

MEMORANDO



Al contestar, por favor cite el radicado:

No.: **20251100092743**

Página 1 de 5

Bogotá D.C., 28 de noviembre de 2025

PARA: **JORGE ALEXIS RODRIGUEZ MEZA**
Oficina de Tecnologías de la Información y las Comunicaciones

DE: Oficina de Control Interno

ASUNTO: Informe evaluación del Modelo de Seguridad y Privacidad de la Información
MSPI – 2025

Respetado ingeniero:

De conformidad con el Plan Anual de Auditorías 2025, la OCI comunica el Informe de Auditoría al Modelo de Seguridad y Privacidad de la Información de la UAESP, en el cual, luego de la verificación realizada, se concluyó que, en atención a la actualización de la normativa de la ISO 27001:2013 a la ISO 27001:2022, se procedió a efectuar una evaluación en dos sentidos:

Primero, se llevó a cabo la verificación de las observaciones y recomendaciones emitidas en la auditoría 2024. Dichas observaciones concluyeron con el cierre de la evaluación del Modelo MSPI bajo la normativa anterior. Como resultado de esta revisión, la OCI validó los puntos evaluados y estableció un nivel de cumplimiento del **83 %**, lo cual representa un incremento del **4 %** respecto a la evaluación realizada en 2024, cuyo resultado fue del 79 %. Asimismo, la evaluación de la efectividad de los controles quedó clasificada en el estado **“OPTIMIZADO”**, de acuerdo con la escala de calificación del instrumento definido por el MinTIC.

Segundo, se adelantó la evaluación de los nuevos controles incorporados por la actualización normativa, correspondientes a **11 controles** y **166 criterios**, distribuidos de la siguiente manera:

- Controles organizacionales: **3**
- Controles físicos: **1**
- Controles técnicos: **7**

A partir de este ejercicio de auditoría se generaron los siguientes resultados

Unidad Administrativa Especial de Servicios Públicos

Cra 10 No. 17-72 L-119

PBX: (+57) 601 358 0400

www.uaesp.gov.co

MEMORANDO



Al contestar, por favor cite el radicado:

No.: **20251100092743**

Página 2 de 5

Bogotá D.C., 28 de noviembre de 2025

Conclusiones:

Tras evaluar el nivel de avance del modelo MSPI frente a la normativa ISO 27001:2013 y los nuevos controles establecidos en la ISO 27001:2022, se concluye lo siguiente:

- A partir de la evaluación de la auditoría para el cierre del MSPI, se obtuvo un resultado del **83%**, frente al **79%** alcanzado en el período anterior. Esta evaluación se realizó con base en el instrumento definido por el MinTIC.
- Para esta vigencia el proceso realizó el autodiagnóstico con la nueva normativa y esta evaluación arrojó un resultado del 74%
- La OCI validó los 11 nuevos controles establecidos en la normativa ISO 27001:2022, obteniendo una calificación del 45%, frente al 42% alcanzado por la OTIC. La diferencia en los puntajes se debe a que la autoevaluación del proceso por parte de la OTIC se realizó en julio de 2025, mientras que la evaluación de la OCI se efectuó en noviembre de 2025, momento en el cual ya se contaba con mayores evidencias y avances en la implementación del modelo para estos nuevos controles. Los resultados de esta evaluación se encuentran en el **Anexo 1- Instrumentos de nuevos controles evaluados**.
- Dado que la evaluación abarcó controles recientemente implementados, se evidenció que la mayoría se encuentran en fases iniciales de su puesta en marcha. Este escenario implica que dichos controles aún no han alcanzado su nivel óptimo de madurez, por lo que su efectividad puede ser parcial y dependerá de ajustes y seguimiento continuo para asegurar el cumplimiento de los objetivos de control establecidos.
- Se considera prioritario designar un responsable de la seguridad de la información y otro de la protección de datos personales, con autoridad y competencias suficientes para garantizar la implementación, seguimiento y mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI). Este rol se recomienda que esté por fuera de la

MEMORANDO



Al contestar, por favor cite el radicado:

No.: **20251100092743**

Página 3 de 5

Bogotá D.C., 28 de noviembre de 2025

estructura de la OTIC, a fin de asegurar la imparcialidad en la gestión y evaluación del modelo.

Recomendaciones

Una vez finalizado el ejercicio de auditoría la OCI presenta las siguientes recomendaciones tanto administrativas como técnicas, esto con el fin de que al interior del proceso el equipo de trabajo de OTIC priorice y ejecute las acciones necesarias para mitigar posibles materializaciones de riesgos que puedan surgir en la seguridad de la información de la entidad.

Recomendaciones a Controles Organizacionales

No.	PROCESO	RECOMENDACIÓN
1	AD.1.7- A 5.7 Inteli- gencia de amenazas	Definir, documentar y formalizar ante el SIG un procedimiento formal de inteligencia de amenazas, integrando fuentes externas confiables y estableciendo análisis y documentando de manera periódica, que complemente la información del SIEM.
2	AD.1.23 – A 5.23 Seguridad de la información para el uso de servicios en la nube	Definir, documentar, socializar y formalizar ante el SIG una política y procedimiento de gestión de servicios en la nube de acuerdo con los criterios establecidos con el control.
3	AD.1.30 - A 5.30 Preparación de las TIC para la continuidad del negocio DRP-BCP	Actualizar y formalizar los requisitos de continuidad TIC basados en los resultados del BIA y la evaluación de riesgos, definiendo RTO, RPO y capacidades de los sistemas, realizar y documentar las pruebas de DRP. Llevar a cabo la gestión necesaria para coordinar con OAP la actualización y pruebas del BCP lo que corresponde a la OTIC.

Recomendaciones a controles Físicos

No.	PROCESO	RECOMENDACIÓN
1	F.1.4 - A 7.4 Supervisión de la seguridad física	Validar la posibilidad de que la OTIC cuente con sus propias cámaras y/o coordinar con la administración de RENOBÓ el acceso a los sistemas de monitoreo del edificio. Lo anterior obedece a los criterios establecidos en el control.

MEMORANDO



Al contestar, por favor cite el radicado:

No.: **20251100092743**

Página 4 de 5

Bogotá D.C., 28 de noviembre de 2025

Recomendaciones a controles Tecnológicos

No.	PROCESO	RECOMENDACIÓN
1	T.1.9 - A 8.9 Gestión de la configuración	Documentar y formalizar lo que corresponde en su totalidad a la Gestión de Configuración, definiendo y aprobando plantillas estándar de configuración segura, documentando roles y responsabilidades, y estableciendo un registro centralizado con el historial de cambios.
2	T.1.10 - A 8.10 Eliminación de información	Formalizar y fortalecer el proceso de eliminación segura de información y garantizar que la información confidencial sea destruida de acuerdo con los periodos de retención, métodos aprobados y requisitos normativos.
3	T.1.11 - A 8.11 Enmascaramiento de datos protección de datos	Implementar técnicas de enmascaramiento, seudonimización o anonimización según la sensibilidad de los datos y realizar verificaciones de su efectividad. Así mismo, restringir accesos por roles para que quede la trazabilidad, esto con base en la normatividad.
4	T.1.12 - A 8.12 Prevención de fuga de datos DLP	Se recomienda avanzar en la implementación de controles de Prevención de Pérdida de Datos (DLP: Data Loss Prevention), que permitan detectar, monitorear y mitigar posibles incidentes de exposición no autorizada de información. Esto contribuirá a reforzar la cultura de seguridad y el cumplimiento de las políticas institucionales de protección y fuga de información sensible
5	T.1.16 - A 8.16 Actividades de seguimiento (monitoreo)	Formalizar e implementar el proceso de monitoreo de seguridad, con los criterios que establece el control.
6	T.1.23 - A 8.23 Filtrado web	Reforzar capacitaciones y/o sensibilizaciones periódicas para los funcionarios sobre la navegación web segura. Y mantener actualizados los documentos sobre bloqueos y excepciones. Así mismo, culminar con la configuración del nuevo Firewall con filtrados de contenido, listas negras, blancas y los criterios establecidos en el control.
7	T.1.28 - A 8.28 Codificación segura	Actualizar, socializar y aplicar el proceso integral de desarrollo seguro de software, incorporando normas de codificación, modelado de amenazas, revisiones de código, uso de herramientas SAST, gestión de librerías externas y capacitación periódica al equipo de desarrollo si es necesario.

MEMORANDO

Al contestar, por favor cite el radicado:

No.: **20251100092743**

Página 5 de 5

Bogotá D.C., 28 de noviembre de 2025

Por último, se recomienda al proceso revisar y considerar la evaluación realizada por la OCI respecto a algunas sugerencias de continuar con las acciones realizadas para las recomendaciones emitidas en el año anterior, así como las observaciones presentadas en esta evaluación sobre los nuevos controles. Es fundamental que el proceso implemente las actividades y/o acciones necesarias con el objetivo de cerrar las recomendaciones identificadas, ya que, de no hacerlo, en una próxima evaluación estas recomendaciones podrían mantenerse como observaciones, afectando el nivel de cumplimiento y madurez del sistema. La adopción oportuna de estas medidas contribuirá a fortalecer la gestión del riesgo y garantizar la mejora continua del modelo.

Por lo anterior, es esencial validar y contemplar las acciones necesarias que permitan avanzar hacia el cumplimiento e implementación total del modelo, de acuerdo con la normatividad vigente aplicable.

La OCI queda atenta a la suscripción del plan de mejoramiento correspondiente a las observaciones descritas, conforme a lo establecido en el procedimiento “PC-03 PM Planes de Mejoramiento V10”, el cual debe ser entregado dentro de los 10 días hábiles siguientes a la recepción del presente informe.

Agradecemos la disposición y colaboración brindada durante el desarrollo de esta auditoría, y quedamos atentos a cualquier inquietud al respecto.

Cordialmente,

Sandra
Beatriz
Alvarado
Salcedo

Firmado
digitalmente por
Sandra Beatriz
Alvarado Salcedo
Fecha: 2025.11.28
20:02:38 -05'00'

SANDRA BEATRIZ ALVARADO SALCEDO

Jefe Oficina de Control Interno

Sandra.alvarados@uaesp.gov.co

Anexos: Informe resultados de auditoría - MSPI_2025

Anexo No 1-Instrumentos de nuevos controles evaluados.

Elaboró: Ligia Marlén Velandia L. P.E – 222-24 - OCI

Revisó y Aprobó: Sandra Beatriz Alvarado Salcedo – jefe Oficina OCI

Unidad Administrativa Especial de Servicios Públicos**Cra 10 No. 17-72 L-119****PBX: (+57) 601 358 0400****www.uaesp.gov.co**

CONTENIDO

1. INFORMACIÓN GENERAL DE LA AUDITORIA	3
2. DESARROLLO DE LA AUDITORIA	5
2.1. Planificación de la Auditoría	5
2.2. Verificación de los avances sobre las observaciones y recomendaciones de la auditoría MSPI - 2024	6
• Seguimiento a Observaciones	6
• Seguimiento a Recomendaciones a controles administrativos	10
• Seguimiento a Recomendaciones a controles técnicos	16
• Cierre de MSPI 27001_2013:	25
2.3. Verificación de los nuevos controles con la nueva normativa ISO/IEC 27001:2022	27
2.4. Controles Organizacionales	27
2.4.1. AD.1.7- A 5.7: Inteligencia de amenazas	28
2.4.2. AD.1.23 - A 5.23: Seguridad de la información para el uso de servicios en la nube	28
2.4.3. AD.1.30 - A 5.30: Preparación de las TIC para la continuidad del negocio DRP-BCP	29
2.5. Controles físicos	29
2.5.1. F.1.4 - A 7.4: Supervisión de la seguridad física	30
2.6. Controles Tecnológicos	30
2.6.1. T.1.9 - A 8.9: Gestión de la configuración	30
2.6.2. T.1.10 - A 8.10: Eliminación de información	31
2.6.3. T.1.11 - A 8.11: Enmascaramiento de datos - protección de datos	31
2.6.4. T.1.12 - A 8.12: Prevención de fuga de datos DLP	32
2.6.5. T.1.16 - A 8.16: Actividades de seguimiento (monitoreo)	32
2.6.6. T.1.23 - A 8.23: Filtrado web	33

2.6.7. T.1.28 - A 8.28: Codificación segura - desarrollo de software	33
2.7. Gestión de Riesgos	34
3. CONFORMIDADES Y FORTALEZAS, O ASPECTOS POSITIVOS ENCONTRADOS ...	35
4. OBSERVACIONES	37
5. SOLICITUD DE CORRECCIÓN O ACCIONES CORRECTIVAS	38
6. CONCLUSIONES	39
7. RECOMENDACIONES	40
8. APROBACIÓN	42

Lista de Tablas

Tabla 1- Información de la auditoría	3
Tabla 2 - Seguimiento a observaciones producto de auditoría 2024	7
Tabla 3 - Seguimiento a Recomendaciones Controles Administrativos Producto Auditoría 2024	10
Tabla 4 - Seguimiento a Recomendaciones Controles Técnicos Producto Auditoría 2024	16
Tabla 5 - Evaluación Cierre MSPI con ISO 27001:2013	26
Tabla 6 - Resultado del Autodiagnóstico del MSPI con la nueva normativa ISO 27001:2022	36
Tabla 7 - Observaciones de la auditoría	38
Tabla 8 – Solicitud de Correcciones o Acciones Correctivas	38
Tabla 9 - Recomendaciones a Controles Organizacionales	40
Tabla 10 - Recomendaciones a controles Físicos	40
Tabla 11 - Recomendaciones a controles Tecnológicos	41

Lista de Ilustraciones

Ilustración 1 - Riesgos Seguridad de la Información OTIC	35
Ilustración 2 - Evidencias nueva infraestructura TIC	37

1. INFORMACIÓN GENERAL DE LA AUDITORIA

Tabla 1- Información de la auditoria

ENFOQUE DE LA AUDITORIA INTERNA	- Gestión y Resultados. - Modelo de Seguridad y Privacidad de la Información (MSPI).
INFORME	Informe de la auditoría realizada al (MSPI) con corte a 30 de septiembre de 2025 de la Unidad Administrativa Especial de Servicios Públicos (UAESP).
PROCESO, PROCEDIMIENTO	Oficina de tecnologías de la información y las comunicaciones (OTIC).
RESPONSABLE O AUDITADOS	Jefe de la OTIC y equipo designado.
OBJETIVO	Evaluar el Sistema de Gestión de la Seguridad de la Información (SGSI) vigente en la UAESP, conforme a los lineamientos establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI) y en la norma ISO/IEC 27001:2022, incluyendo la verificación de la implementación de los nuevos controles del Anexo A.
ALCANCE	- Verificar las acciones implementadas en atención a las observaciones y recomendaciones derivadas de la auditoría 2024, con el propósito de dar cierre al MSPI bajo la norma ISO 27001:2013. - Validar la aplicación del nuevo instrumento definido en la Resolución 2277 de junio de 2025, con especial énfasis en los nuevos controles incorporados en la norma ISO 27001:2022
PERIODO DE EJECUCIÓN	Del 01/10/2025 al 30/11/2025
EQUIPO AUDITOR	Ligia Marlén Velandia León – LMVL
DOCUMENTACIÓN ANALIZADA	- Norma ISO/IEC 27001:2022. Controles del Anexo A (documento de referencia). - Requisitos legales aplicables (Ley 1581 de 2012 sobre protección de datos personales, Decreto 1377, etc.). - Políticas y procedimientos internos de seguridad de la información de la UAESP.

