MEMORANDO

Al contestar, por favor cite el radicado:
No.:**20241100095143**
Página 1 de 2

Bogotá D.C., 28 de Noviembre de 2024

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 - 2024

Respetado ingeniero:

De conformidad con el Plan Anual de Auditorías 2024, la OCI comunica el Informe de Auditoría al Modelo de Seguridad y Privacidad de la Información de la UAESP, en el que luego de la verificación realizada, se concluyó que la implementación se encuentra en estado **"OPTIMIZADO**" respecto a la escala de calificación del instrumento del MinTIC, evidenciándose un descenso del 4% en el nivel de implementación, pasando **de 83% en el 2023 al 79% en el 2024**.

Igualmente, frente al modelo de operación del ciclo **PHVA** se evidenció que se mantiene en un porcentaje del **88%** para el 2024.

En cuanto a la madurez del modelo, se verificó que este continúa en etapa de **"DEFINIDO**" para el año 2024, es decir se mantiene igual respecto al año 2023.

Por otra parte, dentro de las mejores prácticas de Ciberseguridad definidas por el NIST, se observó una disminución en esta perspectiva pasando de un 75% a un 73%, así mismo, la puntuación obtenida para las funciones **IDENTIFICAR y PROTEGER** cuyos porcentajes fueron 81% y 77% respectivamente. Para las funciones **DETECTAR, y RESPONDER** las puntuaciones obtenidas fueron de 72% y 75% respectivamente, y en cuanto a la función de **RECUPERAR** se mantuvo en el 60%.

La auditoría identificó un descenso respecto a la evaluación del año anterior; por lo tanto, es importante que la entidad a través de la OTIC emprenda acciones prioritarias para continuar

Bogotá D.C., 28 de Noviembre de 2024

avanzando en la implementación efectiva del MSPI; es esencial que se validen y se contemplen las acciones necesarias que permitan cumplir con la implementación total del modelo de acuerdo con la normatividad vigente aplicable.

La OCI, queda atenta a la suscripción del plan de mejoramiento sobre las observaciones descritas, de acuerdo con lo establecido en el procedimiento "PC-03 PM Planes de mejoramiento V10", el cual se debe entregar 10 días hábiles después de recibido el presente informe.

En el informe anexo, podrá detallar y analizar junto con su equipo de trabajo las observaciones y recomendaciones dadas por cada uno de los dominios del MSPI, en el marco de esta auditoría interna.

Agradecemos la disposición y colaboración prestada para 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: 2024.11.28 17:54:38 -05'00'

SANDRA BEATRIZ ALVARADO SALCEDO
Jefe Oficina de Control Interno
Sandra.alvarados@uaesp.gov.co
Anexos: Informe resultados de auditoría - MSPI_2023

Anexo No 1 Evaluación MSPI – 2024

Anexo 2 - escaneo de red 2024

Anexo 3 - Informe técnico 2024

Anexo 4 Encuesta MSPI 2024

Elaboró: Osbaldo Cortés Lozano P.E.(e) – 222-24-OCI, Ligia Marlén Velandia L. P.E – 222-24 - OCI
Revisó y Aprobó: Sandra Beatriz Alvarado Salcedo – jefe Oficina OCI

CONTENIDO

Lista de Tablas

Lista de Ilustraciones

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 2024 de la Unidad Administrativa Especia 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) de la UAESP, conforme con los lineamientos del MSPI del Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC) y la Organización Internacional de Normalización (ISO) 27001:2013
ALCANCE	Verificar el nivel de madurez del SGSI vigente en la UAESP, respecto de las actuaciones adelantadas sobre los controles establecidos en el MSPI con corte a 30 de septiembre de 2024.
PERIODO DE EJECUCIÓN	Del 01/10/2024 al 30/11/2024.
EQUIPO AUDITOR	Ligia Marlén Velandia León – LMVL y Osbaldo Cortes Lozano – OCL.
DOCUMENTACIÓN ANALIZADA	• Decreto 1008 DE 2018 - Política de gobierno digital. • CONPES 3995 julio de 2020 – Política nacional de confianza y seguridad digital.

	• CONPES 3701 julio de 2011 - Lineamientos de política para ciberseguridad y ciberdefensa. • Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas - anexo 4 de 2018. • Guía para la preparación de las TIC para la continuidad del negocio – MSPI g.10. • 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. • Modelo nacional de gestión de riesgos – de seguridad de la información - Entidades Públicas. • 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 • 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 2024, la Oficina de Control Interno (OCI), llevó a cabo la auditoría al MSPI, notificada mediante Radicado No. 20241100079923 del 2 de octubre de 2024. El objetivo de esta auditoría fue verificar el avance en la implementación de los 114 controles administrativos y técnicos que conforman el SGSI en la UAESP. La evaluación se realizó siguiendo los lineamientos del MSPI, ISO 27001:2013, y los estándares de la NIST.

Durante la auditoría, se evaluaron los siguientes componentes:

1. **Controles del MSPI**: Se revisó el progreso en la implementación de los 114 controles establecidos en el MSPI.
2. **Modelo de Operación PHVA (Planear, Hacer, Verificar y Actuar)**: Se evaluó la efectividad del modelo de operación, bajo la metodología PHVA.
3. **Madurez del Modelo según Criterios del MinTIC**: Se verificó el nivel de madurez del MSPI, conforme a los criterios definidos por el MinTIC.
4. **Porcentaje de Avance sobre el Dominio Ciber**: Se analizó el progreso alcanzado en el dominio de ciberseguridad.
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 se basó en el instrumento proporcionado por el MinTIC, que permitió verificar la ejecución de los controles administrativos y técnicos del MSPI, así como medir la gestión frente a las mejores prácticas de ciberseguridad definidas por el NIST. Este análisis proporcionó un diagnóstico sobre las cinco funciones clave de seguridad: **Detectar**, **Identificar**, **Responder**, **Recuperar** y **Proteger**, alineado con los criterios de auditoría.

