MEMORANDO

Al contestar, por favor cite el radicado:
No.:**20231100147563**

Bogotá D.C., 30 de Noviembre de 2023

PARA: **CESAR MAURICIO BELTRAN LOPEZ**
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 - 2023

Respetado ingeniero:

De conformidad con el Plan Anual de Auditorías 2023, 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, se puede concluir de acuerdo con la escala de valoración de efectividad de controles el Sistema de Gestión de Seguridad de la Información (SGSI) de la UAESP presenta un avance del 5% pasando **de 78% en el 2022 al 83% en el 2023**, en cumplimiento de los lineamientos de la Resolución 500 del MinTIC del 2021.

Igualmente, en cuanto al modelo de operación del ciclo **PHVA** se evidenció un avance pasando del **83%** en la vigencia 2022 al **88%** en el 2023**.**

En cuanto a la madurez del modelo se verificó que este continúa en etapa de **"DEFINIDO**" para el año 2023, es decir se mantiene con respecto al año 2022.

Por otra parte, dentro de las mejores prácticas de Ciberseguridad definidas por el NIST, se observó un avance de esta perspectiva lo cual permite que la UAESP haya avanzado de un 72% a un 75%, sobresaliendo la puntuación obtenida en las funciones **IDENTIFICAR y PROTEGER** cuyos porcentajes fueron 84% y 81% respectivamente. Para las funciones **DETECTAR, y RESPONDER** las puntuaciones obtenidas en promedio fueron de 74% y 76% respectivamente, y en cuanto a la función de **RECUPERAR** se mantuvo en el 60%.

La auditoría verificó un avance respecto a la evaluación del año anterior, pero es importante que la entidad a través de la OTIC continúe avanzando en la implementación del MSPI; por lo tanto, es

Bogotá D.C., 30 de Noviembre de 2023

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 los informes anexos 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: 2023.11.30 15:22:42 -05'00'

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

Anexos: Informe resultados de auditoría - MSPI_2023
Anexo 1: Instrumento MSPI OCI
Anexo 2: Autodiagnóstico MSPI OTIC
Anexo 3: Informe técnico
Anexo 4: Escaneo de Red

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

CONTENIDO

Lista de Tablas

1. INFORMACIÓN GENERAL DE LA AUDITORIA

Tabla 1- Información de la auditoria

ENFOQUE DE LA AUDITORIA INTERNA	• Gestión y Resultados. • Modelo de Seguridad y Privacidad de la Información (MSPI).
INFORME	Informe de la auditoría realizada al modelo de Seguridad y privacidad de la información 2023 – UAESP.
PROCESO, PROCEDIMIENTO	Oficina de tecnologías de la información y las comunicaciones - OTIC.
RESPONSABLE O AUDITADOS	Subdirector 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 Modelo de Seguridad y Privacidad de la información (MSPI) del MinTIC y la ISO 27001:2013
ALCANCE	Verificar el nivel de madurez del Sistema de Gestión de Seguridad de la Información vigente en la UAESP, respecto de las actuaciones adelantadas sobre los controles establecidos en el MSPI.
PERIODO DE EJECUCIÓN	Del 02/10/2023 al 30/11/2023.
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 en 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 y Autodiagnóstico. • Matriz de Riesgos y Oportunidades 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 vigente en la UAESP. • NORMA - NTC: ISO/IEC 27001:2013. • Resolución 500 de 2021 MINTIC.

2. DESARROLLO DE LA AUDITORIA

2.1. Planificación de la Auditoría

En cumplimiento con el Plan Anual de Auditorías para el año 2023, la Oficina de Control Interno (OCI) llevó a cabo la auditoría al Modelo de Seguridad y Privacidad de la Información (MSPI), cuya notificación fue realizada mediante Radicado No. 20231100115933 con fecha del 02 de

octubre de 2023. El objetivo de esta auditoría consistió en verificar el progreso de los 114 controles administrativos y técnicos integrados en el modelo del Sistema de Gestión de la Seguridad de la Información (SGSI) operante en la UAESP.

Esta evaluación se llevó a cabo en concordancia con los lineamientos del MSPI del Ministerio de Tecnologías de Información y las Comunicaciones (MinTIC), la normativa ISO 27001:2013, y los estándares establecidos por el Instituto Nacional de Estándares y Tecnología (NIST).

Los siguientes componentes fueron tenidos en cuenta durante el proceso:

1. Controles del MSPI: Se procedió a un análisis minucioso para evaluar el progreso en la implementación de los 114 controles establecidos en el marco del MSPI.
2. Modelo de Operación del modelo (Planear, Hacer, Verificar y Actuar - PHVA): Se evaluó la efectividad del modelo de operación, siguiendo el ciclo PHVA, para asegurar la mejora continua y eficiente del SGSI.
3. Madurez del Modelo según Criterios de MinTIC: Se realizó una evaluación detallada para determinar la madurez del modelo, conforme a los criterios definidos por el MinTIC.
4. Porcentaje de Avance sobre el Dominio Ciber: Se analizó el progreso en el dominio Ciber, asegurando un enfoque integral y efectivo hacia la seguridad de la información.
5. Evaluación, Gestión y Tratamiento de Riesgos de Seguridad de la Información: Se llevó a cabo un exhaustivo análisis de la evaluación, gestión y tratamiento de los riesgos asociados a la seguridad de la información.