- Resolución 2277 de junio 3 de 2025
- CONPES 3995 de 2020 - Política nacional de confianza y seguridad digital.
- Resolución 500 de 2021 Actualización Anexo 1
- Ley 1341 de 2009
- Decreto 2106 de 2019
- Resolución 746 de 2022
- DECRETO 1008 DE 2018 - Política de gobierno digital
- CONPES 3701 JULIO DE 2011 - Lineamientos de política para ciberseguridad y ciberdefensa.
- Guía para la Gestión Integral del Riesgo en Entidades Públicas Versión 7 – Capitulo 5 de 2025
- Procedimientos OTIC – vigentes.
- Documentación modelo de seguridad y privacidad de la información – MSPI vigente en la UAESP.
- Plan estratégico de tecnologías de la información – PETI, vigente en la UAESP.
- Plan de tratamiento de riesgos de seguridad de la información – vigente en la UAESP
- PMI - Plan de Mejoramiento Interno
- MSPI- Modelo de Seguridad y Privacidad de la Información – Autodiagnóstico
- Mapa de Riesgos y Oportunidades – Riesgos de Seguridad de la Información - vigente en la UAESP
- Inventario de aplicativos – Vigentes en la UAESP
- Documentos del proceso, disponibles en el Sistema Integrado de Gestión - SIGMSPI- Modelo de Seguridad y Privacidad de la Información – Autodiagnóstico
- Mapa de Riesgos y Oportunidades – Riesgos de Seguridad de la Información - vigente en la UAESP
- Ley 1581 y decreto 1377 - Derechos de propiedad intelectual, protección de registros, privacidad de la información relacionada con datos personales Ley 1581 y decreto 1377.
- Inventario de aplicativos – Vigentes en la UAESP.
- Norma - NTC: ISO/IEC 27001:2013 (La norma se encuentra actualizada a la versión 2022, sin embargo, el MSPI sigue operando bajo la versión 2013).
- Resolución 500 de 2021 MinTic.

- Metodología del Instituto Nacional de Estándares y Tecnología (NIST).
- Documentos del proceso, disponibles en el Sistema Integrado de Gestión (SIG).

2. DESARROLLO DE LA AUDITORIA

2.1. Planificación de la Auditoría

En cumplimiento con el Plan Anual de Auditorías (PAA) del año 2025, la Oficina de Control Interno (OCI), llevó a cabo la auditoría al MSPI, notificada mediante Radicado No. 20241100079923 del 2 de octubre de 2025. El objetivo de esta auditoría fue verificar las acciones implementadas en atención a las observaciones y recomendaciones derivadas de la auditoría 2024, con el propósito de dar cierre al MSPI bajo la norma ISO 27001:2013, y validar la aplicación del nuevo instrumento definido en la Resolución 2277 de junio de 2025, con especial énfasis en los nuevos controles incorporados en la norma ISO 27001:2022. La evaluación se realizó siguiendo los lineamientos del MSPI.

Durante la auditoría, se evaluaron los siguientes componentes:

1. **Seguimiento de observaciones del MSPI producto de la auditoría anterior:** Se revisó cada una de las observaciones y sus acciones propuestas para el cumplimiento de estas, así mismo, se tuvo en cuenta el traslado a la nueva sede, toda vez que esto generó cambio de infraestructura tecnológica.
2. **Seguimiento de las recomendaciones del MSPI producto de la auditoria anterior:** Se revisó cada una de las recomendaciones y sus acciones realizadas al interior del proceso, también se tuvo en cuenta el traslado a la nueva sede lo que generó cambio de infraestructura tecnológica, como también producto de esta verificación, las recomendaciones a las cuales no se evidenció avance alguno se procedió a formular las observaciones respectivas.
3. **Cierre del MSPI bajo la norma ISO 27001:2013:** Se verificó el avance alcanzado del modelo con base en los avances realizados producto de las observaciones y recomendaciones durante la vigencia.
4. **Evaluación de los nuevos controles bajo la normativa ISO 27001:2022:** Se verificó uno a uno de los 11 controles nuevos de la nueva normativa junto con sus criterios respectivos; es decir, Controles Organizacionales (3), Físicos (1), Tecnológicos (7), para un total de 11 controles y alrededor de 166 criterios.

5. Evaluación, Gestión y Tratamiento de Riesgos de Seguridad de la Información: Se revisó la gestión de los riesgos asociados a la seguridad y privacidad de la información.

La metodología de evaluación tanto para el cierre del MSPI bajo la normativa del 2013 como para los nuevos controles bajo la nueva normativa de 2022, se basó en el instrumento proporcionado por el MinTIC, que permitió verificar la ejecución de los controles tanto administrativos y técnicos del MSPI anterior, como los controles organizacionales, físicos, tecnológicos del nuevo MSPI.

2.2. Verificación de los avances sobre las observaciones y recomendaciones de la auditoría MSPI - 2024

La Oficina de Control Interno realizó seguimiento a las observaciones y recomendaciones emitidas en la auditoría del MSPI con radicado No. :20241100095143 del 28 de noviembre de 2024. Esta revisión se enfocó en validar los avances realizados hasta septiembre de 2025, tomando en consideración las pruebas documentales presentadas y el nivel de cumplimiento con el Plan de Mejoramiento Interno (PMI) establecido. Así mismo, se tuvo en cuenta que en agosto de 2025 se realizó traslado a una nueva sede y algunas observaciones y recomendaciones dadas ya no fueron objeto de validación porque no aplicaron.

- **Seguimiento a Observaciones:**

De las siete (7) observaciones formuladas, el proceso presentó acciones de las cuales se constató que cuatro (4) de las observaciones junto con sus acciones han sido cerradas, producto del traslado a la nueva sede y las otras tres (3) observaciones junto con sus acciones se encuentran en desarrollo como son las acciones (376,377,378). A continuación, se describe cada una así:

Tabla 2 - Seguimiento a observaciones producto de auditoría 2024

CONTROLES	DESCRIPCIÓN DE LA OBSERVACIÓN	ACCION REALIZADA POR LA OTIC	EVIDENCIA	VALIDACION OCI
T.3.1.3. Seguridad de oficinas recintos e instalaciones. T.3.2.3 Seguridad del cableado.	1. Humedad, evidencia de posibles goteras y ausencia de iluminación, Anexo 3 - Informe técnico 2024: En el centro de datos del 4 piso, se evidenció humedad y rastro de posibles goteras. En los demás centros de datos evaluados se verificó la ausencia de iluminación.	Atentamente se solicita cierre de la observación, toda vez que esta es sobre la infraestructura de la sede anterior (Chapinero) y a partir de agosto de 2025, la UAESP se trasladó de sede.	https://uaespd-my.sharepoint.com/:b:/g/per/sonal/osbaldo_cortes_uaesp_gov_co/EW0hrLY8La9Dgvg6qRaQdi4Bx-1IP7fUnNDlr5jCM04enQ?e=CLFk3g	Con base con las evidencias aportadas por el proceso como como fue el convenio administrativo entre UAESP-RENOBO, esta acción dada a la observación del año anterior se da por cerrada, toda vez que, por el traslado a la nueva sede, las condiciones ambientales cambiaron. Se da por cerrada la observación.
	2. Etiquetado y organización (peinado) del cableado de red: En los centros de datos evaluados se evidenció la falta de orden y etiquetado de los cables de red. En algunos puntos de usuario final se evidenció la falta de organización tanto de los cables de red como de potencia ejemplo casitas.	Atentamente se solicita cierre de la observación, toda vez que está es sobre la infraestructura de la sede anterior (Chapinero) y a partir de agosto de 2025, la UAESP se trasladó de sede.	https://uaespd-my.sharepoint.com/:b:/g/per/sonal/osbaldo_cortes_uaesp_gov_co/EW0hrLY8La9Dgvg6qRaQdi4Bx-1IP7fUnNDlr5jCM04enQ?e=CLFk3g	Con base con las evidencias aportadas por el proceso como como fue el convenio administrativo entre UAESP-RENOBO, esta acción dada a la observación del año anterior se da por cerrada, toda vez que, por el traslado a la nueva sede, las condiciones ambientales cambiaron. Se da por cerrada la observación.
	3. Presencia de Elementos Inflamables en el Perímetro de Seguridad: Se observó la presencia de elementos inflamables en el perímetro de seguridad de la planta eléctrica, exponiéndola a un riesgo de seguridad y potencial amenaza para su integridad y el de la entidad. Adicionalmente las cerraduras de acceso a la planta se encuentran sin seguro y una de ellas no permite su cierre, como se observa en la tabla No. 2	Atentamente se solicita cierre de la observación, toda vez que está es sobre la infraestructura de la sede anterior (Chapinero) y a partir de agosto de 2025, la UAESP se trasladó de sede.	https://uaespd-my.sharepoint.com/:b:/g/per/sonal/osbaldo_cortes_uaesp_gov_co/EW0hrLY8La9Dgvg6qRaQdi4Bx-1IP7fUnNDlr5jCM04enQ?e=CLFk3g	Con base con las evidencias aportadas por el proceso como como fue el convenio administrativo entre UAESP-RENOBO, esta acción dada a la observación del año anterior se da por cerrada, toda vez que, por el traslado a la nueva sede, las condiciones ambientales cambiaron. Se da por cerrada la observación.
	1. Ausencia de un sistema de seguimiento y monitoreo de red e infraestructura crítica de TI.			
T.1.1.2 Acceso a redes y a servicios en red				

CONTROLES	DESCRIPCIÓN DE LA OBSERVACIÓN	ACCIÓN REALIZADA POR LA OTIC	EVIDENCIA	VALIDACION OCI
	La falta de un sistema de monitoreo de red e infraestructura crítica impide a la entidad tener un registro en tiempo real sobre las acciones que puedan afectar tanto la integridad, disponibilidad y confidencialidad de la red e infraestructura crítica de TI.	La OTIC realizó el despliegue y configuración del sistema de monitoreo Zabbix, el cual es una plataforma de código abierto utilizada para monitorizar la infraestructura de TI en tiempo real. Permite supervisar redes, servidores, máquinas virtuales, aplicaciones, bases de datos y servicios en la nube. Por lo expuesto la OTIC solicita el cierre de la observación.	https://uaespd-my.sharepoint.com/:b:/g/per/sonal/osbaldo_cortes_uaesp_gov_co/Eazy1FrVdCVBsxly19gQF7EB1o9FZlWLLcpMevjS18g?e=rwNZhM http://monitoreo.uaesp.gov.co/zabbix/	De acuerdo con las evidencias allegadas por el proceso sobre informe técnico, donde se evidencia la implementación del sistema Zabbix, para monitoreo de la plata forma, se evidenció cumplimiento de la acción. Recomendación: Como este hallazgo se encuentra en el PMI bajo la acción 376 en la herramienta ODOO, se sugiere realizar el respectivo seguimiento y solicitud de cierre, independientemente que su vencimiento sea en mayo de 2026. Cumplimiento evidenciado.
	2. Topología de red desactualizada			
	De acuerdo con la reunión sostenida con el proceso y la visita en sitio, el equipo auditor evidenció que la topología de red se encuentra desactualizada.	Atentamente se solicita cierre de la observación, toda vez que está trata sobre la infraestructura de la sede anterior (Chapinero) y en julio de 2025, la UAESP se trasladó de sede. Por tal motivo la topología de red cambió.	https://uaespd-my.sharepoint.com/:b:/g/per/sonal/osbaldo_cortes_uaesp_gov_co/EW0hrLY8La9Dgvg6qRaQdi4Bx-1IP7fUnNDlr5jCM04enQ?e=CLFk3g	Con base con las evidencias aportadas por el proceso como como fue el convenio administrativo entre UAESP-RENOBO, esta acción dada en el PMI con la acción 377 ya no aplica para esta evaluación, por el traslado a la nueva sede, las condiciones tecnológicas cambiaron, aunque su vencimiento sea en mayo de 2026. Se da por cerrada la observación.
T.5.1. Separación 3 en redes	Ausencia de una separación efectiva de la red, Anexo 2 - escaneo de red 2024.			
	de acuerdo con el escaneo a la red de la entidad realizado por el equipo de la OCI, se obtuvo acceso a los diferentes segmentos de red sin restricción alguna.	Atentamente se solicita cierre de la observación, toda vez que está es sobre la infraestructura de la sede anterior (Chapinero) y a partir de agosto de 2025, la UAESP se trasladó de sede.	https://uaespd-my.sharepoint.com/:b:/g/per/sonal/osbaldo_cortes_uaesp_gov_co/EW0hrLY8La9Dgvg6qRaQdi4Bx-1IP7fUnNDlr5jCM04enQ?e=CLFk3g	Con base con las evidencias aportadas por el proceso como como fue el convenio administrativo entre UAESP-RENOBO, esta acción dada en el PMI con la acción 378 ya no aplica para esta evaluación, por el traslado a la nueva sede, las condiciones tecnológicas cambiaron, aunque su vencimiento sea en mayo de 2026. Se da por cerrada la observación
Control AD5.1.1-A17.1.1 -AD5.1.2-A17.1.2. y AD5.1.3-A17.1.3	Ausencia del plan de continuidad de negocio de TI (BCP) y plan de recuperación de desastres de TI (DRP).			