2.2. Verificación de los avances sobre las observaciones y recomendaciones de la auditoría MSPI - 2023

El equipo auditor realizó seguimiento a las observaciones emitidas en la auditoría del MSPI con radicado No. 20231100147563 del 30 de noviembre de 2023. Esta revisión se enfocó en validar los avances realizados hasta octubre de 2024, tomando en consideración la autoevaluación, las pruebas documentales presentadas y el nivel de cumplimiento con el Plan de Mejoramiento Interno (PMI) establecido.

De las 9 observaciones formuladas, se constató que 8 de ellas han sido cerradas, sin embargo, la acción No. 251, control T.3.1.1 perímetro de seguridad física y T.3.1.2 controles físicos de entrada, presenta reiteración, toda vez que al verificar en sitio el 28/11/2024, se observó lo siguiente:

Tabla 2 - Revisión en sitio de planta eléctrica

No.	Hallazgo	Evidencia
1	Presencia de elementos inflamables en el perímetro de seguridad de la planta eléctrica, exponiéndola a incidentes de seguridad y potencial amenaza para su integridad y el de la entidad	
2	Conexión eléctrica que no cumple con las condiciones de seguridad mínimas requeridas.	
3	Cerraduras de la planta eléctrica abiertas que presenta un daño que no permite su cierre.	

Fuente - Elaboración propia

Por lo expuesto, la OCI procedió a reabrir la observación, esperando que se tomen las medidas correctivas pertinentes.

De otra parte, en cuanto a las 32 recomendaciones formuladas al proceso, se validaron las evidencias aportadas y se constató que se realizaron mejoras a 13 recomendaciones, las demás se encuentran en ejecución por lo que se validarán en la próxima auditoría del MSPI.

2.3. Verificación de los Controles Administrativos

El equipo auditor llevó a cabo la evaluación de los controles administrativos con base en las evidencias aportadas y en el autodiagnóstico efectuado por la OTIC. El porcentaje de implementación correspondiente al año 2024 alcanzó el 79%, marcando una disminución del 4% con respecto al 83% registrado en el año 2023. A continuación, la OCI presenta un análisis general sobre cada uno de los controles:

2.3.1. A1 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN (ISO A.5)

En este aspecto, el equipo auditor verificó el cumplimiento total (100%) de la política y el manual de seguridad y privacidad de la información, los cuales han sido formalizados mediante actos administrativos internos (Res. 613/21 y Res. 491/22), y se encuentran en proceso de formalización la actualización correspondiente al año 2024, toda vez que se evidenció acta de Comité Institucional de Gestión y Desempeño (CIGD) del 22 de marzo de 2024, en el que se aprobó la Versión No. 4 de la política de seguridad de la información de la UAESP.

2.3.2. A2 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ISO A.6)

El equipo auditor observó un descenso en el desempeño de este control, con un resultado del 82%, en comparación con el 91% alcanzado en el período anterior. Este retroceso pone de manifiesto la necesidad de reforzar aspectos relacionados con la gestión de roles y responsabilidades dentro de la entidad.

En primer lugar, se identificó que el alcance de la definición de los roles y responsabilidades de los usuarios nombrados, no ha sido lo suficientemente amplia ni detallada, lo que ha

generado brechas en la cobertura de los sistemas de información. Es esencial, que esta definición sea revisada y extendida para abarcar de manera integral todos los sistemas de información que están en uso, garantizando que cada usuario tenga claramente asignadas sus responsabilidades y permisos en cada uno de ellos. De lo contrario, el riesgo de posibles inconsistencias o fallos en la seguridad podría incrementarse.

De otra parte, la OCI observó que aún persisten avances limitados en la implementación y socialización de las **Resoluciones 648 y 757 del 2023**, especialmente en lo relacionado con la gestión de proyectos de seguridad de la información. Estas resoluciones, que son fundamentales para la regulación y protección de la información, requieren un enfoque más proactivo en su difusión y aplicación en todos los niveles de la entidad. La falta de avances en este ámbito impide una correcta implementación de las mejores prácticas en seguridad de la información, así como una alineación efectiva con la normatividad.

Es importante que la entidad impulse un plan de acción que contemple la actualización y socialización de los roles y responsabilidades, así como la implementación integral de las resoluciones mencionadas. Esto no solo mejorará el control en cuestión, sino que también fortalecerá la postura de seguridad de la información y el cumplimiento normativo en la entidad.

2.3.3. A3 SEGURIDAD DE LOS RECURSOS HUMANOS (ISO A.7)

Se evidenció un cumplimiento total (100%) en este control, ya que la entidad implementó de manera efectiva los acuerdos de confidencialidad, los cuales establecen claramente las responsabilidades de seguridad y confidencialidad para todos los involucrados. Además, se incluyeron cláusulas específicas sobre seguridad y confidencialidad de la información en los contratos suscritos de prestación de servicios profesionales y de apoyo a la gestión, propendiendo que se cumplan con los estándares de seguridad de la información establecidos. Paralelamente, la entidad llevó a cabo un proceso continuo de sensibilización dirigido a los funcionarios, con el objetivo de fortalecer la cultura de seguridad de la información dentro de la entidad. Este esfuerzo busca asegurar que cada empleado comprenda y asuma plenamente su responsabilidad en la protección de la información, tanto

en el desempeño de sus funciones diarias como en el cumplimiento de las políticas y procedimientos establecidos.

