MEMORANDO

Al contestar, por favor cite el radicado:
No.:**20221100071243**

Bogotá D.C., 25 de noviembre de 2022

PARA: **CESAR MAURICIO BELTRÁN LOPEZ**
Oficina de Tecnologías de la Información y las Comunicaciones

DE: Oficina de Control Interno

ASUNTO: Resultados Evaluación del Modelo de Seguridad y Privacidad de la Información 2022

De conformidad con el Plan Anual de Auditorías 2022, hacemos entrega del 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 **"GESTIONADO**" respecto a la escala de calificación del instrumento, se puede concluir de acuerdo con la escala de valoración de efectividad de controles diseñada por el MinTIC, que el sistema implementado evidencia un avance desde la evaluación anterior noviembre de 2021 pasando de **63% a un 78%** en escala de calificación, dando avance a los lineamientos de la Resolución 500 del MinTIC de 2021.

Igualmente, en cuanto al modelo de operación del **PHVA se evidencia avance pasando del 67% en la vigencia 2021 al 83% en esta vigencia 2022.** Si bien es cierto que se ha avanzado en construcción de diferentes documentos e instrumentos, aún se encuentran varios en proceso de elaboración, otros en proceso de aprobación y socialización para implementar, verificar y realizar su mejora continua.

En cuanto a la madurez del modelo se evidencia avance respecto de la evaluación del año 2021 pasando de la etapa **"INICIAL"** del año 2021 a una etapa **"DEFINIDO**" para el año 2022.

Por su parte, dentro de las mejores prácticas de Ciberseguridad definidas por el NIST, se observa un avance de esta perspectiva lo cual permite que la UAESP haya avanzado de un 52% a un 72%, sobresaliendo la puntuación obtenida en las funciones **RESPONDER** y **PROTEGER** cuyos porcentajes fueron 78% para ambas. Para las funciones **IDENTIFICAR, DETECTAR y RECUPERAR** la puntuación obtenida en promedio fueron de 71%, 76% y 60% respectivamente, las cuales también son importantes para la gestión de TI, y se deben ahondar esfuerzos para avanzar en las mismas.

Bogotá D.C., 25 de noviembre de 2022

De otra parte, si bien se evidenció un avance con referencia a la evaluación anterior, es importante continuar avanzando en su implementación; por lo tanto, es esencial que se valide y se contemplen acciones de tal manera que permitan llegar a buen término en el proceso de implementación total del modelo.

De esta manera, quedamos atentos a la suscripción de un 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 (virtual) 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: 2022.11.25 15:20:49 -05'00'

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

Anexos: Informe resultados de auditoría - MSPI_2022
Instrumento de Evaluación - MSPI

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

Informe de auditoría interna

ENFOQUE DE LA AUDITORIA INTERNA	GESTIÓN Y RESULTADOS (1)	ANÁLISIS FINANCIERO Y CONTABLE (1)	LEGAL (1)	SISTEMA DE GESTIÓN (2)
	X			MSPI, MIPG
INFORME (3)	**INFORME DE AUDITORIA EVALUACIÓN AL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2022 - UAESP**			
PROCESO, PROCEDIMIENTO, Y/O DEPENDENCIA	OFICINA DE TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES – OTIC.			
RESPONSABLE Y/O AUDITADOS	Ing. Cesar Beltrán, Paola Murcia, Sayra Paola Murcia y equipo de trabajo de la OTIC.			
OBJETIVO	**Evaluar el Sistema de Gestión de la Seguridad de la Información operante en la UAESP, conforme con los lineamientos del Modelo de Seguridad y Privacidad de la información (MSPI) del MinTIC y la ISO 27001:2013.**			
ALCANCE	Se verificó el avance en la implementación del Sistema de Gestión de Seguridad de la Información vigente, respecto de las actuaciones adelantadas a septiembre de 2022, teniendo en cuenta los 114 controles del MSPI.			
PERIODO DE EJECUCIÓN	Del 03/10/2022 al 30/11/2022			
EQUIPO AUDITOR	Ligia Marlén Velandia León – LMVL			
DOCUMENTACIÓN ANALIZADA (4)	- **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 - **Matriz –** 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** - **RESOLUCION 500 DE 2021 MINTIC**