CONTROLES	DESCRIPCIÓN DE LA OBSERVACIÓN	ACCIÓN REALIZADA POR LA OTIC	EVIDENCIA	VALIDACION OCI
	El proceso no presentó evidencias sobre la implementación de estos planes y en reunión con el proceso este manifestó que estos planes se encuentran en proceso de actualización.	LA OTIC, elaboró el DRP documento que establece un conjunto de procedimientos y medidas técnicas, organizativas y operativas que permitan garantizar la continuidad de los servicios críticos de la UAESP y la recuperación efectiva de la infraestructura tecnológica y los datos institucionales ante eventos disruptivos, minimizando el impacto en la operación, asegurando la disponibilidad de los recursos y preservando la integridad y confidencialidad de la información. Plan de respaldos: La OTIC elaboró el "Plan de respaldos y recuperación de la información" La aplicación de este documento permite mitigar riesgos ante posibles interrupciones o desastres que puedan afectar la operatividad de las diferentes aplicaciones de la entidad. GTI-PC-11 V4 Gestión de respaldos: Este documento , asegurar la integridad y disponibilidad de los datos críticos que se encuentran en los servidores y repositorios de información de la Entidad. Estableciendo el paso a paso que se debe llevar a cabo ante errores irreversibles sobre las aplicaciones de la entidad. Se observa un BCP aprobado por el CIGD en diciembre del 2022 Por lo expuesto y con base en la evidencia se solicita el cierre de la observación.	https://uaespd-my.sharepoint.com/:f/g/personal/osbaldo_cortes_uaesp_gov_co/EPL_v6APW29Fhj6QakUkitQBpXUYLNIFTGnFn5w8CTobKw?email=ligia.velandia%40uaesp.gov.co&e=XW4xPK https://uaespd-my.sharepoint.com/:b/g/personal/osbaldo_cortes_uaesp_gov_co/ERmJhfO-jWpFoljgTcpxZAMBOMu92QQtfnMmZvhPkfT8_w?e=iFKSqm https://www.uaesp.gov.co/mipg/documentos-sig/gestionti/procedimientos/GTI-PC-11%20V4%20Gesti%C3%B3n%20de%20respaldos.pdf	Con base en las evidencias aportadas por el proceso respecto al BCP y al DRP, se confirma el cumplimiento en cuanto a la existencia y documentación de ambos planes. Se evidenció la ejecución de una prueba de respaldo en el servidor Veeam Backup donde se observó en el video la funcionalidad de esta restauración en aproximadamente 10 minutos; no obstante, se requiere establecer y ejecutar un plan de trabajo que permita completar las pruebas pendientes y realizar una prueba integral del DRP, con el fin de verificar su operatividad y determinar los tiempos reales de recuperación de los servicios ante una eventual contingencia, así mismo coordinar con OAP para realizar un plan de pruebas con el BCP. Se da por cerrada la observación.

Fuente- Elaboración propia

De lo anterior, es relevante mencionar especialmente al control: “**Ausencia del plan de continuidad de negocio de TI (BCP) y plan de recuperación de desastres de TI (DRP).**” que se insta al proceso a continuar la ejecución del plan de pruebas que permita verificar el cumplimiento

del DRP en su totalidad haciendo énfasis en integridad de la información. Así mismo, coordinar con OAP la actualización, realización y verificación de un plan de pruebas con el BCP. Lo anterior, con el fin de verificar su operatividad y determinar los tiempos reales de recuperación de los servicios ante una eventual contingencia.

- **Seguimiento a Recomendaciones a controles administrativos**

De las once (11) recomendaciones formuladas, se evidenció que el proceso realizó la ejecución de diversas acciones orientadas a su cumplimiento. Durante esta verificación se constató que dichas acciones fueron encaminadas a atender de manera directa las recomendaciones emitidas, así como a fortalecer y mejorar los aspectos identificados en la auditoría anterior. Se adjunta verificación y evaluación:

Tabla 3 - Seguimiento a Recomendaciones Controles Administrativos Producto Auditoría 2024

PROCESO	RECOMENDACIÓN OCI	ACCIÓN REALIZADA POR LA OTIC	EVIDENCIA	VALIDACION OCI
Control AD.1.1, AD1.2 – A.5.1.1, A.5.1.2	Contar con el acto administrativo, es decir, la resolución de la Política General de Seguridad y Privacidad de la Información y el Manual de la Política General de Seguridad y Privacidad de la Información V4 y realizar su correspondiente socialización y sensibilización a funcionarios públicos de la UAESP, a través de estrategias de comunicación que puede ser apoyada por la OACRI.	Se actualizó el manual de políticas de seguridad mediante la Resolución No 00158 de 2025. En cuanto a las capacitaciones se realizaron sensibilizaciones dirigidas a todo el personal sobre políticas y buenas prácticas de seguridad: - 8/07/2025: Ingeniería social y phishing - 16/07/2025; Buenas prácticas de correo y criptografía - 29/08/2025: Última parada de nuestro viaje de seguridad digital.	7.1 Control AD.1.1, AD1.2 –A.5.1.1, A.5.1.2	Tras la validación de las evidencias aportadas por el proceso, se confirmó el cumplimiento de la recomendación emitida, es decir, se actualizó la política de seguridad de la información con la Resolución 00158 de 2025. Las evidencias presentadas como Buenas Prácticas de Correo Electrónico, Contraseñas y Criptografía (1-16), capacitaciones dadas por la OTIC sobre buenas prácticas y phishing, que respaldan la ejecución efectiva de la acción recomendada, lo que permite dar cumplimiento dentro de la mejora continua del proceso. Cumplimiento evidenciado.

PROCESO	RECOMENDACIÓN OCI	ACCIÓN REALIZADA POR LA OTIC	EVIDENCIA	VALIDACION OCI
	software de dispositivos móviles y aplicar parches.			controles del MSPI 27001:2023.
Control AD.3.2.1-A.7.2.1	Buscar estrategias que permitan que las capacitaciones y sensibilizaciones de seguridad de la información al interior de la entidad sean más asertivas.	En cuanto a las capacitaciones se realizaron sensibilización dirigido a todo el personal sobre políticas y buenas prácticas de seguridad, phishing, entre otros. La realización de phishing controlado permite que las capacitaciones sean más asertivas, ya que se traslada un caso real de phishing a un escenario controlado donde los usuarios pueden poner en práctica el conocimiento adquirido y en caso de equivocarse realizar un curso impartido por Microsoft.	7.5 Control AD.3.2.1-A.7.2.1	Al validar las diferentes capacitaciones impartidas por el proceso en el marco del PIC, se evidenció que sí se han realizado acciones concretas en este sentido. Además, a partir de este año, se ha incorporado una evaluación de impacto dentro del PIC, la cual permite validar el asertividad de las capacitaciones realizadas. Se insta al proceso a continuar con la evaluación de impacto de las capacitaciones para asegurar su efectividad y ajustar los contenidos según los resultados obtenidos.
Control AD4.2.2-A8.2.2	Sensibilizar a los funcionarios de la entidad en el etiquetado de la información para todos los documentos que produzca la entidad con base en la matriz de activos de información definido.	De acuerdo con la capacitación del 4/06/2025 - "Actualización - Políticas de Seguridad y Privacidad de la Información" Se abordó el capítulo de gestión de activos. Adicional se actualizaron los siguientes documentos que apoyan el etiquetado de la información: - GTI-MN-02 V4 Clasificación de Activos de Información - GTI-PC-04 V5 Activos de Información.	7.6 Control AD4.2.2-A8.2.2	Dado que se evidenció las diferentes capacitaciones frente a esta recomendación, se verificó cumplimiento y ejecución de acciones sobre la recomendación dada. Lo anterior, con el objetivo de continuar y promover la mejora continua y fortalecer la sensibilización sobre el etiquetado de la información. Esto permitirá que los funcionarios apropien adecuadamente esta práctica al interior de cada proceso.
Control AD4.2.3-A8.2.3	Tener en cuenta lo establecido en la política de Backup y evitar la materialización de riesgo de pérdida de información por falta de copias de respaldo.	LA OTIC, elaboró el DRP documento que establece un conjunto de procedimientos y medidas técnicas, organizativas y operativas que permitan garantizar la continuidad de los servicios críticos de la	https://uaespdcmys.sharepoint.com/:f/g/personal/osbaldo_cortes_u_aesp_gov_co/EpL_v6APW29Fhj60akUkitQBpXUYLNIFTGnFn5w8CTobKw?email=ligia.velandia%40uaesp.gov.co&e=XW4xPK	La OTIC ha elaborado documentos importantes como el DRP, el Plan de respaldos y el procedimiento GTI-PC-11 V4, que fortalecen la continuidad operativa y la seguridad de la información. Además, se

PROCESO	RECOMENDACIÓN OCI	ACCIÓN REALIZADA POR LA OTIC	EVIDENCIA	VALIDACION OCI
		UAESP y la recuperación efectiva de la infraestructura tecnológica y los datos institucionales ante eventos disruptivos, minimizando el impacto en la operación, asegurando la disponibilidad de los recursos y preservando la integridad y confidencialidad de la información. Plan de respaldos: La OTIC elaboró el "Plan de respaldos y recuperación de la información." La aplicación de este documento permite mitigar riesgos ante posibles interrupciones o desastres que puedan afectar la operatividad de las diferentes aplicaciones de la entidad. GTI-PC-11 V4 Gestión de respaldos: Este documento, asegurar la integridad y disponibilidad de los datos críticos que se encuentran en los servidores y repositorios de información de la Entidad. Estableciendo el paso a paso que se debe llevar a cabo ante errores irreversibles sobre las aplicaciones de la entidad. La UAESP cuenta con un BCP aprobado por el CIGD en diciembre del 2022.	https://uaespdcmys.sharepoint.com/:b/g/personal/osbaldo_cortes_uaesp_gov_co/ERmJhfO-jWpFoligTcpxZAMBOMu92QQtfnMmZvhPkFT8_w?e=iFKSqm https://www.uaesp.gov.co/mipg/documentos-sig/gestioni/procedimientos/GTI-PC-11%20V4%20Gesti%C3%B3n%20de%20respaldos.pdf	cuenta con un BCP aprobado por el CIGD en diciembre de 2022. Sin embargo, no se evidencia la aplicabilidad y práctica de estos planes. Se insta al proceso a continuar la realización pruebas periódicas de recuperación y seguimiento para validar la efectividad de los planes establecidos.

PROCESO	RECOMENDACIÓN OCI	ACCIÓN REALIZADA POR LA OTIC	EVIDENCIA	VALIDACION OCI
Control AD5.2.1-A17.2.1	Contar con un esquema y sistemas redundantes que garanticen continuidad en una emergencia o falla.	Atentamente se solicita cierre de la recomendación, toda vez que esta es sobre la infraestructura de la sede anterior (Chapinero) y a partir de agosto de 2025, la UAESP se trasladó de sede.	https://uaespdcmys.sharepoint.com/:b/g/personal/osbaldo_cortes_uasp_gov_co/EW0hrLY8La9Dgvg6gRaqdi4Bx-1IP7fUnNDlr5jCM04enQ?e=CLFk3g	De acuerdo con esta sustentación dada por el proceso y con evidencia aportada, esta recomendación ya no aplica para evaluar por el cambio de sede. Este control se revisa en el marco de los nuevos controles del MSPi 27001:2023.
Control AD6.1.3-A18.1.3	Actualizar las TRD y aplicar el procedimiento de Gestión de Respaldos en su totalidad, ejemplo (pruebas de restauración)	Con relación a la actualización de las TRD de la Oficina TIC, anexo informe de las actividades realizadas durante el año 2025, que se han hecho conforme a los lineamientos del proceso de Gestión Documental de la Subdirección Administrativa y Financiera, para la organización de archivos y posterior convalidación de TRD. En cuanto a la gestión de respaldos, se elaboraron los siguientes documentos: 1 GTI-PC-11 V4 Gestión de respaldos 2 DRP - OTIC 2025 3 Plan de respaldos y recuperación de la información Y se realizó la gestión y pruebas de restauración como se observa en los informes de respaldos.	7.9 Control AD6.1.3-A18.1.3	Al validar las evidencias aportadas por el proceso, se constató la ejecución de la recomendación, lo que permite concluir que sí se realizaron acciones al interior del proceso en relación con el tema de respaldos de información. En consecuencia, se valida el cumplimiento de la recomendación, resaltando la importancia de mantener la aplicación periódica del procedimiento de gestión de respaldos para garantizar la disponibilidad y recuperación oportuna de la información institucional. Se validó la actualización de los FUID y el cumplimiento de la gestión documental. Importante que la OTIC continúe con el plan de restauraciones de la totalidad de los servicios tecnológicos que tiene la entidad, con el fin de garantizar la disponibilidad y continuidad operativa en caso de presentarse una falla, asegurando que todos los sistemas cuenten con respaldos actualizados y funcionales de manera prioritaria.