2.3.4. A4 GESTIÓN DE ACTIVOS (ISO A.8)

La OCI, determinó una calificación del 81%, lo que evidenció un descenso del 2%, en relación con la evaluación anterior que fue del 83%, de lo anterior, se identificaron algunas brechas que requieren atención para asegurar la efectividad total de los procedimientos y políticas implementadas. Las principales áreas de mejora son las siguientes:

- **Capacitación especializada sobre los procedimientos de gestión de activos de información y manejo de datos reservados y clasificados**: A pesar de los avances, se observó la necesidad de fortalecer las capacitaciones dirigidas a los colaboradores en temas específicos, como los procedimientos relacionados con los activos de información y las normativas sobre la clasificación y manejo de la información sensible. El objetivo es que todo el personal comprenda y aplique correctamente estos procedimientos en su labor diaria, reduciendo el riesgo de manejo inadecuado de información crítica.
- **Gestión del conocimiento ante la rotación de personal**: La rotación de personal presenta un desafío en la continuidad del conocimiento dentro de la entidad. Si bien se han implementado medidas para mitigar este impacto, es necesario profundizar en las estrategias de transferencia de conocimiento, asegurando que los nuevos colaboradores cuenten con la información y las habilidades necesarias para mantener la eficacia de los procesos relacionados con la seguridad y gestión de la información.
- **Política de rotación y modernización de activos tecnológicos**: La obsolescencia de los activos tecnológicos es otro desafío identificado. Aunque existen proyectos en marcha, es imprescindible llevar a cabo la renovación de los activos de TI, con el fin de evitar que los equipos y sistemas se vuelvan vulnerables a riesgos de seguridad. Una estrategia más definida y un presupuesto adecuado para la modernización de los activos garantizarán un entorno tecnológico seguro y eficiente.

2.3.5. A5 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO (ISO A.17)

Este dominio presenta una calificación del 50%, lo que refleja una disminución respecto a la evaluación anterior, que obtuvo un 74%. El equipo auditor identificó varias brechas críticas que requieren atención para mejorar el nivel de cumplimiento y garantizar la continuidad operativa de la entidad. Entre los principales aspectos con oportunidad de mejora se destacan:

- **Implementación y pruebas del Plan de Continuidad del Negocio (BCP) y el Plan de Recuperación ante Desastres (DRP)**: Si bien la entidad ha elaborado estos planes, no se ha avanzado en su implementación efectiva ni en la realización de pruebas que permitan validar su efectividad en situaciones reales. Lo anterior compromete la capacidad de respuesta ante incidentes y aumenta el riesgo de interrupciones de los servicios críticos de TI.
- **Sistema redundante para servicios críticos**: Aunque la entidad ha reconocido la importancia de contar con un sistema redundante para garantizar la disponibilidad de los servicios críticos de TI, no ha implementado una infraestructura adecuada que respalde esta necesidad. La ausencia de una arquitectura de respaldo puede poner en riesgo la estabilidad de los servicios de TI en caso de fallas.

Las anteriores brechas identificadas, presentan una oportunidad de mejora, particularmente en lo que respecta a la puesta en marcha de los planes de contingencia. La entidad debe no solo formalizar y mantener actualizada la documentación del BCP y DRP, sino también implementar procesos prácticos que incluyan simulacros y pruebas regulares para asegurar la operatividad de estos planes en situaciones de emergencia. Además, es importante avanzar en la instalación de sistemas redundantes para la infraestructura on-premises, con el objetivo de asegurar la alta disponibilidad de los servicios críticos.

2.3.6. A6 CUMPLIMIENTO NORMATIVO (ISO A.18)

Este dominio presentó una calificación del 79% lo que refleja una disminución respecto a la evaluación anterior, que obtuvo un 81%. El equipo auditor identificó las siguientes oportunidades de mejora:

- **Cifrado de la información y tratamiento de datos personales**: Es necesario fortalecer los mecanismos de protección de la información sensible, garantizando que los datos personales sean adecuadamente cifrados y gestionados conforme a la normatividad vigente en materia de protección de datos personales.
- **Actualización de las Tablas de Retención Documental (TRD)**: Se recomienda llevar a cabo la actualización de las TRD, con el fin de optimizar la gestión y conservación de los documentos, asegurando que se alineen con los estándares legales y operacionales actuales.
- **Socialización del instrumento definido en la mesa de seguridad digital**: Es importante realizar una difusión y capacitación sobre el instrumento de seguridad digital adoptado por la entidad, garantizando que todo el personal esté familiarizado con su implementación y sus procedimientos.
- **Diseño y desarrollo de los planes de trabajo con las recomendaciones de las auditorías de vulnerabilidades (PENTEST)**: La OCI recomienda la elaboración de planes de trabajo sobre los resultados de las auditorías PENTEST e informes de infraestructura, que permita a la entidad priorizar y subsanar las vulnerabilidades encontradas en dichos informes, minimizando la posible materialización de riesgos.

Lo anterior permitirá mejorar el nivel de madurez y seguridad de la información del MSPI de la entidad.

2.3.7. A7 RELACIONES CON LOS PROVEEDORES (ISO A.15)

El equipo auditor evidenció una calificación del 80%, manteniéndose igual que en el período anterior. Esto indica una oportunidad de mejora en la relación con los proveedores, considerando los siguientes aspectos:

1. **Gestión de riesgos e incidentes de seguridad**: Implementar estrategias efectivas para identificar, evaluar y mitigar riesgos, así como para responder adecuadamente a incidentes de seguridad y definir en los contratos de concesión futuros, los requerimientos para la gestión de incidentes seguridad y privacidad de la información.
2. **Monitoreo y protocolos respecto a los Acuerdos de Nivel de Servicio (ANS) contractuales**: Asegurar que los ANS se cumplan mediante un monitoreo constante y la implementación de protocolos claros y efectivos.
3. **Procedimientos de verificación del cumplimiento de la política de seguridad y privacidad de información**: Establecer procedimientos rigurosos para verificar que todas las partes interesadas conozcan y cumplan con las políticas de seguridad y privacidad de la información.

Estas mejoras garantizan que todos los proveedores relacionados con la seguridad de la información cumplan con los estándares establecidos, fortaleciendo así la seguridad y la privacidad de la entidad.

En la siguiente tabla se resume el análisis presentado en cuanto a la evaluación de la OTIC en contraste con la de la OCI respectivamente para el año 2024.