La metodología de evaluación se implementó de acuerdo al instrumento suministrado por el MinTIC, el cual permitió verificar la línea base de los controles administrativos y técnicos del MSPI, así como medir el desempeño frente a las mejores prácticas en ciberseguridad definidas por el NIST. Este análisis proporcionó un diagnóstico detallado sobre las cinco funciones básicas de seguridad: Detectar, Identificar, Responder, Recuperar y Proteger, frente a los lineamientos de la política de ciberseguridad y ciberdefensa establecidos en los documentos CONPES 3701, 3994 y 3854 de acuerdo con la información presentada por la OTIC de la UAESP.

2.2. Verificación del avance sobre las observaciones de la Auditoría del MSPI - 2022

El equipo auditor realizó seguimiento a las observaciones emitidas en la auditoría del MSPI con radicado No. 0221100071243del 25 de noviembre de 2022. Esta revisión se enfocó en

validar los avances realizados hasta octubre de 2023, tomando en consideración la autoevaluación, las pruebas documentales presentadas y el nivel de cumplimiento con el Plan de Mejoramiento Interno (PMI) establecido.

De las 30 observaciones inicialmente identificadas, se constató que 25 de ellas han sido satisfactoriamente cerradas, reflejando un progreso significativo en la implementación de las acciones correctivas. En cuanto a las restantes 5 observaciones, se encuentran actualmente en proceso, indicando un compromiso continuo con la mejora y la corrección de las áreas señaladas.

Este análisis proporcionó información del estado actual de las observaciones, evidenciando compromiso en su cumplimiento, como los esfuerzos en curso para abordar de manera efectiva los aspectos pendientes. Además, se destaca el compromiso de la OTIC con la actualización y seguimiento del Plan de Mejoramiento Interno (PMI).

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 2023 alcanzó el 83%, marcando aumento del 5% con respecto al 78% registrado en el año 2022. A continuación, la OCI presenta un análisis detallado 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 del (100%) con la política y el manual de seguridad y privacidad de la información debidamente formalizadas mediante actos administrativos internos (Res. 613/21, Res. 491/22) y en proceso de formalización la actualización de 2023.

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

El equipo auditor verificó un importante avance en este control llegando al 91%. Falta ampliar el alcance en la definición de los roles y responsabilidades de los usuarios nombrados, de tal forma que cubra la totalidad de los sistemas de información activos. Igualmente falta avanzar

en la implementación y socialización de la Resolución 648 del 2023 sobre la gestión de proyectos de seguridad de la información.

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

Se evidenció el cumplimiento completo sobre este dominio (100%) ya que los acuerdos de confidencialidad se encuentran implementados, así como la inclusión de obligaciones sobre seguridad y confidencialidad a los contratistas y sensibilización continua a los funcionarios para toma de conciencia de la seguridad de la información en el cumplimiento de sus funciones.

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

La OCI, evidenció un avance del (83%) en este dominio, prevaleciendo algunas brechas como son: capacitaciones focalizadas sobre los procedimientos de los activos de información y del manejo de la información reservada y clasificada, la gestión del conocimiento por rotación de personal, y la política de rotación y modernización de activos para evitar obsolescencia.

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

Este dominio presenta un avance del (74%), el equipo auditor verificó que sobresalen brechas como; implementación y pruebas del BCP, toda vez que en los informes de seguimiento al proceso se verificó que no se ejecutaron las pruebas en su totalidad. Mejorar la gestión oportuna de incidentes. Se evidenció una oportunidad de mejora en el BCP y DRP, toda vez que la entidad cuenta con la documentación más no con la implementación.

2.3.6. A6 CUMPLIMIENTO NORMATIVO (ISO A.18).

El equipo auditor evidenció el 81% de avance Este dominio presenta oportunidad de mejora sobre los siguientes aspectos: cifrado de la información y tratamiento de datos personales, actualización de las TRD, socialización en la entidad del instrumento definido en la mesa de seguridad digital, y el diseño y desarrollo de los planes de auditorías de vulnerabilidades e infraestructura.

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

El equipo auditor evidenció el 80% de avance, evidenciándose una oportunidad de mejora sobre la relación con los proveedores que tengan en cuenta los siguientes aspectos: gestión de riesgos e incidentes de seguridad, monitoreo y protocolos respecto a los Acuerdos de Nivel de Servicio (ANS) contractuales, y los procedimientos de verificación del cumplimiento de la política de seguridad y privacidad de información.

En la siguiente tabla se resume el análisis presentado en cuanto a la evaluación de la OTIC y los de la OCI respectivamente para el año 2023.

Tabla 2 - Controles Administrativos

ID	Ítem	ISO	Eval. OTIC (%) 2023	Eval. OCI (%) 2023	Diferencia (%)
A1	Políticas de seguridad de la información	A.5	100	100	0
A2	Organización de la seguridad de la información	A.6	94	91	-3
A3	Seguridad de los recursos humanos	A.7	100	100	0
A4	Gestión de activos	A.8	83	83	0
A5	Aspectos de seguridad de la información de la gestión de la continuidad del negocio	A.17	80	73,5	-6,5
A6	Cumplimiento	A.18	81	81	0
A7	Relaciones con los proveedores	A.15	80	80	0
		Promedio	**88**	**86**	**-2**

Nota: Elaboración propia

El detalle y análisis de las evaluaciones se puede consultar en el anexo No. 2 Evaluación MSPI - 2023/OTIC y el anexo No. 1 Evaluación MSPI – 2023/OCI. De otra parte, se invita a la OTIC

a tener presente las diferentes recomendaciones que se describen en el anexo correspondiente para que se inicien las acciones para minimizar estas diferencias.