PROCESO	RECOMENDACIÓN OCI	ACCIÓN REALIZADA POR LA OTIC	EVIDENCIA	VALIDACION OCI
Control AD6.1.4-A18.1.4	Aplicabilidad de procedimientos para la protección de datos personales (PDP), y tener en cuenta la unificación de un repositorio para PDP.	El 25/06/2025 Se publicó el podcast sobre derechos de autor en el cual de manera amena se socializan los lineamientos relacionados a derecho de autor. Se socializó en el marco de la Mesa Técnica Gobierno y Seguridad Digital Abril 29, 2025: actividad GDI230 Podcast derechos de autor Julio 28, 2025: 2.3 Avances PETI - Proyecto uso y apropiación: presentación Podcast derechos de autor en la Mt - GDI230 creación muestra: Canales de Atención - sede electrónica Informe uso y apropiación - podcast Capitulo 1 Propiedad intelectual y derechos de autor	7.10 Control AD6.1.4-A18.1.4	Se evidenciaron ejercicios importantes en lo que corresponde al tema de PDP en cuanto a derechos de autor, con podcast y en el marco de mesas técnicas realizadas. Sin embargo, dado que no se evidenció lo correspondiente al control se reitera nuevamente como observación, para ser tratada por el proceso de acuerdo con el procedimiento de planes de mejoramiento de la OCI.
Control AD.6.2.3-A18.2.3	Realizar y validar planes de trabajo, para ejecutar los hallazgos y recomendaciones de los informes de PENTEST y de infraestructura.	La OTIC elabora los planes de infraestructura y las recomendaciones emitidas se verifican en reuniones de trabajo. Enlace reunión octubre	7.11 Control AD.6.2.3-A18.2.3	Se evidenció la elaboración de informes mes a mes sobre riesgos y respaldos, donde se describen las diferentes actividades desarrolladas y recomendaciones. Lo anterior evidenció seguimiento frente a la recomendación dada.

De lo anterior, se puede observar, que se desarrollaron acciones importantes para estos controles, sin embargo, para el control: “Aplicabilidad de procedimientos para la protección de datos personales (PDP)”,. Según la verificación y dado que no se evidenció la implementación de acciones frente a esta recomendación, como a lo referido frente a los procedimientos para la protección de datos personales (PDP) de acuerdo con la normatividad vigente, se reitera la necesidad de su desarrollo durante el periodo vigente, con el fin de promover la mejora continua y fortalecer la aplicabilidad de los procedimientos relacionados con la protección de datos personales (PDP). Asimismo, validar la posibilidad de contar con

un repositorio institucional para la gestión de la PDP, lo que facilitará la apropiación y cumplimiento de esta práctica por parte de los funcionarios en cada proceso.

- **Seguimiento a Recomendaciones a controles técnicos**

De las veinte siete (27) recomendaciones formuladas, se evidenció el proceso realizó la ejecución de diversas acciones orientadas a su cumplimiento por parte del proceso. Durante esta verificación se constató que dichas acciones fueron encaminadas a atender de manera directa las recomendaciones emitidas, así como a fortalecer y mejorar los aspectos identificados en la auditoría anterior. Se adjunta verificación y evaluación:

Tabla 4 - Seguimiento a Recomendaciones Controles Técnicos Producto Auditoría 2024

PROCESO	RECOMENDACIÓN OCI	ACCION REALIZADA POR LA OTIC	EVIDENCIA	VALIDACION OCI
Control T.1.1.1.1 – A.9.1.1 y T.1.1.2 – A.9.1.2	Validar la efectiva implementación y aplicación de lo establecido en la Política de Seguridad y Privacidad de la Información, así como en los procedimientos definidos por la OTIC, con relación a la política de control de acceso.	Se actualizó el manual de políticas de seguridad mediante la Resolución No 00158 de 2025. La OTIC, realizó sensibilizaciones dirigidas a todo el personal sobre políticas y buenas prácticas de seguridad: - 8/07/2025: Ingeniería social y phishing - 16/07/2025; Buenas prácticas de correo y criptografía - 29/08/2025: Última parada de nuestro viaje de seguridad digital. La OTIC tiene establecidos los roles y perfiles para los siguientes sistemas de información en cumplimiento de lo solicitado: ODOO Orfeo Run My Process Sicapital, PFET, Predis, Limay Sira	https://uaespd-my.sharepoint.com/:f:/g/personal/osbaldo_cortes_uaesp_gov_co/EvpYUbvNBCJlIipmEe0K6ZsB47nrGO3pCBRT4u4Q-JsBWQ?email=ligia.velandia%40uaesp.gov.co&e=crlxTA	Una vez validadas las evidencias allegadas por el proceso, tales como la matriz de roles y perfiles de los aplicativos, y el informe "2024 MSPI ECM-FM-06 V12 Informe de auditoría interna MSPI", se considera cumplida la recomendación dada. A partir del informe mencionado y elaborado por el proceso, se sugiere continuar con las tareas propuestas para ejecutar las acciones propuestas para cada uno de los puntos expuestos en el informe elaborado por el proceso, especialmente en lo relacionado con los roles y perfiles en los aplicativos ODOO, ORFEO, SICAPITAL y el sistema LDAP

PROCESO	RECOMENDACIÓN OCI	ACCION REALIZADA POR LA OTIC	EVIDENCIA	VALIDACION OCI
Control T.1.2.4 – A.9.2.4	Configurar el Directorio Activo y aplicaciones para que, en el primer inicio de sesión, se solicite a los usuarios el cambio de contraseña. Adicionalmente, establecer alertas que alerten a los funcionarios para realizar el cambio de contraseña dentro del plazo definido en la Política de Seguridad de la Información de la entidad.	Políticas de Seguridad y Privacidad de la Información 2025 numeral 9.6 Auditorías de derechos de acceso Auditoría Directorio Activo	7.13	Se evidencia avance en la atención de la recomendación; sin embargo, persisten oportunidades de mejora y vulnerabilidades en el Directorio Activo, por lo que se requiere atención inmediata y fortalecimiento de las acciones implementadas. Continuar con el plan de trabajo establecido por la OTIC, para mitigar las brechas al interior del proceso con la revisión de las GPOs y la reducción de cuentas con permisos administrativos, garantizando que cada usuario cuente solo con los accesos estrictamente necesarios para sus funciones.
Control T.1.3.1 – A.9.3.1	Ejecutar lo descrito en el literal C: " cambiar la información de autenticación secreta siempre que haya cualquier indicio de que se pueda comprometer la información" y en concordancia con lo descrito en el numeral 7.6.4 Lineamientos – Responsabilidades de los Usuarios para el uso de contraseñas – 5 del manual de políticas de seguridad de la información de la UAESP.	Políticas de Seguridad y Privacidad de la Información 2025 numeral 9.6 Auditorías de derechos de acceso Auditoría Directorio Activo	7.14	Con base en la política de seguridad de la información actualizada con la Resolución 158, se evidenció cumplimiento con la recomendación dada. Así mismo a través del procedimiento de gestión de incidentes.
Control T.1.4.1 – A.9.4.1	Contar con el DLP configurado y funcionando como mecanismo de protección de la información de la entidad.	Para esta recomendación no se ejecutaron acciones.	N/A	Dado que no se evidenció la implementación de acciones frente a esta recomendación, se reitera la necesidad de su desarrollo, con el fin de fortalecer la seguridad de la información y prevenir la pérdida o fuga de datos sensibles, en el marco de la mejora continua de los procesos institucionales. Se recomienda avanzar en la implementación de controles de Prevención de Pérdida de Datos (DLP: Data Loss Prevention), que permitan detectar, monitorear y mitigar posibles incidentes de exposición no autorizada de información. Esto contribuirá a reforzar la cultura de seguridad y el cumplimiento de las políticas institucionales de protección y fuga de información sensible.

PROCESO	RECOMENDACIÓN OCI	ACCION REALIZADA POR LA OTIC	EVIDENCIA	VALIDACION OCI
Control T.1.4.4 – A.9.4.5	1- Realizar las configuraciones en el directorio activo (DA), para que las políticas establecidas se ejecuten en la totalidad de los equipos de la UAESP y en lo posible en los equipos que traen los usuarios bajo la modalidad (bring your own device - BYOD).	Atentamente se solicita cierre de la recomendación, toda vez que está es sobre la infraestructura de la sede anterior (Chapinero) y a partir de agosto de 2025, la UAESP se trasladó de sede.	https://uaespd-my.sharepoint.com/:b/g/personal/osbaldo_cortes_uaesp_gov_co/EW0hrLY8La9Dgvg6qRaqdi4Bx-1IP7fUnNDlr5jCM04enQ?e=CLFk3g	De acuerdo con esta sustentación dada por el proceso y con evidencia aportada, esta recomendación ya no aplica para evaluar por el cambio de sede. Este control se revisa en el marco de los nuevos controles del MSPI 27001:2023.
	2- Realizar escaneos periódicos en búsqueda de software no autorizado e implementar las acciones necesarias para evitar su instalación local o web.	La OTI realiza la revisión del software instalado en los equipos de la UAESP, para lo cual se apoya en actividades como: Instalación agente fusioninventory: Se realizó instalación en los equipos de la Entidad, a fin de recolectar información del software instalado en cada uno de ellos. 2. Creación consulta a la base de datos: Con el fin de generar listado del software instalado en cada uno de los equipos, se creó un query directamente a la base de datos GLPI para extraer la información reportada por el agente, relacionada con el software instalado en cada uno de los equipos. 3. Depuración de listado a través de lista blanca: Con el fin de depurar la lista de software permitido, partir del listado generado se excluyeron registros de programas instalados como plugins, complementos, actualizaciones del sistema operativo y software libre permitido en la Entidad.	2	De acuerdo con las evidencias allegadas por el proceso, se evidenció la ejecución de acciones orientadas a mejorar la administración del software, destacándose la migración al sistema GLPI, dado que FusionInventory ha presentado limitaciones de eficiencia y compatibilidad con las versiones recientes de dicha plataforma. Asimismo, se encuentra en evaluación la adopción de herramientas complementarias para la gestión de activos tecnológicos. Se insta al proceso gestionar de manera oportuna la implementación del nuevo esquema de administración de activos de software, considerando los resultados de la evaluación anual de derechos de autor, con el fin de prevenir la materialización de riesgos asociados al uso o licenciamiento de software no autorizado.
Control T.2.1.1 – A.10.1.1	Implementar los lineamientos establecidos en la política prestando especial atención a la protección de los certificados y otros secretos.	políticas de seguridad 2025 (Resolución 00158) 9.9. POLÍTICA DE CONTROLES CRIPTOGRÁFICOS 9.6. POLÍTICA DE CONTROL DE ACCESO	7.17	Una vez validadas las evidencias presentadas por el proceso, se verificó en los capítulos respectivos la inclusión de lineamientos relacionados con la protección de certificados digitales.
Control T.2.1.2 – A.10.2	Implementar los lineamientos establecidos en la política prestando especial atención a la gestión de llaves y los protocolos seguros sobre la totalidad de los aplicativos expuestos a Internet.	Políticas de seguridad 2025 (Resolución 00158) 9.9. POLÍTICA DE CONTROLES CRIPTOGRÁFICOS 9.6. POLÍTICA DE CONTROL DE ACCESO	7.18	Una vez validadas las evidencias presentadas por el proceso, se verificó en los capítulos respectivos la inclusión de lineamientos relacionados con la protección de certificados digitales.