Tabla 3 - Comparación controles administrativos MSPI 2023-2024

ID	Ítem	ISO	Eval. OTIC (%) 2024	Eval. OCI (%) 2024	Diferencia (%)2024	Diferencia (%)2023
1	Políticas de seguridad de la información	A.5	100	100	0	0
2	Organización de la seguridad de la información	A.6	94	82	-12	-3
3	Seguridad de los recursos humanos	A.7	100	100	0	0
4	Gestión de activos	A.8	83	81	-2	0
5	Aspectos de seguridad de la información de la gestión de la continuidad del negocio	A.17	80	50	-30	-6,5
6	Cumplimiento	A.18	81	79	-2	0
7	Relaciones con los proveedores	A.15	80	80	0	0
		Promedio	**88**	**81**	**-7**	**-2**

ID	Ítem	ISO	Eval. OTIC (%) 2024	Eval. OCI (%) 2024	Diferencia (%)2024	Diferencia (%)2023
		Diferencia 2023/2024				**-5**

Fuente - Elaboración propia

El anterior cuadro muestra el resumen de lo evaluado por la OTIC como la evaluación realizada por la OCI para la vigencia de 2024.

El detalle completo y el análisis de la evaluación se puede ver en el Anexo No. 1 Evaluación MSPI – 2024. En este sentido, se recomienda a la OTIC tener en cuenta las diversas recomendaciones que se exponen en este informe, con el fin de iniciar las acciones necesarias para reducir y corregir las brechas identificadas.

En el transcurso de esta evaluación, se observó un retroceso de 5 puntos en los controles administrativos en comparación con la evaluación realizada en el periodo anterior, lo que indica una tendencia desfavorable en el caso que no se tomen las acciones pertinentes, las cuales deben ser abordadas de manera prioritaria.

2.4. Verificación de los Controles Técnicos

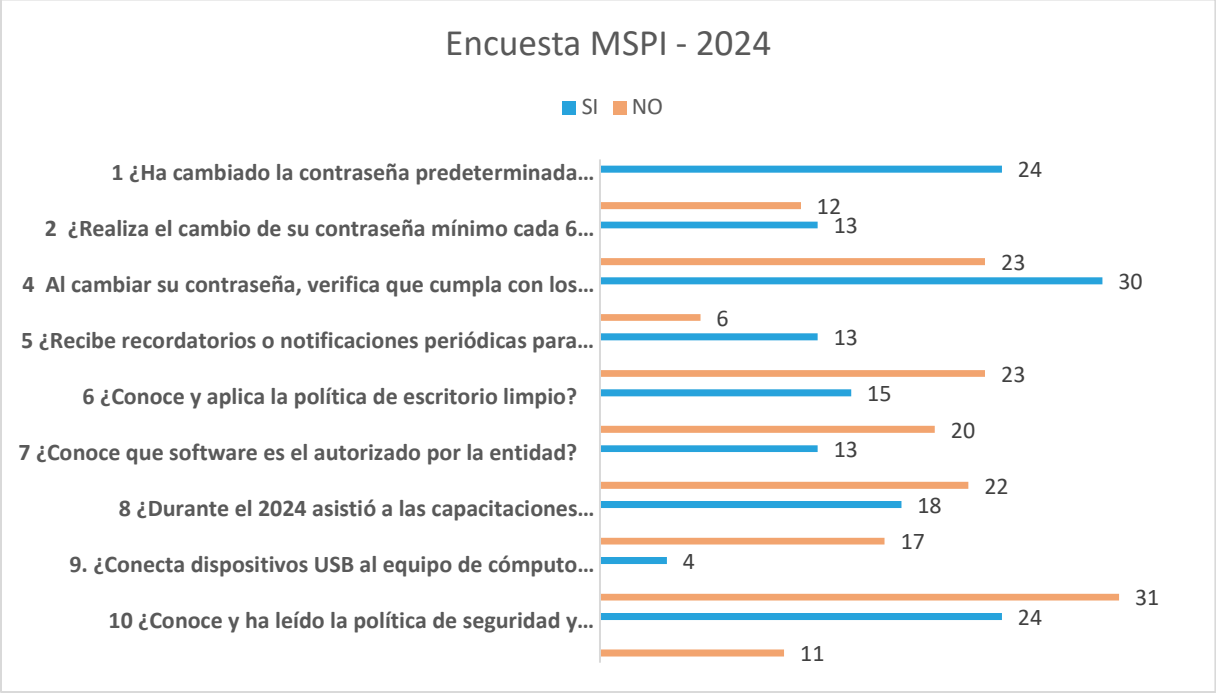
La OCI realizó una revisión del autodiagnóstico y de las evidencias proporcionadas por la OTIC, con el propósito de determinar el nivel de madurez de los controles técnicos de seguridad de la información implementados en el MSPI. A continuación, se presenta un resumen de los resultados obtenidos, los cuales pueden consultarse con mayor detalle en el el Anexo No. 1 Evaluación MSPI – 2024.

2.4.1. T.1 Control de Acceso

El proceso reportó un avance del 85 %, en contraste la OCI validó un avance del 70%, la diferencia del -15%, se encontró en los controles relacionados con la aplicación de la política de control de acceso y acceso a redes y servicios de red.

La OCI realizó una encuesta de manera anónima, compuesta de 10 preguntas a 36 colaboradores de todas las dependencias de la entidad. De estas preguntas 5 están relacionadas a la gestión de contraseñas en la entidad. Los resultados se observan en la siguiente gráfica:

Ilustración 1 Encuesta MSPI - 2024



***Nota**:* Fuente elaboración propia. Disponible en Anexo 4 Encuesta MSPI 2024

A continuación, se presenta el análisis de la encuesta sobre las preguntas relacionadas con la gestión de contraseñas:

- **Cambio de contraseñas predeterminadas:**

  Un 66.67% de los encuestados (24 de 36) cambiaron la contraseña predeterminada proporcionada por la entidad. Sin embargo, un 33.33% aún no lo ha hecho, lo que

implica un riesgo significativo de acceso no autorizado a los sistemas debido al uso de credenciales por defecto.