Igualmente, es importante ilustrar el avance que ha tenido la implementación del modelo de seguridad y privacidad de la información – MSPI en la entidad bajo el direccionamiento de la Oficina de TI con el apoyo de la alta dirección. A continuación, en la siguiente tabla se presenta el avance que se ha dado en la implementación de los controles administrativos del MSPI de acuerdo con las auditorías realizadas por la OCI desde el año 2020 al 2023:

Tabla 3 - Avance controles administrativos MSPI 2020-2023

ID	ITEM	ISO	Eval. OCI (%) 2020	Eval. OCI (%) 2021	Eval. OCI (%) 2022	Eval. OCI (%) 2023	Avance (%) 2022 vs. 2023
A1	Políticas de seguridad de la información	A.5	80	80	100	100	0
A2	Organización de la seguridad de la información	A.6	58	61	82	91	+9
A3	Seguridad de los recursos humanos	A.7	71	71	77	100	+23
A4	Gestión de activos	A.8	62	69	77	83	+6
A5	Aspectos de seguridad de la información de la gestión de la continuidad del negocio	A.17	26,5	33,5	70	73,5	+3,5
A6	Cumplimiento	A.18	61	71	76	81	+5
A7	Relaciones con los proveedores	A.15	60	70	80	80	0
		Promedio	**58**	**64**	**78**	**86**	**+8**

Nota: Elaboración propia

Con base en la tabla anterior, la Oficina de control interno verificó un avance considerable en la implementación del MSPI pasando de 78% del 2022 al 83% en el 2023.

Nota: El detalle de los resultados correspondiente a la evaluación de los controles administrativos realizada por la OCI se puede consultar en el anexo No. 1 - Evaluación OCI

2.4 Controles Técnicos

Para evaluar el cumplimiento del MSPI, el equipo auditor llevó a cabo una revisión del autodiagnóstico realizado y de las evidencias proporcionadas por la OTIC con el objetivo de medir el nivel de madurez de los controles técnicos de seguridad de la información. A continuación, se presenta de manera resumida los resultados obtenidos durante este ejercicio:

2.4.1 T.1 Control de acceso

El proceso reportó un avance del 86% y la OCI verificó un avance del 84%, la diferencia se encuentra en unos controles relacionados con la administración de contraseñas.

2.4.2 T.2 Criptografía

Este ítem obtuvo una evaluación del 70%, siendo el control de "Gestión de llaves" el que presenta menor ejecución, según las evaluaciones tanto de la OTIC como de la OCI.

2.4.3 T.3 Seguridad Física y de entorno

El proceso reportó un avance del 86%, contrastado con el 82% evaluado por la OCI. La diferencia se atribuye a la no conformidad en el control de acceso físico al cuarto y planta eléctrica de la entidad.

2.4.4 T.4 Seguridad de las operaciones

Las calificaciones de la OTIC y la OCI fueron del 89% y 84%, respectivamente, con una diferencia del 5%. Esta diferencia se explica por la ausencia de un sistema que permita correlacionar los eventos de los sistemas, la caída del sistema de monitoreo de red y la fase

de aprendizaje en la que se encuentra la implementación del Sistema de Prevención de Pérdida de Datos (DLP).

2.4.5 T.5 Seguridad de las Comunicaciones

Este ítem obtuvo una calificación del 74%, evidenciando un rezago significativo. La OCI enfatiza la necesidad prioritaria de reforzar el control de separación de redes, contar con los diagramas de red actualizadas y realizar el monitoreo de redes.

2.4.6 T.6 Adquisición, desarrollo y mantenimiento de sistemas

El proceso informó un avance del 87%, contrastado con el 86% evaluado por la OCI. La diferencia se explica, entre otros aspectos, por la falta de supervisión y seguimiento de los desarrollos de software de los concesionarios de la entidad, así como por modificaciones en los cronogramas de desarrollo de software que han ocasionado atrasos.

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

Este ítem obtuvo una calificación del 80%. Siendo la respuesta ágil y efectiva a los incidentes de seguridad, el control que se debe reforzar desde el proceso.

En la tabla No. 4 se observa el resumen de los datos consolidados, tanto de la información entregada por la OTIC y la OCI, donde se evidencia una diferencia del 2% debida a las causas expuestas anteriormente:

Nota: El detalle de los resultados correspondiente a la evaluación de los controles técnicos realizada por la OCI se puede consultar en el anexo No. 1 - Evaluación OCI.

Tabla 4 - Controles Técnicos

ID	Ítem	ISO	Eval OTIC 2023	Eval OCI 2023	Diferencia
T.1	Control de acceso	A.9	86	84	-2
T.2	Criptografía	A.10	70	70	0
T.3	Seguridad física y del entorno	A.11	86	82	-4
T.4	Seguridad de las operaciones	A.12	89	84	-5

ID	Ítem	ISO	Eval OTIC 2023	Eval OCI 2023	Diferencia
T.5	Seguridad de las comunicaciones	A.13	74	74	0
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			**82**	**80**	**-2**

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

El detalle de las evaluaciones se puede consultar el anexo No. 2 Evaluación MSPI - 2023/OTIC y el anexo No. 1 Evaluación MSPI – 2023/OCI.