PROCESO	RECOMENDACIÓN OCI	ACCION REALIZADA POR LA OTIC	EVIDENCIA	VALIDACION OCI
Control T.3.1.1 – A.11.1.1	Fortalecer los sistemas de control de acceso sobre los activos de infraestructura crítica de TI de la entidad.	Atentamente se solicita cierre de la recomendación, toda vez que esta es sobre la infraestructura de la sede anterior (Chapinero) y a partir de agosto de 2025, la UAESP se trasladó de sede.	https://uaespd-my.sharepoint.com/:b:/g/personal/osbaldo_cortes_uaesp_gov_co/EW0hrLY8La9Dgvg6qRaqdi4Bx-1IP7fUnNDlr5jCM04enQ?e=CLFk3g	De acuerdo con esta sustentación dada por el proceso y con evidencia aportada, esta recomendación ya no aplica para evaluar por el cambio de sede. Este control se revisa en el marco de los nuevos controles del MSPI 27001:2023.
Control T.3.1.4 – A.11.1.4	1. Realizar los respaldos sobre la infraestructura y datos.	En cuanto a la gestión de respaldos, se elaboraron los siguientes documentos: 1 GTI-PC-11 V4 Gestión de respaldos 2 DRP - OTIC 2025 3 Plan de respaldos y recuperación de la información Y se realizó la gestión y pruebas de restauración como se observa en los informes de respaldos.	1 - Respaldos	De acuerdo con la evidencia documentada proporcionada por el proceso, se verificó la implementación de la recomendación relacionada con la gestión de respaldos. Esta acción contribuye directamente a la autogestión y mejora continua del proceso, fortaleciendo la seguridad de la información de la entidad
	2- Actualizar y ejecutar las pruebas correspondientes de los planes de recuperación de desastres.	Con base en el cronograma establecido se realizan y documentan las pruebas de restauración.	2 - Infome respaldos y recuperación.	La OTIC ha elaborado documentos importantes como el DRP, el Plan de respaldos y el procedimiento GTI-PC-11 V4, que fortalecen la continuidad operativa y la seguridad de la información. Además, se cuenta con un BCP aprobado por el CIGD en diciembre de 2022. Sin embargo, no se evidencia la aplicabilidad y práctica de estos planes. Se insta al proceso a continuar la realización pruebas periódicas de recuperación y seguimiento para validar la efectividad de los planes establecidos.
	3- Implementar un sistema de monitoreo centralizado para la infraestructura y redes de la entidad.	La OTIC realizó el despliegue y configuración del sistema de monitoreo Zabbix, la cual es una plataforma de código abierto utilizada para monitorizar la infraestructura de TI en tiempo real. Permite supervisar redes, servidores, máquinas virtuales, aplicaciones, bases de datos y servicios en la nube.	3 - Informe Zabbix	Con base con lo aportado por el proceso se evidenció la implementación del sistema Zabbix para el monitoreo de la infraestructura TI, lo que mejora la detección y respuesta ante incidentes. Importante, que se dé continuidad a su mantenimiento y optimización para garantizar su efectividad.
Control T.3.1.5 – A.11.1.5	Realizar intervención sobre los centros de datos de los diferentes pisos, realizando la organización y etiquetado del cableado y coordinando con SAF las mejoras locativas.	Atentamente se solicita cierre de la recomendación, toda vez que esta es sobre la infraestructura de la sede anterior (Chapinero) y a partir de agosto de 2025, la UAESP se trasladó de sede.	https://uaespd-my.sharepoint.com/:b:/g/personal/osbaldo_cortes_uaesp_gov_co/EW0hrLY8La9Dgvg6qRaqdi4Bx-1IP7fUnNDlr5jCM04enQ?e=CLFk3g	De acuerdo con esta sustentación dada por el proceso y con evidencia aportada, esta recomendación ya no aplica para evaluar por el cambio de sede.

PROCESO	RECOMENDACIÓN OCI	ACCION REALIZADA POR LA OTIC	EVIDENCIA	VALIDACION OCI
Control T.3.2.2 – A.11.2.2	Continuar con las acciones necesarias para mantener la UPS en su funcionamiento óptimo, toda vez su capacidad se encuentra en estado crítico por las baterías fuera de servicio.	Atentamente se solicita cierre de la recomendación, toda vez que esta es sobre la infraestructura de la sede anterior (Chapinero) y a partir de agosto de 2025, la UAESP se trasladó de sede.	https://uaespd-my.sharepoint.com/:b/g/personal/osbaldo_cortes_uaesp_gov_co/EW0hrLY8La9Dgvg6qRaqdi4Bx-1IP7fUnNDlr5jCM04enQ?e=CLFk3g	De acuerdo con esta sustentación dada por el proceso y con evidencia aportada, esta recomendación ya no aplica para evaluar por el cambio de sede.
Control T.3.2.3 – A.11.2.3	Revisar e intervenir las diferentes conexiones de datos y eléctricas, tanto de usuario final como la de centros de datos, verificando que cumplan con lo solicitado en el control.	Atentamente se solicita cierre de la recomendación, toda vez que está es sobre la infraestructura de la sede anterior (Chapinero) y a partir de agosto de 2025, la UAESP se trasladó de sede.	https://uaespd-my.sharepoint.com/:b/g/personal/osbaldo_cortes_uaesp_gov_co/EW0hrLY8La9Dgvg6qRaqdi4Bx-1IP7fUnNDlr5jCM04enQ?e=CLFk3g	De acuerdo con esta sustentación dada por el proceso y con evidencia aportada, esta recomendación ya no aplica para evaluar por el cambio de sede.
Control T.4.1.1 – A.12.1.1	1- Ampliar la gestión de las copias de respaldo a todas las bases de datos y aplicativos de la entidad.	En cuanto a la gestión de respaldos, se elaboraron los siguientes documentos: 1 GTI-PC-11 V4 Gestión de respaldos 2 DRP - OTIC 2025 3 Plan de respaldos y recuperación de la información 4 En el informe de Backup de Bases de datos, se documenta en el proceso de copias de BD. Y se realizó la gestión y pruebas de restauración como se observa en los informes de respaldos.	1. Copias de respaldos BD	Se evidenció por parte del proceso la implementación del procedimiento de respaldos, la actualización del Plan de Recuperación ante Desastres (DRP) y la creación, en julio de 2025, del Plan de Respaldos y Recuperación de la Información, cuyo objetivo es: “Establecer procedimientos, mejores prácticas y controles para la gestión de copias de seguridad y la recuperación oportuna y efectiva de la información en caso de incidentes, fallos técnicos, desastres o requerimientos de entes de control.” Lo anterior evidencia la ejecución de acciones concretas para atender la recomendación emitida, fortaleciendo la gestión de continuidad y disponibilidad de la información de la entidad.
	2- Establecer un sistema de monitoreo, así como realizar la gestión y análisis sobre la información de rastros de auditoría y de información de los logs de los sistemas.	La OTIC realizó el despliegue y configuración del correlacionador de eventos Wazuh, solución de ciberseguridad que recopila, gestiona y analiza datos de redes y sistemas. Su objetivo es detectar amenazas y vulnerabilidades de seguridad antes de que interrumpan las operaciones de una organización. Además, permite una respuesta rápida a incidentes de seguridad, mejorando así la protección general de la infraestructura de TI.	2. SIEM	Al validar la evidencia aportada por el proceso, se constató la implementación del correlacionador de eventos Wazuh. Esta herramienta permitió establecer acciones efectivas orientadas a contar con un sistema de monitoreo y análisis de logs.

PROCESO	RECOMENDACIÓN OCI	ACCION REALIZADA POR LA OTIC	EVIDENCIA	VALIDACION OCI
Control T.4.1.3 – A.12.1.3	Actualizar o elaborar un proceso para eliminación de información obsoleta que permita a la UAESP optimizar recursos de almacenamiento.	En la política de seguridad y privacidad de la información se establece el lineamiento para medios removibles: 9.5.2. Medios Removibles - Literal G LA OTIC realiza el proceso de borrado de información obsoleta lo que permite cumplir con las normatividad y buenas prácticas: - lista borrado seguro - Informe_tecnico_borrado de información_Rad.20251400015873 - Informe_tecnico_borrado de información	7.25	Se evidenció un informe de eliminación segura de información en discos duros de equipos dados de baja, utilizando el programa de código abierto ERASER. Esta acción se realizó en cumplimiento del instructivo GTI-IN-04 V2, específicamente en su numeral 7, relacionado con el borrado seguro de la información. Lo anterior demuestra la ejecución de acciones alineadas con la recomendación previamente establecida.
Control T.4.2.1 – A.12.2.1	1- Actualizar los documentos relacionados con la alta disponibilidad y los diagramas de red.	Atentamente se solicita cierre de la recomendación, toda vez que esta es sobre la infraestructura de la sede anterior (Chapinero) y a partir de agosto de 2025, la UAESP se trasladó de sede.	https://uaespd-my.sharepoint.com/:b:/g/personal/osbaldo_cortes_uaesp_gov_co/EW0hrLY8La9Dgvg6qRaQdi4Bx-1IP7fUnNDlr5jCM04enQ?e=CLFk3g	De acuerdo con esta sustentación dada por el proceso y con evidencia aportada, esta recomendación ya no aplica para evaluar por el cambio de sede.
	2- Establecer que los controles cubran de manera efectiva tanto a la modalidad de trabajo en sitio como trabajo remoto.	Resolución No. 537 de 2023 Por la cual se adopta la política interna de teletrabajo. Resoluciones individuales de autorización de teletrabajo como: Resolución No. 612 De 2023 Resolución No. 646 De 2023 Resolución No. 694 De 2023	2	Se evidenciaron resoluciones relacionadas con la modalidad de teletrabajo, tanto a nivel general como específicas para algunos funcionarios que actualmente la aplican.
	3- Establecer que los funcionarios con BYOD, cumplan con lo solicitado en el control al momento de conectar los equipos personales en la red de la UAESP.	Resolución No. 537 de 2023 Por la cual se adopta la política interna de teletrabajo. Resoluciones individuales de autorización de teletrabajo como: Resolución No. 612 De 2023 Resolución No. 646 De 2023 Resolución No. 694 De 2023	3	Se evidenciaron resoluciones relacionadas con la modalidad de teletrabajo, tanto a nivel general como específicas para algunos funcionarios que actualmente la aplican.
Control T.4.3.1 – A.12.3.1	Habilitar un sistema de correlación de eventos que pueda monitorear de manera efectiva los diferentes sistemas de TI con los que cuenta la entidad.	La OTIC realizó el despliegue y configuración del correlacionador de eventos Wazuh, solución de ciberseguridad que recopila, gestiona y analiza datos de redes y sistemas. Su objetivo es detectar amenazas y vulnerabilidades de seguridad antes de que interrumpan las operaciones de una organización. Además, permite una respuesta rápida a incidentes de seguridad, mejorando así la protección general de la infraestructura de TI.	7.27	Al validar la evidencia aportada por el proceso, se constató la implementación del correlacionador de eventos Wazuh. Esta herramienta permitió establecer acciones efectivas orientadas a contar con un sistema de monitoreo y análisis de logs.

PROCESO	RECOMENDACIÓN OCI	ACCION REALIZADA POR LA OTIC	EVIDENCIA	VALIDACION OCI
Control T.4.4.1 – A.12.4.1	Verificar la viabilidad de implementar de manera efectiva un sistema de prevención de pérdida de datos (DLP).	Para esta recomendación no se ejecutaron acciones.	N/A	Dado que no se evidenció la implementación de acciones frente a esta recomendación, se reitera la necesidad de su desarrollo, con el fin de fortalecer la seguridad de la información y prevenir la pérdida o fuga de datos sensibles, en el marco de la mejora continua de los procesos institucionales.
Control T.4.4.2 – A.12.4.2	Implementar un sistema de monitoreo sobre la infraestructura crítica y contar con un sistema para realizar el análisis de los logs generados.	La OTIC realizó el despliegue y configuración del correlacionador de eventos Wazuh, solución de ciberseguridad que recopila, gestiona y analiza datos de redes y sistemas. Su objetivo es detectar amenazas y vulnerabilidades de seguridad antes de que interrumpan las operaciones de una organización. Además, permite una respuesta rápida a incidentes de seguridad, mejorando así la protección general de la infraestructura de TI.	7.29	Al validar la evidencia aportada por el proceso, se constató la implementación del correlacionador de eventos Wazuh. Esta herramienta permitió establecer acciones efectivas orientadas a contar con un sistema de monitoreo y análisis de logs.
Control T.4.5.1 – A.12.5.1	Realizar las configuraciones en el servidor de actualizaciones de Windows (WSUS), para que los equipos de usuario final ejecuten las actualizaciones tanto de sistema operativo como de aplicativos.	La OTIC implementó el servicio centralizado de actualizaciones en la infraestructura de red de la entidad, mediante la instalación y configuración de Windows Server Update Services (WSUS), con el fin de reducir el consumo de ancho de banda, controlar la aplicación de parches y mejorar la seguridad en estaciones de trabajo y servidores.	7.30	De acuerdo con las evidencias que aportó el proceso se evidenció el cumplimiento en acciones para la recomendación dada, se evidenció que este servicio centralizado de actualizaciones redundaba en la optimización de consumo de ancho de banda al validar la Implementación de Windows Server Update Services (WSUS)
Control T.5.1.1 – A13.1.1	Llevar a cabo las configuraciones necesarias para implementar una segmentación efectiva de la red.	Atentamente se solicita cierre de la recomendación, toda vez que esta es sobre la infraestructura de la sede anterior (Chapinero) y a partir de agosto de 2025, la UAESP se trasladó de sede.	https://uaespd-my.sharepoint.com/:b/g/personal/osbaldo_cortes_uaesp_gov_co/EW0hrLY8La9Dgvg6qRaQdi4Bx-1IP7fUnNDlr5jCM04enQ?e=CLFk3g	De acuerdo con esta sustentación dada por el proceso y con evidencia aportada, esta recomendación ya no aplica para evaluar por el cambio de sede.
Control T.5.1.2 – A13.1.2	Llevar a cabo las configuraciones necesarias para supervisar o bloquear dispositivos no institucionales conectados a la red de la UAESP.	Atentamente se solicita cierre de la recomendación, toda vez que esta es sobre la infraestructura de la sede anterior (Chapinero) y a partir de agosto de 2025, la UAESP se trasladó de sede.	https://uaespd-my.sharepoint.com/:b/g/personal/osbaldo_cortes_uaesp_gov_co/EW0hrLY8La9Dgvg6qRaQdi4Bx-1IP7fUnNDlr5jCM04enQ?e=CLFk3g	De acuerdo con esta sustentación dada por el proceso y con evidencia aportada, esta recomendación ya no aplica para evaluar por el cambio de sede.