- **Cambio periódico de contraseñas:**

  Solo el 36.11% (13 de 36) realiza el cambio de contraseña cada seis meses, como indica la política de seguridad. Esto muestra un bajo nivel de cumplimiento con las normas internas, dejando expuesta la seguridad de las cuentas, al riesgo de ataques basados en credenciales comprometidas o ataques de tipo diccionario.

- **Cumplimiento de criterios de calidad al cambiar contraseñas:**

  El 83.33% de los encuestados (30 de 36) verifica que sus contraseñas cumplan con los criterios de calidad establecidos (longitud mínima y uso de caracteres diversos). Esto resalta el entendimiento en la implementación de contraseñas seguras.

- **Recepción de notificaciones para cambio de contraseña:**

  Solo el 36.11% (13 de 36) recibe recordatorios periódicos para cambiar sus contraseñas, lo que podría ser un factor que influya en la baja frecuencia de renovación de estas. Es fundamental implementar notificaciones automáticas y periódicas para fomentar mejores prácticas.

2.4.2. T.2 Criptografía

Este control obtuvo una evaluación del 70 % tanto por la OTIC como por la OCI, siendo el control de "Gestión de llaves" con el 60% de calificación, el que presenta mayor oportunidad de mejora.

2.4.3. T.3 Seguridad física y de entorno

El proceso reportó una calificación del 85%, contrastado con el 83% evaluado por la OCI. Los aspectos que la OCI recomienda para mejorar la calificación son:

- Realizar intervención sobre los centros de datos de los diferentes pisos, coordinando con la SAF las mejoras locativas urgentes.

- Realizar los respaldos sobre la infraestructura y datos. Actualizar, ejecutar y realizar las pruebas correspondientes de los planes de recuperación de desastres
- Implementar un sistema de monitoreo centralizado para la infraestructura y redes de la entidad.

2.4.4. T.4 Seguridad de las operaciones

Las calificaciones de la OTIC y la OCI fue del 81%. Esta calificación se debe a los siguientes factores:

- Ausencia de un sistema que permita correlacionar los eventos de los logs de los sistemas.
- Continuar con la implementación y puesta en funcionamiento de un Sistema de Prevención de Pérdida de Datos (DLP).
- Con base en el escaneo a la red de la entidad se encontraron sistemas operativos sin soporte por parte del fabricante, información que se puede consultar con mayor detalle en el Anexo 2 - escaneo de red 2024:

Tabla 4 - Sistemas Operativos fuera de soporte

#	Cantidad	SO	Versión
1	1	Windows	Server 2008
2	10	Windows	Server 2012
3	1	Windows	7
4	1	Windows	XP

Nota: Fuente elaboración propia.

2.4.5. T.5 Seguridad de las comunicaciones

Las calificaciones de la OTIC y la OCI fueron del 76%. Esta calificación se debe a los siguientes factores:

- Ausencia de una segmentación efectiva de la red de la entidad.
- Ausencia de un sistema de monitoreo de red e infraestructura crítica de TI, el cual según información de la OTIC se encuentra en fase de implementación.

- Continuar con el etiquetado de la información sensible o crítica, que asegure que el significado de la etiqueta se entienda de inmediato, y que la información está protegida apropiadamente.
- Realizar un análisis tendiente a actualizar o deshabilitar el protocolo SMBv1 sin firmar.

2.4.6. T.6 Adquisición, desarrollo y mantenimiento de sistemas

Las calificaciones de la OTIC y la OCI fueron del 87% y 84% respectivamente, con una diferencia del 3%. Esta diferencia se explica por los siguientes factores:

- Definir en los nuevos contratos de concesión que los aplicativos y sistemas de información deben contar con unos requerimientos mínimos a nivel de seguridad, de acuerdo con los literales del control.
- Estudiar la viabilidad de implementar firmas electrónicas o certificados digitales.
- Revisar y actualizar el plan de continuidad del negocio de acuerdo con las revisiones de procedimientos y control de aplicaciones críticas.
- Realizar pruebas de seguridad para todos los desarrollos antes y después de pasarlos a producción.

2.4.7. T.7 Gestión de incidentes de seguridad de la información

Las calificaciones de la OTIC y la OCI fueron del 80%. Esta calificación se debe a los siguientes factores:

- Definir en los contratos de concesión futuros, los requerimientos para la gestión de incidentes seguridad y privacidad de la información.
- Tener en cuenta los tiempos establecidos por los entes de control para asegurar la entrega oportuna de los diferentes reportes.
- Actualizar y ejecutar lineamientos de seguridad relacionados con informática forense.

En la tabla No. 5 se observa el resumen de los datos consolidados, tanto de la información entregada por la OTIC, como la información de la OCI, donde se evidenció una diferencia del - 4% debida a las causas expuestas anteriormente:

Nota: El detalle de los resultados correspondiente a la evaluación de los controles técnicos realizados por la OCI se puede consultar en el Anexo No. 1 Evaluación MSPI – 2024.

Tabla 5 - Controles Técnicos

ID	Ítem	ISO	Eval OTIC 2024	Eval OCI 2024	Diferencia
T.1	Control de acceso	A.9	85	70	-15
T.2	Criptografía	A.10	70	70	0
T.3	Seguridad física y del entorno	A.11	85	83	-2
T.4	Seguridad de las operaciones	A.12	81	77	-4
T.5	Seguridad de las comunicaciones	A.13	76	74	-2
T.6	Adquisición, desarrollo y mantenimiento de sistemas	A.14	87	86	-1
T.7	Gestión de incidentes de seguridad de la información	A.16	80	80	0
Promedio			**81**	**77**	**-4**

Nota: Elaboración propia tomado del instrumento del MSPI – MINTIC.

La OCI recomienda una revisión detallada de los hallazgos señalados en este informe y en los anexos, con especial atención a las áreas que presentan diferencias entre las evaluaciones de la OTIC y la OCI, con el fin de implementar acciones correctivas que fortalezcan el SGSI conforme a lo establecido en el MSPI.