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 2023:

Tabla 5 - Avance controles técnicos MSPI 2020-2023

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

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

De acuerdo a la anterior información, se observa la evolución en la implementación de los controles técnicos, pasando del 48% en 2020 al 80% en 2023. Este análisis detallado revela que el control de "Criptografía" se destaca como el dominio con mayor rezago en su implementación.

Al comparar los resultados entre los años 2022 y 2023, se nota un avance consolidado del 4%, evidenciando mejoras en diversos aspectos del Sistema de Gestión de la Seguridad de la Información (SGSI). Es importante resaltar que el dominio "Adquisición, desarrollo y mantenimiento de sistemas" se distingue por registrar el mayor nivel de avance, experimentando un incremento del 13% con respecto al año anterior.

Este análisis comparativo subraya no solo la mejorar en el nivel de implementación del MSPI a lo largo del tiempo, sino también la identificación de áreas específicas que requieren mayor

atención y priorización. La información recolectada por la OCI en las auditorías al MSPI ofrece una visión clara de los avances y áreas de enfoque para la mejora continua del SGSI.

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

Para esta vigencia, respecto al ciclo PHVA (Planear, Hacer, Verificar y Actuar), la OCI, verificó una calificación para el 2023 del 88%, lo que representa un avance 5 puntos con base en la calificación otorgada en el 2022 que fue del 83%. Se evidenció la elaboración de diferentes documentos e instrumentos, otros se encuentran en proceso de aprobación y socialización, como lo la actualización de la política y manual de la políticas de seguridad y privacidad de la información en su versión 4.

2.6 Evaluación de madurez del MSPI.

En esta auditoria se evidenció un avance en el nivel de madurez de la implementación del MSPI, aunque se mantiene en el nivel DEFINIDO de acuerdo con el instrumento de medición del MinTIC, hay tres aspectos que no permitieron avanzar al siguiente nivel de madurez “GESTIONADO CUANTITATIVAMENTE” como son:

- Los planes de continuidad de negocio y de servicios: Si bien están documentados la OTIC no cuenta con suficientes evidencias de su implementación, pruebas documentadas satisfactorias y evaluación de la efectividad del DRP (ítem AD.5.1.1). De acuerdo con las evidencias allegadas y la evaluación realizada la calificación es 60.
- Si bien el proceso cuenta con la definición de la separación de redes a través de VLANs en el manual de políticas de seguridad y privacidad de la información, la OTIC debe seguir trabajando en la segmentación efectiva de las redes, toda vez que el equipo auditor al realizar un escaneo fue posible ver todos los equipos conectados a la red inclusive los de la granja de servidores anexo 4 – Escaneo de Red (ítem T.5.1.3). La calificación de este control es 40.
- Si bien la OTIC cuenta con documentación relacionada al de desarrollo seguro software, el 14 de marzo de 2023, se presentó un incidente de seguridad causado por obsolescencia tecnológica el cual ocasionó la perdida de algunos ambientes de

desarrollo y perdida de información. (ítem T.6.2.6), por esta razón la calificación es 80 en contraste con el 100 de la autoevaluación del proceso.

Por las razones expuestas, el nivel de madurez del MPSI de la entidad se mantiene en estado “Definido”. Esta situación ofrece una oportunidad de mejora para el proceso, permitiendo priorizar los aspectos que han impedido avanzar al siguiente nivel.

2.7 Evaluación sobre las mejores prácticas de ciberseguridad NIST.

La evaluación de la perspectiva de ciberseguridad permitió concluir que la UAESP avanzó de un 72% a un 75% en la implementación de las mejores prácticas en ciberseguridad definidas por el NIST. Sobresale la puntuación obtenida en las funciones IDENTIFICAR y PROTEGER cuyos porcentajes fueron 84% y 81% respectivamente. Para las funciones DETECTAR y RESPONDER la puntuación obtenida en promedio fue de 74% y 76% respectivamente. En cuanto a la función de RECUPERAR se puede observar que se mantiene en una puntuación del 60%.

De acuerdo con esta evaluación, la OTIC debe priorizar las acciones encaminadas a reforzar las funciones que se encuentran con un nivel bajo de avance, en especial el de RECUPERAR de acuerdo con los lineamientos establecidos en la NIST. Para consultar los detalles de la evaluación se puede consultar el anexo No. 1 - Evaluación OCI.

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 83% frente al 78% obtenido en la evaluación de la vigencia 2022. El avance del 5% se atribuye a la verificación de la totalidad de los controles. Este avance es atribuible en gran parte a que aún se encuentran en proceso de implementación; es decir, hay algunos Dominios que componen el sistema, que se encontraban en etapas tempranas de avance ahora ya se encuentran en niveles más avanzados de implementación. En la siguiente gráfica se puede evidenciar el avance:

Ilustración 1- Efectividad de Controles

No.	Evaluación de Efectividad de controles					ESCALA DE CALIFICACIÓN	ESCALA DE CALIFICACIÓN
	DOMINIO	DOMINIO	Calificación Seguimiento OCI_noviembre 2022	Calificación Seguimiento OCI_noviembre 2023	Calificación Objetivo	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 DE LA INFORMACIÓN	100	100	100	OPTIMIZADO	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	82	91	100	OPTIMIZADO	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	A.7 SEGURIDAD DE LOS RECURSOS HUMANOS	77	100	100	OPTIMIZADO	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	A.8 GESTIÓN DE ACTIVOS	77	83	100	OPTIMIZADO	GESTIONADO
A.9	CONTROL DE ACCESO	A.9 CONTROL DE ACCESO	83	84	100	OPTIMIZADO	OPTIMIZADO
A.10	CRIPTOGRAFÍA	A.10 CRIPTOGRAFÍA	70	70	100	GESTIONADO	GESTIONADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	A.11 SEGURIDAD FÍSICA Y DEL ENTORNO	76	82	100	OPTIMIZADO	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	A.12 SEGURIDAD DE LAS OPERACIONES	82	84	100	OPTIMIZADO	OPTIMIZADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	A.13 SEGURIDAD DE LAS COMUNICACIONES	72	74	100	GESTIONADO	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	73	86	100	OPTIMIZADO	GESTIONADO
A.15	RELACIONES CON LOS PROVEEDORES	A.15 RELACIONES CON LOS PROVEEDORES	80	80	100	GESTIONADO	GESTIONADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	77	80	100	GESTIONADO	GESTIONADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	70	74	100	GESTIONADO	GESTIONADO
A.18	CUMPLIMIENTO	A.18 CUMPLIMIENTO	76	81	100	OPTIMIZADO	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES			78	83	100	OPTIMIZADO	GESTIONADO

Nota elaboración propia – Basado en el instrumento del MSPI

2.9 Evaluación 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,

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

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 lineamientos 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:

Ilustración 2 - Riesgos OTIC

Tipo	Riesgos	Controles	Acciones	Materialización
Gestión	2	5	4	0
Corrupción	1	1	1	0
Seguridad de la información	2	11	8	1
Oportunidades	N/A	N/A	2	N/A
Totales	**5**	**17**	**15**	**1**

Nota: Fuente elaboración propia

2.9.1 Materialización de riesgo:

A continuación, se listan los detalles del riesgo por obsolescencia tecnológica el cual se materializó en marzo de 2023:

Ilustración 3 - Riesgo Materializado

Ítem Matriz de riesgo	Descripción
Descripción del riesgo Materializado	"Posibilidad de pérdida de la disponibilidad de los sistemas de información accidental o deliberada, debido a errores en los sistemas de información, falta de mantenimiento de la infraestructura de TI, adquisición del software con vulnerabilidades, ataques cibernéticos e incumplimiento de las políticas, procedimientos y legislación vigente relacionada"
Activos Afectados:	Infraestructura de TI
Impacto	Económico y reputacional
Amenaza	Falta de mantenimiento del equipo
Vulnerabilidad	Mantenimiento insuficiente
Probabilidad inherente	Media
Impacto inherente	Mayor
Zona de riesgo inherente	Alto
Descripción del control	"*Seguimiento a los mantenimiento preventivo y correctivo de equipos de usuario final, infraestructura TI, planta eléctrica, UPS. Informe de mesa de ayuda sobre los mantenimientos realizados a los equipos de usuario final*"
Seguimiento:	"*Se materializa riesgo por obsolescencia tecnológica en la infraestructura onpremises afectando SICAPITAL, AD, DNS, DHCP, Zabbix, y ambientes de desarrollos y pruebas no críticos para la operación de la Entidad*".
Fecha de materialización	14/03/2023
Actividades ejecutadas	*"Activación del DRP y procedimiento y manual GTI-IN-03 V1 Gestión de incidentes de seguridad de la información"*

Nota: Elaboración propia, tomado de la matriz de riesgos de la OTIC

La materialización del riesgo por obsolescencia tecnológica, de acuerdo con lo solicitado en el MSPI en el numeral T.3.2.4 (Mantenimiento de equipos) y el control ISO 27001:2013, refuerza la necesidad de seguir las directrices para el mantenimiento de equipos, que incluyen mantenerlos conforme a los intervalos y especificaciones de servicio recomendados por el proveedor. La OCI evidenció que la entidad no llevó a cabo la renovación tecnológica de los equipos que se encontraban fuera del soporte de los fabricantes y sin garantía. Esta situación tuvo un impacto significativo en la disponibilidad y la capacidad de la OTIC para cumplir con sus actividades de manera efectiva.

La obsolescencia tecnológica no solo implica la pérdida de garantías, soporte técnico y actualizaciones, sino que también puede tener consecuencias en la interoperabilidad de los sistemas, su integración con sistemas existentes y su capacidad de adaptación a cambios futuros en el entorno tecnológico. Esta amenaza subraya la necesidad urgente de que la entidad aborde de manera proactiva la gestión de la obsolescencia, reconociendo su impacto en diversos aspectos críticos.

Para mitigar este riesgo, se sugiere implementar un plan estratégico de renovación tecnológica, priorizando la actualización o reemplazo de equipos obsoletos. Este enfoque no solo salvaguardará la eficiencia y disponibilidad operativa, sino que también fortalecerá la capacidad de la entidad para enfrentar los desafíos tecnológicos futuros. Es imperativo que la OTIC adopte medidas preventivas y proactivas para garantizar la sostenibilidad y eficacia a largo plazo de sus operaciones en un entorno tecnológico en constante evolución.