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

1. DESCRIPCIÓN GENERAL DEL DESARROLLO DE LA AUDITORIA

Conforme con el Plan Anual de Auditorías de 2022, la Oficina de Control Interno - OCI dando cumplimiento a dicho plan, procedió a planificar y desarrollar la auditoria del MSPI notificado mediante Radicado 20221100056273 del 04 de octubre de 2022, cuyo propósito consistió en realizar la evaluación sobre el avance total de los 114 controles administrativos y técnicos que corresponden al modelo del Sistema de Gestión de la Seguridad de la Información operante en la UAESP, de conformidad con los lineamientos del Modelo de Seguridad y Privacidad de la información (MSPI) del Ministerio de TIC e ISO 27001:2013.

La Metodología utilizada fue realizada conforme con lo establecido por el Procedimiento de Auditorías Internas V.11-PC- 04, con el apoyo de los lineamientos y guías del Modelo de Seguridad y Privacidad de la Información MSPI de la Política de Gobierno Digital del Ministerio de TIC.

Para realizar la evaluación fue analizada la efectividad de los controles definidos según la norma ISO 27001:2013 para catorce (14) dominios evaluables en componentes administrativos y técnicos, con el propósito de identificar el nivel de madurez del Modelo de Seguridad y Privacidad de la Información de la UAESP.

Con base en los controles referidos en el MSPI, se procedió a analizar el avance del ciclo de funcionamiento del modelo de operación (Planear Hacer Verificar y Actuar - PHVA), y validar las hojas de Madurez y Ciber en el Instrumento de identificación de la línea base de seguridad administrativa y técnica de MINTIC, esta medición frente a las mejores prácticas en ciberseguridad definidas por el Instituto Nacional de Estándares y Tecnología - NIST, lo cual permitió generar un diagnóstico de las cinco (5) funciones básicas de seguridad (Detectar, Identificar, Responder, Recuperar y Proteger), frente a los lineamientos de la política de ciberseguridad y ciberdefensa definidos en los documentos CONPES 3701 y 3854 con base en la información presentada por la Oficina de TIC de la UAESP.

Igualmente, en el marco de la auditoría se procedió a validar las diferentes acciones e implementaciones de los controles que eran necesario llevar a cabo, de acuerdo a los resultados obtenidos en la auditoría

1. DESCRIPCIÓN GENERAL DEL DESARROLLO DE LA AUDITORIA

de la vigencia 2021, sobre la cual la OCI dejó observaciones y recomendaciones comunicadas mediante radicado con el N° 20211100056953, de igual forma, se validó los avances en la implementación del MSPI, así como las acciones planteadas en el plan de mejoramiento interno cuyo seguimiento también se describe a continuación:

Es importante tener en cuenta que aun cuando varios de los controles o acciones establecidas en el plan de mejoramiento se encontraron en estado de cumplimiento, una vez analizado el contexto sobre el cual se establecieron dichas acciones o controles, en el marco de esta auditoría se evidenció la oportunidad de mejora frente a las mismas, de tal manera que se asegure la continuidad de acciones posteriores a las ya implementadas que permitan la implementación del control total bajo los criterios del MSPI; así mismo para las que se encontraron con cierre por incumplimiento, se validaron en la presente auditoria y se generaron las recomendaciones respectivas, con el fin de tenerlas en cuenta en el próximo plan de acción o de mejoramiento que surta de la presente evaluación.