En la siguiente tabla se observa la evolución en la implementación de los controles técnicos del MSPI de acuerdo con las auditorías realizadas por la OCI desde el año 2020 al 2024.

El promedio general de evaluación muestra una mejora significativa desde 2020 hasta 2023, pasando de 48 a 80 puntos. Sin embargo, en 2024 el promedio disminuyó a 77, marcando un retroceso de -3 puntos respecto al 2023, atribuido especialmente por el control T.1 Control de acceso.

Tabla 6 – Avance Controles Técnicos 2020 - 2024

ID	Ítem	ISO	OCI 2020	OCI 2021	OCI 2022	OCI 2023	OCI 2024	2023 Vs 2024
T.1	Control de acceso	A.9	75	76	83	84	70	1
T.2	Criptografía	A.10	30	60	70	70	70	0
T.3	Seguridad física y del entorno	A.11	69	71	76	82	83	6
T.4	Seguridad de las operaciones	A.12	41	61	82	84	77	2
T.5	Seguridad Comunicaciones	A.13	63	68	72	74	74	2
T.6	Adquisición, desarrollo y mantenimiento de sistemas	A.14	40	42	73	86	86	13
T.7	Gestión de incidentes de seguridad de la información	A.16	17	43	77	80	80	3
Promedio			**48**	**60**	**76**	**80**	**77**	**-3**

Nota: Elaboración propia tomado del instrumento del MSPI – MINTIC.

Aunque el desempeño global mejoró en el período 2020-2023, los resultados de 2024 evidencian una oportunidad de mejora. Es fundamental revisar las estrategias para mitigar el descenso en control de acceso ya que se trata de un control crítico para la integridad del SGSI.

2.5. Avance del ciclo de funcionamiento del modelo de operación (PHVA)

Para la vigencia actual, en relación con el ciclo PHVA (Planear, Hacer, Verificar y Actuar), la OCI evaluó y confirmó una calificación del 88% para el año 2024. Este resultado se mantiene consistente con la calificación obtenida en el año 2023, la cual también fue del 88%. Durante el proceso de verificación, se evidenció la actualización de algunos documentos e instrumentos importantes del MSPI. Sin embargo, algunos de ellos aún están en proceso de aprobación.

Uno de los avances más significativos durante este período ha sido la actualización y unificación de la política de seguridad y privacidad de la información, así como de su respectivo manual, que ha alcanzado la versión 4, la cual ha sido aprobadas por el Comité

Institucional de Gestión y Desempeño (CIGD). Sin embargo, para que su implementación sea oficial y operativa, aún es necesario que se emita el acto administrativo correspondiente, que se constituye como requisito indispensable para formalizar y garantizar el cumplimiento.

2.6. Evaluación de madurez del MSPI

El equipo auditor evidenció que el nivel de madurez en la implementación del MSPI se mantiene en el nivel "DEFINIDO" conforme al instrumento de medición del MinTIC. No obstante, se identificaron tres aspectos claves que han impedido avanzar al siguiente nivel de madurez, denominado "GESTIONADO CUANTITATIVAMENTE", los cuales se detallan a continuación:

1. **Planes de continuidad de negocio y de servicios**:

   Aunque estos planes se encuentran documentados, la OTIC no allegó las evidencias que respalden su implementación efectiva. En particular, se carece de pruebas documentadas satisfactorias que certifiquen la ejecución y la evaluación de la efectividad del Plan de Recuperación ante Desastres (DRP), conforme al ítem AD.5.1.1. Tras la revisión de las evidencias presentadas y la evaluación realizada, se concluye que la calificación para este control se mantiene en 60.

2. **Gestión de la seguridad en redes**

   Si bien el proceso ha definido la separación de redes a través de VLANs en el manual de políticas de seguridad y privacidad de la información, la OTIC aún debe fortalecer la gestión de seguridad en sus redes. En particular, es necesario avanzar en la segmentación efectiva de las redes. Durante la auditoría, se detectaron segmentos de red que deberían estar protegidos e inaccesibles a escaneos incluyendo dispositivos de la granja de servidores, como se puede verificar en Anexo 2 - escaneo de red 2024 (ítem T.5.1.3). La calificación de este control se mantiene en 40 debido a la necesidad de tratar esta vulnerabilidad.

3. **Desarrollo seguro de software**

   Aunque la OTIC dispone de documentación relacionada con el desarrollo seguro de software, es importante que se incorporen de manera explícita los requerimientos de seguridad para los desarrollos de software contratados externamente, tales como los realizados bajo concesiones. Este aspecto es fundamental para garantizar la seguridad en todas las fases de desarrollo y mantenimiento del software (ítem T.6.2.7). Debido a esta omisión, la calificación en este control es de 60.

A raíz de los puntos señalados, el nivel de madurez del MSPI de la entidad se mantiene en estado “Definido". Sin embargo, esta situación representa una oportunidad de mejora, ya que permite priorizar los aspectos pendientes, para avanzar al siguiente nivel de madurez. Es recomendable que la OTIC se enfoque en estos puntos críticos para optimizar la implementación del MSPI y asegurar un progreso hacia el nivel "GESTIONADO CUANTITATIVAMENTE" o “ADMINISTRADO”.

2.7. Evaluación sobre las mejores prácticas de ciberseguridad NIST.

La evaluación de este componente de ciberseguridad para esta vigencia presenta una calificación total del 73%, esto hace referencia a la implementación de las mejores prácticas en ciberseguridad definidas por NIST. Es así como se presenta una calificación para los cinco criterios de la siguiente manera:

- Detectar: presentó una calificación del 72%
- Identificar: presentó una calificación de 81%
- Proteger: presentó una calificación de 77%
- Recuperar: presentó una calificación de 60%
- Responder: presentó una calificación de 75%

De lo anterior, se puede evidenciar que se presentó una disminución en este aspecto con una calificación del 73% con relación a la evaluación anterior que obtuvo una calificación de 75%, es decir, se disminuyó en dos (2) puntos porcentuales.