3. CONFORMIDADES Y FORTALEZAS, O ASPECTOS POSITIVOS ENCONTRADOS

El equipo auditor identificó las siguientes conformidades, fortalezas y aspectos positivos:

3.1 Cumplimiento normativo

La entidad cumple con los requisitos normativos relacionados con la seguridad de la información, demostrando un compromiso legal y regulatorio.

3.2 Políticas de Seguridad de la Información definidas[2]

El equipo auditor observó que las políticas de seguridad de la información están claramente definidas, documentadas, publicadas y socializadas, cumpliendo con los requisitos establecidos en el MSPI.

3.3 Compromiso de la alta dirección

La OCI, destaca el compromiso de la alta dirección con la seguridad de la información, evidenciado por su participación en la implementación y mantenimiento del SGSI el cual se observa en la política de seguridad de la información.

3.4 Identificación y evaluación de riesgos

El proceso de identificación y evaluación de riesgos se llevó a cabo de acuerdo con la política de riesgos de la entidad, evidenciando una identificación de las amenazas potenciales y sus impactos en la seguridad de la información.

3.5 Gestión de incidentes

La OTIC dispone de un procedimiento de gestión de incidentes, proporcionando a la entidad la capacidad de gestionar y responder de manera efectiva ante cualquier incidente

3.6 Registros y documentación

La documentación relacionada con el SGSI cumple con los estándares de la norma ISO 27001. Los registros son completos, precisos y se mantienen de manera organizada en el sistema de gestión de la entidad.

3.7 Roles y responsabilidades

Los roles y responsabilidades en relación con la seguridad de la información están claramente definidos, en especial la designación del Responsable de Seguridad de la Información y de Datos Personales.

[2] Política de Seguridad de la Información | Unidad Administrativa Especial de Servicios Públicos -UAESP-

3.8 Conciencia de seguridad

La OTIC ha realizado durante el año varias capacitaciones relacionadas con la seguridad de la información y realizó un ejercicio de phishing controlado, lo que permite a los funcionarios de la entidad contar con herramientas para responder ante incidentes de seguridad.

3.9 Mejora continua

El equipo auditor evidenció un compromiso de la OTIC con la mejora continua del MSPI, tanto con la elaboración del autodiagnóstico, como un avance importante de la ejecución de las acciones generadas de las observaciones reportadas en las diferentes auditorías tanto internas como externas.

4. OBSERVACIONES

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

Tabla 6 - Observaciones de la auditoría

No.	PROCESO / CONTROL	DESCRIPCIÓN DE LA OBSERVACIÓN
4.1	**T.1.2.4: Gestión de información secreta de usuarios.** **A.9.2.4 – ISO 27001:2013**	**1. Contraseñas por Defecto:** Durante la revisión a las contraseñas de la OCI, el equipo auditor evidenció la presencia de usuarios con contraseñas por defecto, las cuales fueron asignadas al momento de la firma del contrato, incumpliendo con lo solicitado en los literales d y e del control correspondiente, presentando un riesgo de vulnerabilidad debido a contraseñas preestablecidas no modificadas. **2. No Solicitud de Cambio de Contraseña:** Se identificaron funcionarios para los cuales el sistema no está solicitando el cambio de contraseña de acuerdo con la periodicidad establecida en las políticas de seguridad de la información, incumpliendo las políticas de seguridad,

No.	PROCESO / CONTROL	DESCRIPCIÓN DE LA OBSERVACIÓN
		aumentando el riesgo de acceso no autorizado y comprometiendo la integridad de las contraseñas. **3. Contraseñas Débiles o por Defecto en Plataformas TI:** Durante la revisión realizada por la OCI, se evidenciaron plataformas de Tecnologías de la Información que utilizan contraseñas por defecto o débiles, contraviniendo lo establecido en el literal g del control y generando una exposición a amenazas de seguridad, comprometiendo la confidencialidad y la integridad de la información almacenada en dichas plataformas.
4.2	**T.3.1.1 Perímetro de seguridad física.** **T.3.1.2. Controles físicos de entrada - Protección contra amenazas externas y ambientales.** **T.3.1.3. Seguridad de oficinas recintos e instalaciones**	Durante la revisión realizada en sitio al cuarto y planta eléctricos se evidenciaron las siguientes oportunidades de mejora: **Cuarto eléctrico:** **1. Ausencia de Sistema de Control de Acceso:** La falta de un sistema de control de acceso impide tener un registro preciso de la fecha y hora de entrada y salida de visitantes en el cuarto eléctrico, generando riesgo por la falta de trazabilidad y supervisión adecuada de las actividades en el cuarto eléctrico. **2. Carencia de Controles de Acceso Apropiados:** La ausencia de controles de acceso adecuados, como la implementación de un mecanismo de autenticación de dos factores mediante una tarjeta de acceso o proximidad y un PIN secreto, compromete la seguridad en el cuarto eléctrico, exponiendo el cuarto eléctrico a vulnerabilidad a accesos no autorizados y potencial compromiso de su integridad.