De esta manera en la siguiente tabla se presentan los avances respecto de las observaciones de la evaluación anterior que muestran su estado y seguimiento a la fecha, teniendo en cuenta la autoevaluación y el cumplimiento al plan de mejoramiento:

DOMINIO	OBSERVACIÓN	ESTADO	ULTIMO SEGUIMIENTO OCI
A.5. Políticas de Seguridad de la Información	Aún pendiente acto administrativo que adopta la Política General de Seguridad y Privacidad de la Información.	CERRADA	Se evidenció acto administrativo de Política de Seguridad de la Información con la Res. 491/22 y también el Manual de Seguridad de la Información V3 (versión 3) y la socialización a los servidores públicos.
A.6. Organización de la Seguridad de la Información	No se cuenta con una matriz de Roles y Perfiles para asignación de usuarios a las aplicaciones con base en las funciones particulares del cargo que ocupa o que va a ocupar, puesto que esta asignación se realiza a medida que ingresa el funcionario de manera uniforme no diferenciada.	CERRADA	Se evidenció matriz de roles y perfiles de los sistemas que actualmente están en producción como es SI CAPITAL, ORFEO.
	En cuanto al ingreso de aplicaciones se encuentra ORFEO integrado con LDAP, mientras que SI CAPITAL se realiza manual.	CERRADA INCUMPLIDA	Una vez validado el tema se determina después de realizar estudio de viabilidad que no es posible actualmente su cumplimiento, dada la obsolescencia tecnológica de SI CAPITAL, tema que no es del resorte de la OTIC.
	No se evidencia una metodología o lineamientos para la Gestión de Proyectos que contemple: -a) Activos que se involucran en el proyecto; b) Si hay información confidencial; c) Si hay riesgos de seguridad que tengan que ver con el proyecto; d) Condiciones de propiedad intelectual; e) Criterios o condiciones de aceptación de aspectos de seguridad en los desarrollos - entre otros.	CERRADA INCUMPLIDA	Este tema aún se encuentra en etapa prematura de desarrollo; no obstante, se ha coordinado con OAP sus etapas iniciales. Dentro del plan de acción de MSPI se cuenta con la actividad: "Definir los lineamientos para la inclusión de la seguridad y privacidad de la información en la metodología de proyectos que tenga la Entidad" fecha estimada febrero de 2023.
	Dada la emergencia sanitaria los funcionarios y contratistas tienen en su mayoría modalidad de teletrabajo y con	CERRADA	Se evidenció documentación de teletrabajo.