2.8. Evaluación de Cumplimiento

Como resultado de la evaluación efectuada al MSPI por parte de la OCI, el modelo obtuvo una calificación cuantitativa promedio de 79%, en comparación con el 83% obtenido en la evaluación de la vigencia 2023. Esto evidenció una disminución en la ejecución de la totalidad de los controles. Esta disminución se atribuye en gran parte a que varios controles aún se encuentran en proceso de implementación y al hecho de que el traslado de sede de la entidad está latente, por lo cual, algunos de estos controles deben adaptarse a la nueva infraestructura de la futura sede, lo que implica que los controles implementados en la ubicación actual podrían cambiar o requerir ajustes significativos en el nuevo entorno.
En otras palabras, algunos de los dominios que componen el sistema se encuentran en etapas tempranas de implementación. En la siguiente gráfica se puede evidenciar el avance:

Ilustración 2 - Efectividad de Controles

No.	Evaluación de Efectividad de controles														DE CALIFICA	CALIFICACIÓN	DE CALIFICAC
	DOMINIO	DOMINIO	Calificación Seguimiento septiembre 2019	Calificación Autodiagnostico junio 2020	Calificación Seguimiento diciembre 2020	Calificación Autodiagnostico 2021	Calificación Seguimiento OCI_Octubre 2021	Calificación Autodiagnostico 2022	Calificación Seguimiento OCI_noviembre 2022	Calificación Autodiagnostico 2023	Calificación Seguimiento OCI_noviembre 2023	Calificación Autodiagnostico 2024	Calificación Seguimiento OCI_noviembre 2024	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL 2024	EVALUACIÓN DE EFECTIVIDAD DE CONTROL 2023	EVALUACIÓN DE EFECTIVIDAD DE CONTROL 2022
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	A.5 POLITICAS DE SEGURIDAD	60	70	80	100	80	100	100	100	100	100	100	100	OPTIMIZADO	OPTIMIZADO	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA	55	73	58	72	61	89	82	94	91	94	82	100	OPTIMIZADO	OPTIMIZADO	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	A.7 SEGURIDAD DE LOS RECURSOS	64	64	71	71	71	78	77	100	100	100	100	100	OPTIMIZADO	OPTIMIZADO	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	A.8 GESTIÓN DE	47	78	62	77	69	89	77	83	83	83	81	100	OPTIMIZADO	OPTIMIZADO	GESTIONADO
A.9	CONTROL DE ACCESO	A.9 CONTROL	72	79	75	69	76	70	83	86	84	85	76	100	GESTIONADO	OPTIMIZADO	OPTIMIZADO
A.10	CRIPTOGRAFÍA	A.10 CRIPTOGRA	30	40	30	60	60	60	70	70	70	70	60	100	EFECTIVO	GESTIONADO	GESTIONADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	A.11 SEGURIDAD FÍSICA Y DEL	65	73	69	71	71	80	76	86	82	85	84	100	OPTIMIZADO	OPTIMIZADO	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	A.12 SEGURIDAD DE LAS OPERACION	53	67	41	66	61	69	82	89	84	81	81	100	OPTIMIZADO	OPTIMIZADO	OPTIMIZADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	A.13 SEGURIDAD DE LAS COMUNICACIONES	56	70	63	68	68	67	72	74	74	76	76	100	GESTIONADO	GESTIONADO	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	A.14 ADQUISICIÓN, DESARROLLO Y	24	53	40	59	42	58	73	87	86	87	84	100	OPTIMIZADO	OPTIMIZADO	GESTIONADO
A.15	RELACIONES CON LOS PROVEEDORES	A.15 RELACIONES CON LOS PROVEEDOR	40	60	60	70	70	70	80	80	80	80	80	100	GESTIONADO	GESTIONADO	GESTIONADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD	20	54	17	83	43	71	77	80	80	80	80	100	GESTIONADO	GESTIONADO	GESTIONADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	A.17 ASPECTOS DE SEGURIDAD	24	54	27	44	34	34	70	80	74	80	50	100	EFECTIVO	GESTIONADO	GESTIONADO
A.18	CUMPLIMIENTO	A.18 CUMPLIMIE	54	83	61	86	71	92	76	81	81	81	79	100	GESTIONADO	OPTIMIZADO	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES			**47**	**66**	**54**	**71**	**63**	**73**	**78**	**85**	**83**	**84**	**79**	**100**	GESTIONADO	OPTIMIZADO	GESTIONADO

Nota elaboración propia – Basado en el instrumento del MSPI

2.9. 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 nuevos lineamientos establecidos por la Guía V6 del Departamento Administrativo de la Función Pública (DAFP) y en cumplimientos 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 mismos 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 su gestión, mitigando el impacto de ocurrencia y definiendo planes de contingencia ante la materialización de estos.

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

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

La OTIC identificó los siguientes riesgos:

Ilustración 3 - Riesgos OTIC

Tipo	Riesgos	Controles	Acciones	Materialización
Gestión	2	4	3	0
Corrupción	1	1	1	0
Seguridad de la información	3	8	5	0
Oportunidades	N/A	N/A	1	N/A
Totales	**6**	**13**	**10**	**0**

Nota: Fuente elaboración propia

De lo anterior se puede destacar que durante la vigencia de 2024 no se materializó ningún 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 estos reflejan 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:

- Se cuenta con la política y manual de seguridad de la información unificada y actualizada a la versión cuatro (4).
- Se fortaleció el cuarto de UPS mejorando la postura de seguridad física y de entorno.
- Se realizó el cierre oportuno de 8 observaciones sobre 9 formuladas, y frente a las recomendaciones formuladas en la auditoría del 2023, se encuentran ejecutando acciones de mejora, con el objetivo de subsanarlas.
- 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	**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. **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. **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
4.2	**T.1.1.2 Acceso a redes y a servicios en red**	**1. Ausencia de un sistema de seguimiento y monitoreo de red e infraestructura crítica de TI.** 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. **2. Topología de red desactualizada** Se evidenció que la topología de red se encuentra desactualizada.
4.3	**T.5.1.3 Separación 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 evidenció que no existe separación efectiva de la red de datos.
4.4	**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).** El proceso no presentó evidencias sobre la implementación de estos planes.