No.	PROCESO / CONTROL	DESCRIPCIÓN DE LA OBSERVACIÓN
		Planta eléctrica: **3. Cerradura Dañada en Consola de Administración:** Se evidenció que la cerradura de la consola de administración de la planta eléctrica está dañada, lo que afecta la integridad de los controles de seguridad, presentado un riesgo de acceso no autorizado y pérdida de control sobre la administración de la planta eléctrica. **4. 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 incidentes de seguridad y potencial amenaza para su integridad y el de la entidad.
4.3	**T.3.2.4: Mantenimiento de equipos.**	**1. Materialización del riesgo por Obsolescencia Tecnológica:** La materialización del riesgo asociado con la obsolescencia tecnológica representa una amenaza significativa para la disponibilidad de los activos de información de la UAESP, presentando una afectación en la disponibilidad de los activos y servicios de TI. **2. Identificación de Activos con Potencial Obsolescencia:** Durante la auditoría, se identificaron activos de información tanto de infraestructura crítica de TI como equipos de usuario final que presentan la posibilidad de quedar obsoletos en un futuro cercano, presentando un riesgo de pérdida de eficiencia operativa y afectación de la capacidad (OTIC) para cumplir efectivamente con sus funciones.

5. SOLICITUD DE CORRECCCIÓN O ACCIONES CORRECTIVAS

Tabla 7 – 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, Ciber del MSPI en UASP se concluye que:

6.1 Resultados MSPI

El resultado de la evaluación efectuada al Modelo de seguridad y privacidad de la información en calificación cuantitativa es del 83%, frente al 78% obtenido en la vigencia 2022, se evidencia un avance de cinco (5) puntos porcentuales para esta vigencia.

6.2 Valoración Controles MSPI

Según la escala de valoración de efectividad de controles con base en el instrumento diseñado por el MINTIC, se puede concluir que el sistema implementado a la fecha se clasifica en **OPTIMIZADO**, es decir, superó de **GESTIONADO** que se encontraba en la evaluación anterior; lo que significa que buena parte de los procesos y controles se documentan, se comunican y algunos se gestionan; sin embargo, es poco probable la detección de incidentes que han surgido de la obsolescencia y que no se aplicado el control oportunamente.

6.3 Avance PHVA

En cuanto al avance en PHVA se encuentra en 88%, con respecto a la evaluación del año inmediatamente anterior que fue del 83%; es decir, avanzó en cinco (5) puntos porcentuales; lo anterior evidencia que se ha avanzado en el componente de **PLANEAR** con un 35%,

mientras que lo que corresponde a los componentes IMPLEMENTACIÓN, EVALUACIÖN de DESEMPEÑO, y MEJORA CONTÏNUA, cuentan en promedio de 17% y 18% respectivamente. Lo que evidencia que se deben emprender acciones más eficientes para el HACER, VERICAR y ACTUAR.

6.4 Madurez MSPI

Lo que corresponde a madurez del modelo continúa en nivel **DEFINIDO**, por los tres (3) aspectos mencionados como fueron: Plan de continuidad (BCP), Desarrollo seguro, segmentación de VLAN´S. (ver anexo No. 1 - Evaluación OCI)

6.5 Avances CIBER

Para el componente de CIBER se clasifica con una calificación de 75% en comparación con la evaluación del año anterior ha subido en tres (3) puntos porcentuales por cuanto estaba en 72% respectivamente.

6.6 Oportunidad en los sistemas de control de acceso

El equipo auditor identificó áreas de oportunidad en el control de acceso y autenticación, especialmente en la falta de un sistema de control de acceso en ciertas áreas críticas. La implementación de mecanismos de doble factor de autenticación se presenta como una medida esencial para fortalecer la seguridad.

6.7 Oportunidad de mejora en la gestión de contraseñas

La revisión de contraseñas reveló tanto la presencia de contraseñas por defecto como la falta de solicitud de cambio de contraseña para algunos funcionarios. Estos hallazgos subrayan la necesidad de mejoras en la gestión de contraseñas para mitigar riesgos de acceso no autorizado.

6.8 Riesgos de Seguridad de la Información

Al presentarse la materialización del riesgo de obsolescencia tecnológica, la entidad debe ejecutar las acciones necesarias que permitan mantener actualizadas las plataformas de TI y

contar con un soporte profesional tanto para los elementos críticos como para los de usuario final.

6.9 Instrumento MSPI OCI

Debido al alto número de controles, se recomienda al proceso revisar el detalle de las recomendaciones tanto de los controles administrativos como técnicos en Anexo 1: Instrumento MSPI OCI.

7. RECOMENDACIONES

Tabla 8 - 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 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
7.2	**Control AD2.1.2-A.6.1.2.**	Definir también roles y perfiles para todos los SI de la entidad, no solo ORFEO y SICAPITAL.
7.3	**Control AD.2.1.5-A.6.1.5**	Socializar los lineamientos establecidos en la resolución la resolución 648 de 2023, por la cual se emiten directrices en la seguridad de la información en la gestión de proyectos en la UAESP y validar la aplicabilidad de los lineamientos en lo que respecta a seguridad de la información.
7.4	**Control AD.2.2.1-A.6.2.1**	Hacer seguimiento a los lineamientos dados en el manual de la política y su aplicabilidad en lo que

No.	PROCESO	RECOMENDACIÓN
		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 sus sensibilizaciones de seguridad de la información al interior de la entidad sean más asertivas.
7.6	**Control AD4.1.4-A8.1.4**	Continuar con Gestión del conocimiento, en especial por el ítem del control solicitado: "En caso en que un empleado o usuario de una parte externa posea conocimientos que son importantes para las operaciones regulares, esa información se debería documentar y transferir a la Entidad."
7.7	**Control AD4.2.2-A8.2.2**	Sensibilizar a los funcionarios de la entidad el completar el etiquetado de la información para todos los documentos que produzca la entidad con base en la matriz de activos de información definido.
7.8	**Control AD4.2.3-A8.2.3**	Evitar al máximo materialización de riesgos como el generado en marzo de 2023. Y solucionar las fallas presentadas en los servidores Blade. Obsolescencias tecnológicas.
7.9	**Control AD4.3.2-A8.3.2; AD4.3.3-A8.3.3**	Procedimientos de baja de bienes y traslado de bienes susceptible de actualizarlo por cuanto datan del año 2017.
7.10	**Control AD.5.1.1-A17.1.1**	Realizar pruebas y verificar su aplicabilidad, funcionalidad y efectividad del BCP.