PROCESO	RECOMENDACIÓN OCI	ACCION REALIZADA POR LA OTIC	EVIDENCIA	VALIDACION OCI
Control T.5.2.2 – A13.2.2	Continuar con el etiquetado de la información sensible o crítica, que asegure que el significado de la etiqueta se entiende de inmediato, y que la información está protegida apropiadamente.	De acuerdo con el procedimiento de activos de información, estos se etiquetan de acuerdo con los lineamientos del manual GTI-MN-02 Clasificación de Activos de Información. De igual forma, como ayuda para los custodios y responsables de los activos el formato GTI-FM-08 Inventario de activos de información y Cuadro de caracterización documental genera las etiquetas de forma automática. Son herramientas que permiten que la etiqueta se entienda de inmediato y protegen la información.	7.33 Control T.5.5.5 - A13.2.2	Se evidenció el documento GTI-PC-04 V5 "Activos de Información" junto con el formato correspondiente para el inventario de activos de información. Sin embargo, no se observó continuidad en el proceso de etiquetado de la información sensible. Se insta al proceso a continuar con el etiquetado de la información en todos los procesos de la entidad, con el fin de garantizar la adecuada clasificación y protección de los datos sensibles.
Control T.6.1.1 – A14.1.1	Definir en los nuevos contratos de concesión que los aplicativos y sistemas de información deben contar con los requerimientos mínimos a nivel de seguridad de acuerdo con los literales del control.	La OTIC, está presente desde el área técnica para apoyar en los nuevos contratos, los requerimientos mínimos de seguridad de la información, tal y como se observa en el contrato EPISA, el cual se anexa como evidencia. En el manual de adquisición, desarrollo y mantenimiento seguro en el numeral 6, se hace énfasis en el "Acompañamiento Técnico en la Adquisición de Software"	7.34	Con base con las evidencias aportadas por el proceso se cumple para los servicios tecnológicos, sin embargo, en cuanto a los servicios de las misionales la OTIC manifestó que este se realiza a través de las interventorías.
Control T.6.1.3 – A14.1.3	- Estudiar la viabilidad de implementar firmas electrónicas o certificados digitales.	La OTIC presta acompañamiento técnico a oficinas como la SAF que, por sus funciones, debe realizar uso de certificados digitales, en su registro y uso. Adicionalmente la OTIC contrató con una empresa la adquisición de los certificados digitales HTTPS para todas las aplicaciones, lo que refuerza la postura de seguridad de la entidad.	1	De acuerdo con la información dada por el proceso en lo que hace referencia GTI-PC-13 V2 Cifrado de información, y el certificado *.uaesp.gov.c; se evidenció acciones sobre la recomendación dada.
	- Realizar el análisis tendiente a actualizar o deshabilitar el protocolo SMBv1 sin firmar.	En cumplimiento de los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y las buenas prácticas recomendadas por Microsoft, se realizó la verificación del estado del protocolo **SMB versión 1 (SMBv1)** en los servidores pertenecientes a la infraestructura institucional. El resultado es que los servidores en producción con Windows tienen este protocolo deshabilitado.	2	Con base en las evidencias presentadas por el proceso, se verificó el cumplimiento de las acciones implementadas, las cuales fueron desarrolladas de manera efectiva y ejecutadas conforme a la recomendación establecida en la auditoría.

PROCESO	RECOMENDACIÓN OCI	ACCION REALIZADA POR LA OTIC	EVIDENCIA	VALIDACION OCI
Control T.6.2.3 – A.14.2.3	Revisar y actualizar el plan de continuidad del negocio de acuerdo con las revisiones de procedimientos y control de aplicaciones críticas.	"LA OTIC, elaboró el DRP documento que establece un conjunto de procedimientos y medidas técnicas, organizativas y operativas que permitan garantizar la continuidad de los servicios críticos de la UAESP y la recuperación efectiva de la infraestructura tecnológica y los datos institucionales ante eventos disruptivos, minimizando el impacto en la operación, asegurando la disponibilidad de los recursos y preservando la integridad y confidencialidad de la información. Plan de respaldos: La OTIC elaboró el ""Plan de respaldos y recuperación de la información"" La aplicación de este documento permite mitigar riesgos ante posibles interrupciones o desastres que puedan afectar la operatividad de las diferentes aplicaciones de la entidad. GTI-PC-11 V4 Gestión de respaldos: Este documento , asegurar la integridad y disponibilidad de los datos críticos que se encuentran en los servidores y repositorios de información de la Entidad. Estableciendo el paso a paso que se debe llevar a cabo ante errores irreversibles sobre las aplicaciones de la entidad. La UAESP cuenta con un BCP aprobado por el CIGD en diciembre del 2022 Con base en la evidencia se solicita el cierre de la observación."	7.36	La OTIC ha elaborado documentos importantes como el DRP, el Plan de respaldos y el procedimiento GTI-PC-11 V4, que fortalecen la continuidad operativa y la seguridad de la información. Además, se cuenta con un BCP aprobado por el CIGD en diciembre de 2022. Por lo anterior y con base en las evidencias aportadas por el proceso respecto al BCP y al DRP, se confirma el cumplimiento en cuanto a la existencia y documentación de ambos planes. Se evidenció la ejecución de una prueba de respaldo en el servidor Veeam Backup donde se observó en el video la funcionalidad de esta restauración en aproximadamente 10 minutos; no obstante, se requiere establecer y ejecutar un plan de trabajo que permita completar las pruebas pendientes y realizar una prueba integral del DRP, con el fin de verificar su operatividad y determinar los tiempos reales de recuperación de los servicios ante una eventual contingencia, así mismo coordinar con OAP para realizar alguna plan de pruebas con el BCP. Se da por cerrada la observación. Continuar la ejecución de el plan de pruebas que permita verificar el cumplimiento del DRP en su totalidad haciendo énfasis en integridad de la información. Así mismo, coordinar con OAP la actualización, realización y verificación de un plan de pruebas con el BCP.
Control T.7.1.1 – A.16.1.1	Definir en los contratos de concesión futuros, los requerimientos para la gestión de incidentes seguridad y privacidad de la información.	La OTIC, está presente desde el área técnica para apoyar en los nuevos contratos, los requerimientos mínimos de seguridad de la información, tal y como se observa en el contrato EPISA, el cual se anexa como evidencia. En el manual de adquisición, desarrollo y mantenimiento seguro en el numeral 6, se hace énfasis en el "Acompañamiento Técnico en la Adquisición de Software"	7.37	Con base con las evidencias aportadas por el proceso se cumple para los servicios tecnológicos, sin embargo, en cuanto a los servicios de las misionales la OTIC manifestó que este se realiza a través de las interventorías.

PROCESO	RECOMENDACIÓN OCI	ACCION REALIZADA POR LA OTIC	EVIDENCIA	VALIDACION OCI
Control T.7.1.7 – A.16.1.7	Actualizar y ejecutar lineamientos de seguridad relacionados con informática forense.	La OTIC estableció los siguientes documentos, los cuales apoyan la gestión de evidencias y tratamiento de incidentes, los cuales están directamente relacionados con informática forense: GTI-PC-16 V2 Gestión de incidentes de seguridad de la información: Actividad 9, documentar las evidencias GTI-IN-03 V2 Tratamiento incidentes de seguridad de la información: Actividad 6, detección y análisis	7.38	Se evidenció la existencia de un procedimiento e instructivo para la gestión de incidentes de seguridad de la información. El proceso adelantó acciones orientadas al cumplimiento de la recomendación emitida. Se evidenció en MIPG lo correspondiente a informática forense. https://www.uaesp.gov.co/mipg/documentos-sig/gestionti/protocolos/GTI-PT-01%20V1%20Recolecci%C3%B3n%20y%20adquisici%C3%B3n%20de%20evidencia%20digital%20forense%20On%20premise.pdf y el https://www.uaesp.gov.co/mipg/documentos-sig/gestionti/protocolos/GTI-PT-02%20V1%20Recolecci%C3%B3n%20y%20adquisici%C3%B3n%20de%20evidencia%20digital%20forense%20Cloud.pdf Se insta al proceso a continuar con la apropiación y aplicabilidad del procedimiento dentro de la operación del proceso.

Fuente- Elaboración propia

De lo anterior, es relevante mencionar especialmente en los controles que no se realizaron acciones a lugar como lo es: “**Contar con el DLP configurado y funcionando como mecanismo de protección de la información de la entidad**” y “**Verificar la viabilidad de implementar de manera efectiva un sistema de prevención de pérdida de datos (DLP)** “. Es importante avanzar en la implementación de controles de Prevención de Pérdida de Datos (DLP: Data Loss Prevention), que permitan detectar, monitorear y mitigar posibles incidentes de exposición no autorizada de información. Esto contribuirá a reforzar la cultura de seguridad y el cumplimiento de las políticas institucionales de protección y fuga de información sensible.

- **Cierre de MSPI 27001_2013:**

De acuerdo con el proceso de validación efectuado por la Oficina de Control Interno sobre las observaciones y recomendaciones emitidas en el periodo anterior, se llevó a cabo la verificación del cumplimiento y avance de las acciones implementadas por el proceso de OTIC.

Como resultado de esta revisión, la OCI validó los puntos evaluados, estableciendo un **nivel de cumplimiento del 83 %**, lo que representa un **incremento del 4 %** en comparación con la evaluación realizada en 2024, cuyo resultado fue del **79 %**.

Este avance evidenció una mejora en la atención y cierre de las observaciones, así como en la consolidación de las acciones correctivas y preventivas recomendadas. Igualmente, refleja el fortalecimiento de los controles y la gestión del proceso en materia de seguridad de la información y gestión tecnológica.

En consecuencia, la evaluación se da por cerrada con un resultado favorable bajo los parámetros de la **normativa anterior (ISO/IEC 27001:2013)**, destacando el compromiso del proceso en la implementación de las medidas de mejora y en el cumplimiento de las recomendaciones formuladas por la OCI.

Tabla 5 - Evaluación Cierre MSPI con ISO 27001:2013

DOMINIO	Calificación Seguimiento OCI noviembre 2025	Calificación Seguimiento OCI noviembre 2024	EVALUACIÓN DE EFECTIVIDAD DE CONTROL 2025	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL 2024
A.5 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO	100	OPTIMIZADO
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	86	82	OPTIMIZADO	100	OPTIMIZADO
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS	100	100	OPTIMIZADO	100	OPTIMIZADO
A.8 GESTIÓN DE ACTIVOS	87	81	OPTIMIZADO	100	OPTIMIZADO
A.9 CONTROL DE ACCESO	75	70	GESTIONADO	100	GESTIONADO
A.10 CRIPTOGRAFÍA	70	70	GESTIONADO	100	GESTIONADO
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO	85	83	OPTIMIZADO	100	OPTIMIZADO
A.12 SEGURIDAD DE LAS OPERACIONES	81	77	OPTIMIZADO	100	GESTIONADO
A.13 SEGURIDAD DE LAS COMUNICACIONES	77	74	GESTIONADO	100	GESTIONADO
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	86	86	OPTIMIZADO	100	OPTIMIZADO
A.15 RELACIONES CON LOS PROVEEDORES	80	80	GESTIONADO	100	GESTIONADO
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	80	80	GESTIONADO	100	GESTIONADO

DOMINIO	Calificación Seguimiento OCI noviembre 2025	Calificación Seguimiento OCI noviembre 2024	EVALUACIÓN DE EFECTIVIDAD DE CONTROL 2025	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL 2024
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	70	50	GESTIONADO	100	GESTIONADO
A.18 CUMPLIMIENTO	87	79	OPTIMIZADO	100	GESTIONADO
CIERRE DE MSPI CON NORMA ISO/IEC 27001:2013	83	79	OPTIMIZADO	100	GESTIONADO
Nota: Esta calificación se generó con las acciones realizadas sobre observaciones y recomendaciones por el proceso a la evaluación del período anterior. Con lo cual se da cierre a esta evaluación bajo esta norma.					

Nota elaboración propia – Basado en el instrumento del MSPI

2.3. Verificación de los nuevos controles con la nueva normativa ISO/IEC 27001:2022

Con la nueva normativa se pasaron de 114 controles a 93 controles, sin embargo, se incrementaron los criterios que se debe cumplir para cada uno de los controles.

De acuerdo con lo anterior, la verificación se realizó sobre los nuevos controles establecidos en la normativa vigente desde junio de 2025, conforme a la Resolución 2277 de 2025 del MinTIC. Dado que no se ha definido una fecha específica para su implementación, la OCI procedió a validar uno a uno de estos nuevos controles y sus criterios, con el fin de verificar el avance logrado desde junio hasta la fecha. Por tal motivo, los controles fueron evaluados de manera independiente.

2.4. Controles Organizacionales

Dentro de los nuevos controles que trae la ISO 27001:2022 se incluyen tres controles de tipo organizacional: *inteligencia de amenazas, seguridad de la información para el uso de servicios en la nube y la preparación de las TIC para la continuidad del negocio (DRP-BCP)*. Estos controles buscan fortalecer la manera en que la entidad organiza, anticipa y gestiona los riesgos relacionados con la seguridad de la información. Por tal motivo, se revisaron y evaluaron estos tres controles, los cuales se describen a continuación

2.4.1. AD.1.7- A 5.7: Inteligencia de amenazas

Actualmente, se cuenta con el SIEM, pruebas pentest, gestión de incidentes, con estas evidencias, se observó que el control se encuentra etapa inicial, pero no existe un procedimiento documentado, ni definición de fuentes externas, criterios de análisis, ni mecanismos establecidos de intercambio de información. Por lo tanto, no se tiene la capacidad de anticiparse, para mitigar amenazas de nuevos riesgos y ataques que se puedan presentar. Lo anterior, representa un cumplimiento parcial del control y por qué se ve evidenció debilidad para una respuesta frente a nuevas amenazas.