1. DESCRIPCIÓN GENERAL DEL DESARROLLO DE LA AUDITORIA

	modalidad BYOD (del inglés Bring Your Own Device) con dispositivos de uso personal, para los cuales no se evidencia suficientes controles de acceso sino únicamente VPN (del inglés Virtual Private Network) para que algunos usuarios puedan acceder a aplicativos críticos específicos de su rol.		Es así que por cada uno de los funcionarios que se observó para el asunto de la referencia con los diferentes aplicativos y trazabilidad, en cuanto a que el acuerdo de teletrabajo incluye el ítem de seguridad de la información para servidores públicos. Así mismo, la instalación de aplicativos de acceso y control remoto en los PC fuera de la sede de la Entidad.
A.7. Seguridad de los Recursos Humanos	El Manual de Política de Seguridad de la Información aún en proceso de formalización y adopción	CERRADA	A pesar de que en el marco de seguimiento del PMI quedó incumplida, en el desarrollo de esta auditoría ya se cuenta con el manual de política V3 aprobado y socializado, evidenciando su cumplimiento.
A.8. Gestión de Activos	Para disposición de los medios no se evidencia un "procedimiento de borrado seguro", toda vez que actualmente se realiza solo con formateo de equipos y ello no es garantía de borrado seguro de software, (ejem, equipos que se reasignan).	CERRADA	Se evidencio procedimiento de soporte a la infraestructura tecnológica donde se establece el borrado seguro, es importante validar el cumplimiento continuo al control en la próxima auditoría.
	Para transferencia de medios físicos, no se evidencia un "lineamiento", "protocolo" o "procedimiento" que permita determinar o establecer medidas de protección de medios que contienen información sensible, que contemple análisis de riesgo de equipos que no se encuentran en la sede principal de la Entidad.	CERRADA INCUMPLIDA	Aún adolece de lineamientos claros para contar con estas medidas de protección, el procedimiento de SAF esta susceptible de mejora y actualización. Sin embargo, en el marco de esta auditoría en reunión con la OTIC se manifiesta que el procedimiento actual aplica para la transferencia de medios físicos.
	En la gestión de medios removibles aún en proceso de definición en el Manual de PSI, no se evidencia una herramienta o solución para mitigar riesgos de fugas de información por estos medios.	CERRADA	Se evidenció pruebas piloto de implementación del DLP y estas corresponden a la acción planteada; igualmente, en el marco de la auditoría de MSPÏ se validó su implementación y aún se encuentra en pruebas piloto.
	Según reunión se evidencia debilidad en la gestión del directorio, en particular, en el aplicativo ORFEO por cuanto cuenta aún con debilidades al finalizar vinculación de funcionarios y contratistas no se desactivan ágilmente.	CERRADA	Se evidenció memorando a los jefes de la Entidad con lineamientos para la gestión de usuarios en los sistemas de información y aplicativos de la Entidad.
A.9. Control de Acceso	Actualmente no se cuenta con el repositorio de versionamiento de código fuente para los desarrollos, ajustes y mejoras, lo cual es una oportunidad de mejora mencionada en varias oportunidades.	CERRADA	Se validó con el proceso el cumplimiento, con lo cual se implementó GIT para contar con un repositorio de versiones para desarrollos y así contar con la trazabilidad de cada uno. En la próxima auditoría de MSPI se volverá a validar.
A-10. Criptografía.	En el Manual de Política se evidencia la política de controles criptográficos, pero no se observa el desarrollo en protección y tiempo de vida de las llaves criptográficas	CERRADA INCUMPLIDA	Si bien es cierto que hay un capítulo en el manual de la política, aún no se define herramientas ni mecanismos para gestión de llaves. Se evidencia actividades a desarrollar en el plan de acción para finales de 2022 y 2023.

1. DESCRIPCIÓN GENERAL DEL DESARROLLO DE LA AUDITORIA

	Aún no se evidencia la implementación de la firma digital de documentos y correos electrónicos (cuando aplique), lo cual no está mitigando el riesgo generado por la realización de firmas digitalizadas (escaneadas) que actualmente se utiliza.	CERRADA	Se evidenció prueba de concepto sobre la viabilidad de implementar la firma digital, donde se aprecia su viabilidad y posteriormente, coordinar con gestión documental la continuidad del tema. Po lo tanto, por parte de la OTIC se cumplió con la acción propuesta, pero resulta importante continuar el tema con gestión documental. Sin embargo, en el marco de esta auditoría aún no se cuenta con estos lineamientos.
A.11. Seguridad Física y del Entorno	Con base en reunión con la OTIC, aún no se ha verificado con la SAF un análisis de identificación de riesgos ambientales para establecer los mecanismos de mitigación de riesgos.	..CERRADA INCUMPLIDA	No se evidencia un avance en el tema, más aún cuando se materializó un riesgo ambiental que fue solucionado por el momento (inundación del centro de eléctrico y baterías). De esto se evidencio la importancia de contar con un Ing. Eléctrico/Electricista que pueda dar soporte y solución en estos temas que son igualmente críticos.
	En visita al centro de datos (DC Data Center) se evidencia desorganización del cableado estructurado	CERRADA	En visita en sitio se evidenció la organización de este, por lo cual se dio atención a la observación.
	Igualmente, en DC no se evidenció una bitácora de ingreso y salida de personas externas, por mantenimiento, por visitas esporádicas y/o empresas de mantenimiento.	CERRADA	Se evidencia cumplimiento en la ejecución de la acción con la bitácora de control de ingresos.
A.12. Seguridad de las Operaciones	Se evidencia monitoreo de la plataforma; sin embargo, no se evidencia algún registro con las acciones realizadas; es decir, detallar el evento, la solución, categoría, incidencia y servicio como insumo, para la toma de decisiones en el ciclo de mejoramiento continuo	CERRADA	Se evidencia documento donde hay informe de monitoreo, se validó en sitio la ejecución del módulo en funcionamiento, por lo que resulta importante continuar con este monitoreo,
	Para medir la gestión de la capacidad futura no se evidencia un lineamiento donde se planifique no solo la capacidad de almacenamiento sino también análisis de desempeño, historial, planes de expansión de servicios, migraciones a nube, etc.; es decir, no se evidencia un plan de evolución de infraestructura tanto de servidores como de los demás dispositivos con base en su mantenimiento preventivo, predictivo y correctivo.	EN PROCESO	Se encuentra en desarrollo activo con el plan de acción del MSPI.
	Con base en las reuniones y las evidencias se observa que se realizan backups con la herramienta para generación de copias de seguridad, pero sin evidencia de acciones cuando fallan esos respaldos. De esta manera no se observa que haya un plan de gestión de backups que contemple pruebas de restauraciones. Aún se encuentra en proceso el procedimiento de gestión de respaldos.	CERRADA	Se evidenció informes de restauración de agosto y septiembre de 2022.
	Si bien es cierto que se realizan análisis de vulnerabilidades (página web, ORFEO), según reunión, no se evidencia	EN PROCESO	En el marco de esta auditoría se indagó sobre este análisis y pruebas realizadas y se evidenciaron pruebas de PENTEST. En