Nota elaboración propia – Basado en el instrumento del MSPI

5. SOLICITUD DE CORRECCCIÓN 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

Una vez evaluado el nivel de avance de la implementación, PHVA, madurez y Ciber del MSPI en la UAESP se concluye que:

- La evaluación de la auditoría para esta vigencia arrojó un resultado de calificación al MSPI del 79% frente al 83% del 2023, lo anterior evidenció un retroceso del 4% en lo que respecta a la seguridad y privacidad de la información de la entidad.
- La valoración de controles del modelo del MSPI continúa la clasificación en estado **OPTIMIZADO**, esto debido a la obsolescencia tecnológica y a la no aplicación de los

controles de manera oportuna, afectando la disponibilidad, integridad y confidencialidad de la información.

- El ciclo PHVA, se mantiene en un porcentaje de 88%, es decir, continúa con la misma calificación de la evaluación anterior.
- En cuanto a madurez del modelo, esta se mantiene en estado DEFINIDO, esto debido a los aspectos antes mencionados: Planes de continuidad de negocio y de servicios, Gestión de la seguridad en redes, Desarrollo seguro de software y Control de acceso.
- El componente de Ciber presentó una disminución del 2% respecto a la evaluación de 2023 que estaba en 75%, y para esta evaluación quedó en 73%.

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 Administrativos

No.	PROCESO	RECOMENDACIÓN
7.1	**Control AD.1.1, AD1.2 – A.5.1.1, A.5.1.2**	Contar con el acto administrativo 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 pueden ser apoyadas por la OACRI.

No.	PROCESO	RECOMENDACIÓN
7.2	**Control AD2.1.2-A.6.1.2.**	Definir roles y perfiles para todos los sistemas de información de la entidad, no solo para ORFEO y SI CAPITAL.
7.3	**Control AD.2.1.5-A.6.1.5**	Socializar los lineamientos establecidos en la resolución 648 de 2023, por la cual se emiten directrices de seguridad de la información en la gestión de proyectos en la UAESP y validar la aplicabilidad de los lineamientos establecidos.
7.4	**Control AD.2.2.1-A.6.2.1**	Hacer seguimiento a los lineamientos dados en el manual de la política de seguridad de la información y su aplicabilidad en lo que corresponde a Dispositivos móviles, ejemplo: d) los requisitos para las versiones de software de dispositivos móviles y aplicar parches.
7.5	**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.
7.6	**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.
7.7	**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.
7.8	**Control AD5.2.1-A17.2.1**	Contar con un esquema y sistemas redundantes que garanticen continuidad en una emergencia o falla.
7.9	**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)

No.	PROCESO	RECOMENDACIÓN
7.10	**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 estos.
7.11	**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.

Tabla 10 - Recomendaciones a controles Técnicos

No.	PROCESO	RECOMENDACIÓN
7.12	**Control T.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.
7.13	**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 avisen a los funcionarios para realizar el cambio de contraseña dentro del plazo definido en la Política de Seguridad de la Información de la entidad.
7.14	**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.

No.	PROCESO	RECOMENDACIÓN
7.15	**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.
7.16	**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). 2- Realizar escaneos periódicos en búsqueda de software no autorizado e implementar las acciones necesarias para evitar su instalación local o web.
7.17	**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.
7.18	**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.
7.19	**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.
7.20	**Control T.3.1.4 – A.11.1.4**	1. Realizar los respaldos sobre la infraestructura y datos. 2- Actualizar y ejecutar las pruebas correspondientes de los planes de recuperación de desastres. 3- Implementar un sistema de monitoreo centralizado para la infraestructura y redes de la entidad.
7.21	**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 la SAF las mejoras locativas.

No.	PROCESO	RECOMENDACIÓN
7.22	**Control T.3.2.2 – A.11.2.2**	Continuar con las acciones necesarias para mantener la UPS en su funcionamiento óptimo, toda vez que su capacidad se encuentra en estado crítico por las baterías fuera de servicio.
7.23	**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.
7.24	**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. 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.
7.25	**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.
7.26	**Control T.4.2.1 – A.12.2.1**	1- Actualizar los documentos relacionados con la alta disponibilidad y los diagramas de red. 2- Establecer que los controles cubran de manera efectiva tanto a la modalidad de trabajo en sitio como trabajo remoto. 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.
7.27	**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.

No.	PROCESO	RECOMENDACIÓN
7.28	**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).
7.29	**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.
7.30	**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.
7.31	**Control T.5.1.1 – A13.1.1**	Llevar a cabo las configuraciones necesarias para implementar una segmentación efectiva de la red.
7.32	**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.
7.33	**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.
7.34	**Control T.6.1.1 – A.14.1.1**	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.
7.35	**Control T.6.1.3 – A.14.1.3**	- Estudiar la viabilidad de implementar firmas electrónicas o certificados digitales. - Realizar el análisis tendiente a actualizar o deshabilitar el protocolo SMBv1 sin firmar.
7.36	**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.

No.	PROCESO	RECOMENDACIÓN
7.37	**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.
7.38	**Control T.7.1.7 – A.16.1.7**	Actualizar y ejecutar lineamientos de seguridad relacionados con informática forense.

8. APROBACIÓN

Sandra Beatriz Alvarado Salcedo

Firmado digitalmente por Sandra Beatriz Alvarado Salcedo
Fecha: 2024.11.28 17:25:55 -05'00'

Sandra Beatriz Alvarado Salcedo
Jefe(a) de Oficina de Control Interno

FIRMA(S)

Ligia M. Velandia León – Osbaldo Cortes Lozano
Auditor(es) Interno(s) que ejecutaron el trabajo

FECHA 29/11/2024