No.	PROCESO	RECOMENDACIÓN
7.11	**Control AD.6.1.2-A.18.1.2**	Validar el cumplimiento y la aplicabilidad de política de propiedad intelectual.
7.12	**Control AD.6.1.4-A18.1.4**	Implementar y desarrollar el programa de PDP junto con sus procedimientos respectivos.
7.13	**AD.7.1-A.15.1**	Contar con la identificación de riesgos que se dan con la prestación de servicios de proveedores, a su vez llevar un registro y monitoreo de los ANS de los proveedores.
7.14	**AD.7.2-A.15.2**	Contar con un mecanismo de cumplimiento de la política de seguridad para los proveedores de servicios.

Tabla 9 - Recomendaciones a controles Técnicos

No.	PROCESO	RECOMENDACIÓN
7.15	Control T.1.2.3 – A.9.2.3	Mantener control sobre las cuentas con privilegios en todas sus fases, desde la asignación, cambios y retiro de los responsables de estas, de acuerdo con lo señalado en el control.
7.16	Control T.1.2.4 – A.9.2.4	Reemplazar las contraseñas por defecto o débiles en las plataformas TI de la entidad. Nota: La recomendación se puede ampliar en el anexo 3 – Informe Técnico
7.17	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

No.	PROCESO	RECOMENDACIÓN
		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.
7.18	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.
7.19	Control T.1.4.4 – A.9.4.5	Formalizar, socializar e Implementar y el protocolo de para controlar la instalación de programas utilitarios y demás requerimientos solicitados en el control.
7.20	Control T.2.1.2 – A.10.2	Establecer un procedimiento que permita articular las acciones necesarias para para la gestión de las llaves criptográficas que incluyan su generación, acceso, cambio, actualización, revocación, recuperación, destrucción y auditoría. De acuerdo con lo solicitado en el control y en cumplimiento de lo establecido en el numeral 7.9 Controles criptográficos del manual de políticas de seguridad de la información.
7.21	Control T.3.1.1 – A. 11.1.1	Revisar los controles de seguridad requeridos y realizar la actualización de estos en el cuarto y planta eléctrica de la entidad.
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 la capacidad de la UPS se encuentra en estado crítico por las baterías que se encuentran fuera de servicio.

No.	PROCESO	RECOMENDACIÓN
7.23	Control T.3.2.9 – A.11.2.9	Establecer contraseñas seguras y en lo posible doble factor de autenticación para los diferentes activos de acceso general como por ejemplo las fotocopiadoras y su software de administración.
7.24	Control T.4.2.1 – A.12.2.1	La OCI, recomienda al proceso mantener actualizados los documentos relacionados con la alta disponibilidad y los diagramas de red.
7.25	Control T.4.3.1 – A.12.3.1	Reforzar tanto la política de respaldo de la información como su ejecución efectiva, toda vez que a raíz de la falla por obsolescencia tecnológica no se contaban con respaldo de sistemas como Odoo y Wsuss.
7.26	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.
7.27	Control T.5.1.1 – A13.1.1	Tener en cuenta las recomendaciones incluidas en los diversos informes de RED LAN_WLAN ni desarrollo de un plan que permita abordar las vulnerabilidades señaladas en dichos informes.
7.28	Control T.5.1.3 – A.13.1.3	Realizar la segmentación efectiva de la red de la entidad, para evitar que todas las LAN de la entidad sean visibles entre sí.
7.29	Control T.5.1.3 – A.13.1.3	Continuar con la implementación del DLP y monitorear su funcionamiento.

No.	PROCESO	RECOMENDACIÓN
7.30	Control T.6.2.1 – A.14.2.1	La OCI recomienda realizar las acciones necesarias par cumplir con los cronogramas establecidos, ejemplo: Odoo y la integración de Orfeo con SDQS.
7.31	Control T.6.2.3 – A.14.2.3	Implementar los ambientes de desarrollo, pruebas y producción en la totalidad de los desarrollos de software de la entidad.
7.32	Control T.7.1.3 – A.16.1.3	Ampliar el alcance de las políticas y procedimientos relacionados con desarrollo de software, gestión de incidentes, gestión de riesgos y datos personales, que cubra los sistemas de información operados por las concesiones.

8. APROBACIÓN

Sandra Beatriz Alvarado Salcedo

Firmado digitalmente por Sandra Beatriz Alvarado Salcedo
Fecha: 2023.11.30 15:45:54 -05'00'

Sandra Beatriz Alvarado Salcedo

Jefe(a) de Oficina de Control Interno

Osbaldo Cortes Lozano - Ligia M. Velandia

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

28/11/2023