1. DESCRIPCIÓN GENERAL DEL DESARROLLO DE LA AUDITORIA

	gestión en auditorías preventivas a los sistemas de información ni bases de datos (SICAPITAL- gestión de Logs de BD). Se manifiesta que sólo se realiza en el momento del evento; es decir, son reactivas, por lo que se evidencia debilidad en este control que es susceptible de mejora.		cuanto a la actualización de ORFEO, aún no se encuentra en producción.
A.13. Seguridad de las Comunicaciones	Cuando se trasmite o consulta información a otras entidades no se evidencia los acuerdos o formalidades con todos los lineamientos de confidencialidad, o no divulgación, así como de integridad, disponibilidad, autenticidad, seguridad de la información.	CERRADA INCUMPLIDA	Para este punto se confirma la recomendación dada en la auditoría de seguridad digital sobre el tema de XROAD como medio administrado por la Agencia Nacional Digital – AND para interoperabilidad de sistemas de información de entidades públicas.
A.14. Observación. Adquisición, Desarrollo y Mantenimiento de Sistemas	No se cuenta aún con definición de un documento o política complemento de la minuta de contrato de prestación de servicios que maneja la Entidad, donde se tengan en cuenta de los posibles incumplimientos al contratista que no acate la seguridad de la información de la Entidad.	EN PROCESO	Se encuentra en actividad con plan de acción del MSPI.
	Para los servicios de seguridad de las aplicaciones que utilizan redes públicas que están en los objetivos descritos en el Manual de MPSI, falta complementar su desarrollo en el numeral de trabajo remoto que mencione los aspectos de uso de redes públicas, indispensables para esto, y así una vez formalizado este documento se pueda formalizar su aplicabilidad.	CERRADA	Se definieron los lineamientos en el manual de política V3, en su capítulo 7.3 Seguridad de la Información para el trabajo remoto, donde establece los lineamientos a seguir.
	No se cuenta con los tres ambientes de desarrollo (prueba, desarrollo, operación) con base en la evaluación para ambientes de desarrollo seguro. Sólo se cuenta con dos ambientes (pruebas y operación).	CERRADA	Se validó en sitio y observó que se tiene configurados los tres ambientes para desarrollo seguro de software.
	Para la realización de pruebas con datos personales no se evidencia un protocolo para establecer un acuerdo de confidencialidad para cuando se accede a información sensible.	CERRADA INCUMPLIDA	Aún continúa pendiente. Se validará su cumplimiento en la próxima auditoria.
A.15. Relación con los Proveedores.	No se cuenta con una matriz de ANS con terceros y políticas de estos ANS como guía para todas las actividades, procesos y procedimientos de TIC.	CUMPLIDA	A pesar de que no se encuentra como observación, en el marco de esta evaluación se evidenció esta matriz para algunos proveedores.
A.16. Gestión de Incidentes de Seguridad de la Información	No se evidencia contar con un plan de respuestas para los diferentes incidentes que se presenten una vez clasificados o categorizados.	CERRADA INCUMPLIDA	En el marco de esta auditoría se validó la actividad “Definir protocolo de atención y respuesta a incidentes de seguridad de la información por tipo de incidente” entregable: “Protocolo o procedimiento documentado, incluyendo responsabilidades. Aún no se evidencia.
	No se evidencia documentación o consolidación de información que permitan determinar lecciones aprendidas para mitigar incidentes futuros.	CERRADA	En el instrumento de bitácora de incidentes se cuenta con el consolidado de lecciones aprendidas, por lo que resulta importante tenerlas en cuenta para prevenir o mitigar incidentes similares a futuro.