Nota: Al tratarse de un control nuevo se observó fases iniciales de la implementación de este.

En conclusión, Se evidenció que la entidad no cuenta con un proceso formal de inteligencia de amenazas que incluya la identificación, análisis, contextualización y comunicación de información sobre amenazas, tal como lo requiere la ISO 27101:2022.

2.4.2. AD.1.23 - A 5.23: Seguridad de la información para el uso de servicios en la nube

Actualmente se cuenta con riesgos de seguridad de la información, matriz de roles y responsabilidades, con algunos ANS de proveedores, la entidad no cuenta con una política, lineamientos, procedimientos para incidentes en cloud, es decir, hay etapas iniciales que evidenciaron un cumplimiento parcial del control. Esto limita el cumplimiento del control y genera riesgos con la protección y administración de la información alojada en los servicios en la nube.

Nota: Al tratarse de un control nuevo, se evidenciaron únicamente las fases iniciales de su implementación. Asimismo, la diferencia entre la evaluación realizada por la OTIC y la efectuada por la OCI obedeció a que la autoevaluación del proceso se llevó a cabo en junio, mientras que la evaluación de la OCI se realizó en noviembre. Por este motivo, en este último período se identificó una mayor cantidad de evidencias.

En conclusión, Se evidenció que la entidad cuenta con un procedimiento de gestión de nube pública para aprobación; sin embargo, aún no cuenta con una Política de uso de servicios en la nube acorde con los criterios establecidos en el control.

2.4.3. AD.1.30 - A 5.30: Preparación de las TIC para la continuidad del negocio DRP-BCP

De acuerdo con la evidencia aportada por el proceso, se cuenta con el plan de recuperación de desastres —DRP-UAESP de junio de 2025—; así mismo, se cuenta con un BCP del año 2022. Sin embargo, según la nueva normativa, el proceso de Preparación de las TIC para la Continuidad del Negocio (DRP–BCP) debe contar con una definición completa y actualizada de los requisitos derivados del Análisis de Impacto al Negocio (BIA), incluyendo RTO (Recovery Time Objective: es el tiempo máximo que un servicio, sistema o proceso puede estar caído antes de causar un impacto inaceptable), RPO (Recovery Point Objective: es la cantidad máxima de información que se puede perder, medida en tiempo), capacidades, desempeño y recursos TIC necesarios para la recuperación de los servicios priorizados. Por lo tanto, el control presenta un cumplimiento parcial.

En Conclusión: Se pudo evidenciar que la entidad cuenta con los documentos para la continuidad del negocio – DRP/BCP, pero se deben complementar con: BIA (Análisis de Impacto al Negocio), Definir requisitos de continuidad específicos para TIC, Tener estrategias de continuidad de TIC, probar los planes DRP/BCP, contar con RTO y RPO en lo que corresponde a OTIC.

2.5. Controles físicos

Dentro de los controles físicos orientados a proteger las instalaciones y activos críticos se encuentra la Supervisión de la seguridad física. Este control abarca el uso de CCTV, alarmas, software de gestión, así como el registro de accesos a la data center y su monitoreo continuo. Por ello, se revisaron y evaluaron estos elementos, los cuales se describen a continuación:

2.5.1. F.1.4 - A 7.4: Supervisión de la seguridad física

El proceso allegó evidencias como el contrato RENOB0 por traslado a nueva sede, la política de seguridad de la información y el Informe_septiembre_25_UPS_control de octubre/25. Es decir, el control presenta un cumplimiento avanzado; sin embargo, se encuentran debilidades en cuanto al acceso al monitoreo, por cuanto estos corresponden al edificio y no son administrados por la OTIC.

En conclusión: El edificio de RENOB0 cuenta con sistemas de CCTV y servicios de monitoreo que apoyan la supervisión de la seguridad física. No obstante, la OTIC no cuenta con el acceso directo a los sistemas de monitoreo del edificio, lo que limita su capacidad para verificar de manera autónoma los registros y eventos asociados a la seguridad de las áreas bajo su responsabilidad.

2.6. Controles Tecnológicos

Dentro de la nueva normativa se encuentran siete (7) controles que corresponden a los controles tecnológicos, los cuales son: gestión de configuración, eliminación de información, enmascaramiento de datos y protección de datos, prevención de fuga de datos (DLP), actividades de seguimiento (monitoreo), filtrado web y codificación segura. Estos controles tienen como propósito fortalecer la protección técnica de la información y reducir los riesgos asociados al uso de los sistemas tecnológicos. En este sentido, los siete controles fueron evaluados de la siguiente manera:

2.6.1. T.1.9 - A 8.9: Gestión de la configuración

De acuerdo con las evidencias allegadas por el proceso —como el manual de hardening, el informe de riesgos de servidores on-premises, el procedimiento de gestión de usuarios GTI-PC-03 V6, el procedimiento de administración de la red de datos y comunicaciones, entre otros— se evidenció un cumplimiento parcial del control de Gestión de Configuración. Lo anterior, debido a que aún faltan algunos criterios establecidos por la norma, tales como: definir y aplicar procesos, herramientas y plantillas seguras para configurar hardware, software, servicios y redes; registrar y controlar los cambios; monitorear y revisar

periódicamente las configuraciones; proteger la información de configuración; y utilizar hardening y automatización cuando sea posible.

En conclusión: Definir procedimientos para el control de cambios de configuración para hardware, software, nube, redes y contar con plantillas estándares de configuraciones que permita unificar criterios y oportunidad de respuestas.

2.6.2. T.1.10 - A 8.10: Eliminación de información

Dadas las evidencias aportadas por el proceso, se verificó que el proceso cuenta con informes de borrado realizados mediante el software Eraser y dispone de un instructivo para la eliminación segura de información. Sin embargo, no se evidenció un proceso formalizado que cubra todos los requisitos para la eliminación segura, incluyendo la verificación independiente, trazabilidad completa, control sobre terceros y la aplicación consistente de métodos según el tipo de medio y la verificación de destrucción física, como lo estipula la norma. Por lo tanto, se evidenció un cumplimiento moderado del control, pues si bien es cierto que hay evidencias de herramientas y registros básicos, faltan lineamientos y requisitos para terceros y servicios en la nube que garanticen un proceso completo y alineado con la normativa vigente.

En conclusión: No se cuenta con un procedimiento de eliminación de información donde se contemplen aspectos como: tiempo de eliminación de información, registrar los resultados de la eliminación, evidencia de eliminación por parte de proveedores externos, requisitos de eliminación en acuerdos con terceros, configurar sistemas para destruir de forma segura la información cuando ya no se necesite, eliminar versiones obsoletas, copias y archivos temporales, usar software seguro y aprobado para eliminación permanente, contar con mecanismos adecuados según el tipo de medio de almacenamiento, verificar los métodos de eliminación del proveedor de servicios en la nube, entre otros.

2.6.3. T.1.11 - A 8.11: Enmascaramiento de datos - protección de datos

Al verificar las evidencias aportadas por el proceso, como el procedimiento de gestión de usuarios, el cifrado de información y la política de seguridad, no se evidenciaron técnicas

formales de enmascaramiento, seudonimización o anonimización. Tampoco existen mecanismos para validar su efectividad, restringir accesos según rol o garantizar la trazabilidad del tratamiento de datos sensibles. Por lo anterior, el control presenta un nivel de cumplimiento parcial.

En conclusión: Completar lo que corresponde a protección de datos sensibles y enmascaramiento, como: verificar que la anonimización o seudonimización sea efectiva, implementar técnicas de enmascaramiento de datos, restringir el acceso a los datos según el rol e implementar mecanismos de ofuscación, como lo estipula la normativa.

2.6.4. T.1.12 - A 8.12: Prevención de fuga de datos DLP

Al verificar las evidencias aportadas por el proceso como procedimiento de gestión de usuarios, cifrado de información, política de seguridad, igual como se validó en las recomendaciones dadas de la auditoría anterior, no se evidenció la implementación de acciones frente a este control (DLP), se reitera la necesidad de su desarrollo, con el fin de fortalecer la seguridad de la información y prevenir la pérdida o fuga de datos sensibles, en el marco de la mejora continua de los procesos institucionales.

En conclusión: No se evidencia mecanismos que mitiguen el riesgo de fuga o divulgación no autorizada de información personal o sensible. (DLP).

2.6.5. T.1.16 - A 8.16: Actividades de seguimiento (monitoreo)

Se evidenció que el proceso cuenta con herramientas como Zabbix, Wazuh, antimalware, proxy reverso y reportes de respaldo, entre otros, lo cual constituye un buen avance en el fortalecimiento del monitoreo y la seguridad técnica. Estas soluciones permiten detección de incidentes y control básico de la infraestructura. No obstante, aún no se cuenta con un control integral de monitoreo que abarque todos los requisitos establecidos por la nueva normativa. Por lo tanto, se evidenció cumplimiento parcial del control.

En conclusión: Como ya se cuenta con Zabbix como herramienta de monitoreo de infraestructura y con un SIEM como correlacionador de eventos, se requiere complementarlos con aspectos como: alcance y nivel de monitoreo, registros y periodos de

retención, definición de lo que se va a monitorear, detección de anomalías, respuesta a alertas y gestión de incidentes, entre otros, de acuerdo con la normativa.

2.6.6. T.1.23 - A 8.23: Filtrado web

De acuerdo con las evidencias que presentó el proceso, el control presenta un cumplimiento gestionado, ya que el proceso cuenta con medidas técnicas de protección web, tales como antimalware, certificados HTTPS, proxy reverso y políticas de navegación y seguridad. Así mismo, se contó con el cambio de firewall para el mes de septiembre, lo cual representará una mejor administración y filtrado de contenido web y denegación de servicios. También se contó con la implementación del WAF (Web Application Firewall), el cual actúa como una capa adicional de protección para las aplicaciones web al analizar y filtrar el tráfico HTTP, bloquear solicitudes maliciosas y mitigar vulnerabilidades comunes, fortaleciendo así la seguridad general del entorno web.

En conclusión: Este control se encuentra en estado gestionado y sólo se debe reforzar, actualizar y documentar la gestión de bloqueo por categorías, listas negras/blancas y el filtrado de contenido con el nuevo firewall.

2.6.7. T.1.28 - A 8.28: Codificación segura - desarrollo de software

Con las evidencias que aportó el proceso como fueron manual de desarrollo Seguro, el uso de GIT como repositorio, informes de monitoreo uso de la herramienta GIT, se evidenció un cumplimiento parcial del control, pues aún faltan implementar criterios que describe la nueva normativa.

En conclusión: Aunque existen lineamientos en el manual de desarrollo seguro y repositorio GIT, no se evidenció la implementación completa de lo establecido en el control y la nueva normatividad como: normas de codificación segura obligatorias, diseño y arquitectura seguros, incluido el modelado de amenazas, identificar vulnerabilidades de seguridad en el software, del Desarrollo Seguro de Software a lo largo de todo el ciclo de vida.

2.7. Gestión de Riesgos

La entidad cuenta con la “Política de Administración del Riesgo ¹” actualizada en septiembre de 2023, proceso liderado por la Oficina Asesora de Planeación (OAP). Esta última versión incorpora los lineamientos establecidos por la Guía V6 del Departamento Administrativo de la Función Pública (DAFP) y en cumplimiento de los requisitos de la norma ISO 9001:2015 en su numeral 6.1 en lo relacionado sobre el abordaje de los riesgos y oportunidades.

Esta política establece la manera en que la entidad debe gestionar los riesgos, entre ellos los de seguridad de la información en la UAESP. Estableciendo los siguientes pasos para la gestión de los riesgos, en la que todos los procesos de la entidad deben: identificar, analizar, valorar y dar tratamiento a los riesgos para garantizar el cumplimiento de la misión y los objetivos institucionales:

- Identificación de los riesgos.
- Definición de los controles sobre los riesgos identificados.
- Formulación de acciones para tratar el riesgo residual.
- Formulación del plan de contingencia con el objetivo de actuar de manera oportuna, respecto a la materialización de los riesgos identificados.

De acuerdo con la Oficina Asesora de Planeación (OAP) las anteriores acciones son estandarizadas en un solo formato que unifica; el mapa y plan de manejo de riesgos y oportunidades, que permite de manera eficiente, adecuada y efectiva la gestión al riesgo, mitigando el impacto de ocurrencia y definiendo planes de contingencia ante la materialización del riesgo.

Respecto al MSPI la política de Administración del Riesgo se encuentra alineada con los criterios señalados en el Manual de Políticas de Seguridad y Privacidad de la Información, que hace parte del Sistema Integrado de Gestión (SIG) de la UAESP.

La OTIC identificó los siguientes riesgos:

¹ [Política de Administración del Riesgo.pdf \(uaesp.gov.co\)](#)

Ilustración 1 - Riesgos Seguridad de la Información OTIC

Tipo	Riesgos	Controles	Acciones	Materialización
Seguridad de la información	8	13	9	0

Nota: Fuente elaboración propia

De lo anterior se puede destacar que durante la vigencia de 2025 no se materializó ningún riesgo de seguridad de la información.

Por otra parte, para futuras evaluaciones se incorporará la nueva **Guía para la Gestión Integral del Riesgo en Entidades Públicas (versión 7, agosto de 2025)**, específicamente lo dispuesto en el capítulo V, que aborda los riesgos asociados a la seguridad de la información. Este capítulo enfatiza los lineamientos para la identificación de infraestructuras críticas cibernéticas en el marco del MSPI. Actualmente, la entidad se encuentra en proceso de actualización de la política de riesgos, la cual será aplicada una vez se formalice y se socialice internamente, garantizando su alineación con la normativa vigente y las mejores prácticas en gestión del riesgo.

