado en este criterio. Se deben establecer mecanismos para que "Usuarios desconocidos" no tengan permisos de compartir enlaces con listados de asistencia no autorizados en las reuniones de la entidad, ver Anexo 2 - Evidencias. **4.1. ¿Se tienen identificada las Bases de datos con información personal en los sistemas de información de los procesos?** Validar la viabilidad de realizar un inventario con los operadores externos, con el fin de determinar si están realizando captura y tratamiento de datos personales responsabilidad de la UAESP.

No.	PROCESO	RECOMENDACIÓN
		5.4. ¿Se realiza revisión periódica de los privilegios de accesos otorgados a la información personal? Evaluar la viabilidad de implementar un procedimiento o mecanismo de revisión periódica de los privilegios de acceso otorgados a las bases de datos que almacenan información personal en la entidad. **6.1. ¿Se tiene cifrada la Base de datos para proteger la información de datos personales?** - Verificar los permisos de lectura sobre la información sensible en ORFEO, dado que al filtrar por las siguientes palabras: “contraseña” e “incapacidad”, se obtuvo acceso a información sensible, ver Anexo 2 - Evidencias. - Verificar la viabilidad de implementar mecanismos de seguridad tendientes a proteger las bases de datos con información personal almacenada en OneDrive y equipos de los colaboradores de la entidad. **6.2. ¿Se tiene anonimización la información de datos personales en la base de datos?** Validar la viabilidad de Implementar los controles que permitan realizar la anonimización de los datos personales en la totalidad de las bases de datos y sistemas de información que procesan y almacenan datos personales. **6.3.¿Se tiene activación de registros de auditoría de las acciones realizadas por los usuarios en las Bases de datos con información personal?** Verificar la viabilidad de ampliar los logs de auditoría sobre la totalidad de las bases de datos que contienen datos personales como (OneDrive, Ruro, Sira, etc.) y contar con una herramienta automatizada que le permita realizar una gestión centralizada sobre los registros de auditoría. **6.5. Cuando se hace un campo en los datos personales de la BD, ¿Se replica o actualiza el cambio al resto de BD's?** Ampliar el alcance del control para asegurar el cumplimiento de las especificaciones solicitadas en todos los sistemas de bases de datos que almacenen información personal. **6.6. ¿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?**

No.	PROCESO	RECOMENDACIÓN
		Implementar los controles que permitan conservar los datos personales almacenados solo por el tiempo necesario de la finalidad que fueron recogidos. **7.2. ¿Se tiene establecido una política o control documental para establecer acuerdos de confidencialidad o de no divulgación cuando se comparte información de datos personales con terceras partes?** Implementar la política y controles a la totalidad de bases de datos y sistemas de información de la entidad, ya que el equipo auditor encontró terceros que capturan información sin el cumplimiento de lo solicitado en la norma, ver Anexo 2 - Evidencias. **7.3. ¿Se cuenta con mecanismos de control para cifrar la información punto a punto durante la transferencia?** Las URL's; uaesp.gov.co, gdocumental.uaesp.gov.co, intranet.uaesp.gov.co/wp-login.php, tienen habilitados el puerto 80 (http) protocolo que no cifra la información punto a punto. La OCI, recomienda llevar a cabo los ajustes necesarios para asegurar que las conexiones se realicen solo por protocolos seguros (https). **8.2. ¿Se cuenta con procedimientos de eliminación y retención de datos personales?** Adelantar las acciones necesarias para actualizar o implementar los controles técnicos, que permitan a la entidad la eliminación segura de datos personales atendiendo a los tiempos de retención. **8.3. ¿Se encuentra documentado en el aviso de privacidad la vigencia de los datos personales?** Actualizar el aviso de privacidad, incluyendo "la vigencia de los datos personales" tal y como lo solicita el punto evaluado.

Recomendaciones Generales

A continuación, se relacionan las recomendaciones que aplican a todos los procesos evaluados, para que se tengan en cuenta como oportunidades de mejora:

- Apropiar los conocimientos del plan integral de protección de datos personales, así como la política, manual y procedimientos respectivos; es decir, validar su aplicabilidad, garantizando así una gestión coherente y alineada con las mejores prácticas en protección de datos.

- Es esencial que los procesos conozcan, integren y apliquen adecuadamente los protocolos de -PQRS (Peticiones, Quejas, Reclamos y Sugerencias) diseñados para la gestión de datos personales. Estos protocolos garantizan una respuesta eficiente y conforme a la normativa vigente frente a cualquier solicitud o consulta relacionada con la información personal manejada por la entidad en caso de presentarse.
- Considerar no solo la política de protección de datos, sino también los mecanismos detallados en el manual y en el programa de datos personales, tal como lo ha establecido la Oficina de Tecnologías de la Información y Comunicaciones (OTIC). Estos elementos constituyen herramientas fundamentales para asegurar una gestión adecuada y coherente de la información personal dentro de la UAESP.
- Se sugiere designar un responsable o gestor específico para la gestión de datos personales por cada proceso, quien trabajará en conjunto con el Oficial de Protección de Datos de la entidad. Esta estrategia reforzará el equipo encargado de la protección de datos, facilitando una ejecución consistente y eficaz de las políticas y procedimientos relacionados con la seguridad y privacidad de la información personal de la entidad.
-

8. Aprobación

Sandra Beatriz Alvarado Salcedo

Firmado digitalmente por Sandra Beatriz Alvarado Salcedo
Fecha: 2024.04.29 16:15:11 -05'00'

Sandra Beatriz Alvarado Salcedo

Jefe de Oficina de Control Interno

FIRMA(S)

Auditor(es) Interno(s) que ejecutaron el trabajo

FECHA 26-04-2024