1. DESCRIPCIÓN GENERAL DEL DESARROLLO DE LA AUDITORIA

	Se observa que aún no se realiza el cumplimiento y ejecución del procedimiento e instructivo de Gestión de Incidentes formalizado a partir de agosto de 2021.	CERRADA	Ya se cuenta con el Procedimiento e Instructivo de Gestión de Incidentes radicado No. 20221400025523
A.17. Aspectos de Seguridad de la Información y de la Gestión de la Continuidad del Negocio.	Se evidencio dentro del marco de esta evaluación una ocurrencia de fallo en el servicio de página Web-Orfeo, por el cual se comprueba que aún no se encuentra el DRP (BCP-DR) en alta disponibilidad para contar con una solución de restablecimiento de servicios de manera ágil.	CERRADA INCUMPLIDA	Este hallazgo hacía referencia a que el DRP en su momento no funciono, aún no se cuenta con este plan; actualmente se encuentra en el plan de acción MSPI cuya actividad es: "Elaborar el Plan de Continuidad del Negocio que incluya las estrategias de recuperación, procedimientos adecuados ante incidentes o eventos no deseados, vuelta a la normalidad y requisitos", con fecha de entrega marzo de 2023.
	Según reunión con OTIC, por temas de licenciamientos aún no es posible colocar en el DRP servicios de misión crítica (SI-CAPITAL), lo que evidencia una falla en la planeación de la implementación del DRP, sin haber validado en su momento estas situaciones.	CERRADA INCUMPLIDA	Una vez validado el tema se determina que después de realizar estudio de viabilidad que no es posible actualmente su cumplimiento, dada la obsolescencia tecnológica de SI CAPITAL, tema que no es del resorte de OTIC.
	No se observa el seguimiento de la recomendación de la anterior evaluación, en cuanto a la organización y documentación de la arquitectura para los servicios redundantes que se tienen en la Entidad	CERRADA INCUMPLIDA	En esta nueva validación, se evidencia que aún no se cuenta con esta documentación.
	Aún no se evidencia un documento donde se detalle la estrategia de continuidad de operación de la Entidad y que éste a su vez sea estructurado como una etapa para la construcción del Plan de Continuidad del Negocio y de Recuperación de Desastres; es decir, el BCP–DR (del inglés Business Continuity Plan & Disaster Recovery) y respectiva asignación de responsables.	EN PROCESO	Se encuentra en actividad con plan de acción del MSPI.
A.18. Cumplimiento	Se evidencia un proceso prematuro acerca de protección de datos personales, puesto que aún no se cuenta con una política completa y aplicable donde se establezcan: lineamientos, alcance, finalidades, responsables, procedimientos, formatos, registros de aceptación de términos y condiciones, y en general, tratamiento de Habeas Data.	CERRADA	Se cuenta con la política de datos personales aprobada por parte del CIGD, por lo cual se avanzó en el tema. Sin embargo, es importante que este tema se desarrolle en el marco de los lineamientos de la SIC y su correspondiente ciclo de vida.
	Aún se evidencia que la observación de la auditoría anterior no se ha ejecutado en cuanto al registro de bases de datos personales en la Superintendencia de Industria y Comercio - SIC. Durante el desarrollo de esta auditoría se notificó que el último registro fue en 2019.	CERRADA	Se adelanto el registro de bases de datos ante la SIC y se adjunta listado reportado y certificación.