3. CONFORMIDADES Y FORTALEZAS, O ASPECTOS POSITIVOS ENCONTRADOS

Como resultado de este ejercicio de auditoría la OCI identificó algunas **conformidades**, **fortalezas** y **aspectos positivos** que destacan en el desempeño general evaluado. Es decir, que esto refleja el cumplimiento adecuado de las normativas y evidencian el compromiso por parte del equipo de trabajo de la OTIC en algunos puntos importantes como son:

- La OTIC realizó el respectivo autodiagnóstico del MSPI con la nueva normativa lo que generó una calificación de 74 sobre el objetivo de 100.

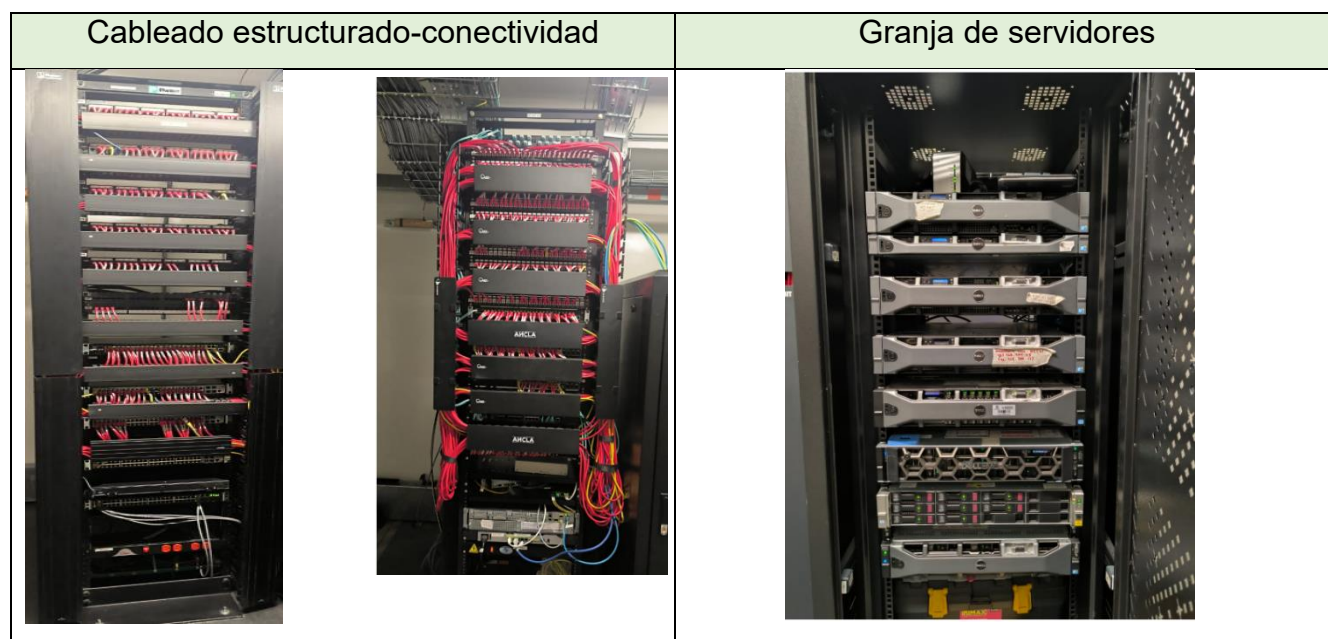
**Tabla 6 - Resultado del Autodiagnóstico del MSPI con la nueva normativa ISO
27001:2022**

No.	DOMINIO	Calificación Actual	Calificación Objetivo	Nivel de Madurez
A.5	CONTROLES ORGANIZACIONALES	72	100	GESTIONADO
A.6	CONTROLES DE PERSONAS	80	100	GESTIONADO
A.7	CONTROLES FÍSICOS	81	100	OPTIMIZADO
A.8	CONTROLES TECNOLÓGICOS	62	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		74	100	GESTIONADO

Fuente- Autodiagnóstico OTIC

- Se cuenta con la política y manual de seguridad de la información unificada y actualizada a la versión cuatro (4).
- Con el traslado a la nueva se fortaleció la infraestructura tecnológica tanto en cableado estructurado, así como en conectividad, equipos de cómputo para usuario final, y migración de algunas aplicaciones a la nube a la nube, mejorando los servicios y seguridad física de los data center.

Ilustración 2 - Evidencias nueva infraestructura TIC



Fuente – Recorrido de los centros de datos

- Se realizó el cierre oportuno de las 7 observaciones formuladas, y la OTIC ejecutó acciones sobre las 38 recomendaciones dadas con el objetivo de dar cumplimiento a las recomendaciones identificadas en la auditoría de 2024
- Para el periodo evaluado no se presentó la materialización de riesgos de seguridad y privacidad de la información.
- La OTIC ha realizado durante el año varias capacitaciones relacionadas con la seguridad y privacidad de la información, realizó un ejercicio de phishing controlado, lo que permite a los funcionarios de la entidad contar con herramientas para responder ante incidentes de seguridad.

4. OBSERVACIONES

A continuación, se enumeran las observaciones encontradas en el marco de esta auditoría:

Tabla 7 - Observaciones de la auditoría

No.	PROCESO	DESCRIPCIÓN DE LA OBSERVACIÓN
4.1	Control AD6.1.4-A18.1.4 – A.5.34	1. Aplicabilidad de procedimientos para la protección de datos personales (PDP), y tener en cuenta la unificación de un repositorio para PDP. No se evidenció la implementación de acciones frente a esta recomendación, como lo que hace referencia a los procedimientos se reitera la necesidad de su desarrollo, con el fin de promover la mejora continua y fortalecer la aplicabilidad de los procedimientos relacionados con la protección de datos personales (PDP).
4.2	Control T.4.4.1 – A.12.4.1 - Control T.4.4.1 – A.12.4.1-. T1.12 - A 8.12: Prevención de fuga de datos DLP	1. Verificar la viabilidad de implementar de manera efectiva un sistema de prevención de pérdida de datos (DLP). No se evidenció mecanismos que mitiguen el riesgo de fuga o divulgación no autorizada de información personal o sensible. (Data Loss Prevention, o Prevención de Pérdida de Datos). Es decir, no se cuenta con una herramienta configurada y funcionando como mecanismo de protección de la información sensible de la entidad.

Nota elaboración propia – Basado en el instrumento del MSPI

5. SOLICITUD DE CORRECCIÓN O ACCIONES CORRECTIVAS

Tabla 8 – 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 el nivel de avance del modelo MSPI frente a la normativa ISO 27001:2013 y los nuevos controles establecidos en la ISO 27001:2022, se concluye lo siguiente:

- A partir de la evaluación de la auditoría para el cierre del MSPI, se obtuvo un resultado del **83%**, frente al **79%** alcanzado en el período anterior. Esta evaluación se realizó con base en el instrumento definido por el MinTIC.
- Para esta vigencia el proceso realizó el autodiagnóstico con la nueva normativa y esta evaluación arrojó un resultado del 74%
- La OCI validó los 11 nuevos controles establecidos en la normativa ISO 27001:2022, obteniendo una calificación del 45%, frente al 42% alcanzado por la OTIC. La diferencia en los puntajes se debe a que la autoevaluación del proceso por parte de la OTIC se realizó en julio de 2025, mientras que la evaluación de la OCI se efectuó en noviembre de 2025, momento en el cual ya se contaba con mayores evidencias y avances en la implementación del modelo para estos nuevos controles. Los resultados de esta evaluación se encuentran en el **Anexo 1- Instrumentos de nuevos controles evaluados**.
- Dado que la evaluación abarcó controles recientemente implementados, se evidenció que la mayoría se encuentran en fases iniciales de su puesta en marcha. Este escenario implica que dichos controles aún no han alcanzado su nivel óptimo de madurez, por lo que su efectividad puede ser parcial y dependerá de ajustes y seguimiento continuo para asegurar el cumplimiento de los objetivos de control establecidos.
- Se considera prioritario designar un responsable de la seguridad de la información y otro de la protección de datos personales, con autoridad y competencias suficientes para garantizar la implementación, seguimiento y mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI). Este rol se recomienda que esté por fuera de la estructura de la OTIC, a fin de asegurar la imparcialidad en la gestión y evaluación del modelo.

7. RECOMENDACIONES

Una vez finalizado el ejercicio de auditoría la OCI presenta las siguientes recomendaciones tanto administrativas como técnicas, esto con el fin de que al interior del proceso el equipo de trabajo de OTIC priorice y ejecute las acciones necesarias para mitigar posibles materializaciones de riesgos que puedan surgir en la seguridad de la información de la entidad.

Tabla 9 - Recomendaciones a Controles Organizacionales

No.	PROCESO	RECOMENDACIÓN
7.1	AD.1.7- A 5.7 Inteligencia de amenazas	Definir, documentar y formalizar ante el SIG un procedimiento formal de inteligencia de amenazas, integrando fuentes externas confiables y estableciendo análisis y documentando de manera periódica, que complemente la información del SIEM.
7.2	AD.1.23 – A 5.23 Seguridad de la información para el uso de servicios en la nube	Definir, documentar, socializar y formalizar ante el SIG una política y procedimiento de gestión de servicios en la nube de acuerdo con los criterios establecidos con el control.
7.3	AD.1.30 - A 5.30 Preparación de las TIC para la continuidad del negocio DRP-BCP	Actualizar y formalizar los requisitos de continuidad TIC basados en los resultados del BIA y la evaluación de riesgos, definiendo RTO, RPO y capacidades de los sistemas, realizar y documentar las pruebas de DRP. Llevar a cabo la gestión necesaria para coordinar con OAP la actualización y pruebas del BCP lo que corresponde a la OTIC.

Tabla 10 - Recomendaciones a controles Físicos

No.	PROCESO	RECOMENDACIÓN
7.4	F.1.4 - A 7.4 Supervisión de la seguridad física	Validar la posibilidad de que la OTIC cuente con sus propias cámaras y/o coordinar con la administración de RENOBO el acceso a los sistemas de monitoreo del

No.	PROCESO	RECOMENDACIÓN
		edificio. Lo anterior obedece a los criterios establecidos en el control.

Tabla 11 - Recomendaciones a controles Tecnológicos

No.	PROCESO	RECOMENDACIÓN
7.5	T.1.9 - A 8.9 Gestión de la configuración	Documentar y formalizar lo que corresponde en su totalidad a la Gestión de Configuración, definiendo y aprobando plantillas estándar de configuración segura, documentando roles y responsabilidades, y estableciendo un registro centralizado con el historial de cambios.
7.6	T.1.10 - A 8.10 Eliminación de información	Formalizar y fortalecer el proceso de eliminación segura de información y garantizar que la información confidencial sea destruida de acuerdo con los periodos de retención, métodos aprobados y requisitos normativos.
7.7	T.1.11 - A 8.11 Enmascaramiento de datos protección de datos	Implementar técnicas de enmascaramiento, seudonimización o anonimización según la sensibilidad de los datos y realizar verificaciones de su efectividad. Así mismo, restringir accesos por roles para que quede la trazabilidad, esto con base en la normatividad.
7.8	T.1.12 - A 8.12 Prevención de fuga de datos DLP	Se recomienda avanzar en la implementación de controles de Prevención de Pérdida de Datos (DLP: Data Loss Prevention), que permitan detectar, monitorear y mitigar posibles incidentes de exposición no autorizada de información. Esto contribuirá a reforzar la cultura de seguridad y el cumplimiento de las políticas institucionales de protección y fuga de información sensible
7.9	T.1.16 - A 8.16 Actividades de seguimiento (monitoreo)	Formalizar e implementar el proceso de monitoreo de seguridad, con los criterios que establece el control.
7.10	T.1.23 - A 8.23 Filtrado web	Reforzar capacitaciones y/o sensibilizaciones periódicas para los funcionarios sobre la navegación web segura. Y mantener actualizados los documentos sobre bloqueos y excepciones. Así mismo, culminar con la configuración del

No.	PROCESO	RECOMENDACIÓN
		nuevo Firewall con filtrados de contenido, listas negras, blancas y los criterios establecidos en el control.
7.11	T.1.28 - A 8.28 Codificación segura	Actualizar, socializar y aplicar el proceso integral de desarrollo seguro de software, incorporando normas de codificación, modelado de amenazas, revisiones de código, uso de herramientas SAST, gestión de librerías externas y capacitación periódica al equipo de desarrollo si es necesario.

Por último, se recomienda al proceso revisar y considerar la evaluación realizada por la OCI respecto a algunas sugerencias de continuar con las acciones realizadas para las recomendaciones emitidas en el año anterior, así como las observaciones presentadas en esta evaluación sobre los nuevos controles. Es fundamental que el proceso implemente las actividades y/o acciones necesarias con el objetivo de cerrar las recomendaciones identificadas, ya que, de no hacerlo, en una próxima evaluación estas recomendaciones podrían mantenerse como observaciones, afectando el nivel de cumplimiento y madurez del sistema. La adopción oportuna de estas medidas contribuirá a fortalecer la gestión del riesgo y garantizar la mejora continua del modelo.

8. APROBACIÓN

Jefe(a) de Oficina de Control Interno

Sandra
Beatriz
Alvarado
Salcedo

Firmado
digitalmente por
Sandra Beatriz
Alvarado Salcedo
Fecha: 2025.11.28
19:44:31 -05'00'

Sandra Beatriz Alvarado Salcedo

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



Ligia M. Velandia León

FECHA 26 /11/2025