Tabla 1 Evaluación observaciones 2021 - Fuente: Elaboración propia

1. DESCRIPCIÓN GENERAL DEL DESARROLLO DE LA AUDITORIA

Finalmente, la evaluación producto de esta auditoria fue comparada con la evaluación realizada en la vigencia de 2021 con el fin de determinar los criterios con los cuales se ha identificado avances y también aquellos que suponen requerir acciones de mejora.

De otra parte, se tuvieron en cuenta las evidencias aportadas por el proceso, la reunión y visita al sitio con recorrido a los centros de datos, sistema eléctrico y datacenter, lo que permitió el diligenciamiento de los papeles de trabajo correspondientes que se anexan dentro de este informe, generando los siguientes resultados:

2. CONFORMIDADES Y FORTALEZAS

Una vez evaluado el modelo con base en el anexo A de la norma ISO 27001:2013 y el instrumento del MinTIC se presenta a continuación conformidades y fortalezas a saber cómo:

2.1. Se cuenta debidamente formalizada la Política General de Seguridad de la Información (Resolución 491 de 2022) y el Manual de la Políticas de Seguridad y Privacidad de la Información (versión 3.0), revisados, actualizados, aprobados, socializados y publicados tanto al interior de la Entidad como en el micrositio del MIPG, Transparencia, así como se evidencia sensibilización a los funcionarios públicos de la UAESP.

2.2. Según la evaluación realizada por la OCI, se presenta un avance importante en la calificación en todos los dominios con referencia a la evaluación de 2021, lo que genera igualmente el avance en la efectividad de algunos controles; también se presenta un avance en el porcentaje de implementación para la evaluación de esta vigencia pasando de un 63 % en el 2021 a un 78% para la evaluación de este período 2022.

2.3. Se observa un avance importante en lo que respecta al ciclo de funcionamiento del modelo de operación (PHVA) con respecto a la evaluación de 2021, pasando del 67% al 83% respectivamente.

2.4. Se evidencia avance en la madurez del modelo con respecto a la evaluación inmediatamente anterior por cuanto en el año 2021 se encontraba en etapa “INICIAL” y en el desarrollo de esta evaluación se encuentra en nivel “**DEFINIDO”.**

2.5. Se observa también un avance en Modelo Framework Ciberseguridad NIST (Instituto Nacional de Estándares y Tecnología), pasando del 52% del año 2021 al 72% para esta evaluación 2022.

2.6. Se evidencia la evolución en la construcción de los procedimientos, aprobación de Política General de Seguridad y Privacidad de la Información, Manual de Políticas de Seguridad y Privacidad de la Información V.3, procedimientos Gestión de Respaldos V3, reporte de incidentes de seguridad de la información, instructivo de gestión de incidentes de seguridad de la información, actualización del PETI, lineamientos, formatos, guías; así como se encuentra en proceso los demás procedimientos e instructivos. Se evidencian esfuerzos

2. CONFORMIDADES Y FORTALEZAS

importantes con la realización de la documentación; es decir, se ha evolucionado en la construcción de los procedimientos, guías, formatos e instructivos del MSPI.

2.7. Seguimiento y acatamiento a las observaciones emitidas de la auditoría anterior. Durante el proceso de seguimiento y evaluación realizado en esta auditoria se evidencia un avance significativo en la consideración de las observaciones generadas con el seguimiento a las recomendaciones emitidas para la implementación de MSPI. Se resalta el compromiso del jefe de la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC y sus profesionales; y a su vez se evidencia un Talento Humano competente y comprometido para desarrollar las diferentes actividades que contribuyen al logro de objetivos institucionales.

2.8. Evaluación del PMI con observaciones generadas Vs cerradas: de un total de 34 observaciones al corte de esta auditoría se encuentran cerradas 19 (diecinueve) y 4 (cuatro) en proceso.

2.9. Se cuenta con un Plan de Acción que considera las diferentes actividades, entregables y fechas a cumplir para la implementación del modelo del MSPI.

2.10. Se observó la expedición de la Resolución 490 de 2022, por la cual se nombran los oficiales tanto de MSPI como PDP, según lo establecido en el rol de la Política General de Seguridad de la Información para apoyar a la Entidad en el diseño, implementación y mantenimiento del Modelo de Seguridad y Privacidad de la Información – MPSI de conformidad con la regulación vigente.

2.11. Los profesionales y jefe de la OTIC participan en diferentes grupos de seguridad de la información y ciberseguridad con la Alta Consejería de la Alcaldía de Bogotá.

2.12. Se realiza el correspondiente autodiagnóstico del modelo del MSPI al interior del proceso, lo que evidencia seguimiento y mejora continua del mismo.

2.13. Se realizan diferentes sensibilizaciones por parte del proceso al interior de la Entidad lo que evidencia que la OTIC demuestra su compromiso y esfuerzo por propender en la UESP el "*Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital*", que viene de la Política de Gobierno Digital – PGD.

3. OBSERVACIONES

A continuación, se describen las diferentes observaciones encontradas en el marco de esta auditoría, las cuales se dividen de acuerdo al tipo de control como son los administrativos y los técnicos frente a cada uno de los dominios asociados a los mismos, y que a su vez son susceptibles de mejora, incluyendo las acciones que se encontraban incumplidas en el marco del seguimiento del plan de mejoramiento interno - PMI, así:

3. OBSERVACIONES

3.1. OBSERVACIONES A CONTROLES ADMINISTRATIVOS:

DOMINIO	CONTROL	OBSERVACIÓN
A2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	AD.2.1.5: Seguridad de la información en la gestión de proyectos.	Faltan lineamientos y/o documentación sobre la Gestión de Proyectos a nivel de la Entidad que tenga en cuenta los diferentes ítems que se describen en el control propuesto del instrumento – MSPI.
AD3. SEGURIDAD DE LOS RECURSOS HUMANOS	AD.3.1.2: Términos y condiciones del empleo.	Faltan acuerdos de confidencialidad para funcionarios como lo establece la descripción de este control.
AD4. GESTIÓN DE ACTIVOS	AD.4.1.1: Inventario de Activos.	Falta actualizar el inventario de activos de información según el control, considerando como activos los establecidos por el NIST: el personal, dispositivos, sistemas e instalaciones físicas que permiten a la entidad cumplir con su misión y objetivos, dada su importancia y riesgos estratégicos.
	AD.4.1.4: Devolución de Activos	No se evidencia la 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". NOTA: Este control es importante tenerlo en cuenta toda vez que de la forma centralizada como se tiene la gestión se tiene el riesgo de perder el KnowHow (destrezas, habilidades, conocimiento, etc.) que se tiene para la operación normal y el negocio.
	AD.4.2.2: Etiquetado de la información	No se cuenta con la totalidad de etiquetado de la información respecto de los procedimientos, de tal manera que estén alineados y levantados como lo especifica el control en sus numerales (1,2,3,4).
	AD.4.3.1: Gestión de Medios Removibles	Aún no se evidencia la aplicabilidad de directrices, guías, lineamientos y procedimientos para la gestión de medios removibles, y su seguimiento correspondiente en producción (DLP - *Data Loss Prevention*).
AD5. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	AD. 5.1.2: Implementación de la continuidad de la seguridad de la información	Falta de gestión de conocimiento – GC por parte de los profesionales del área para minimizar riesgos de respaldo para administración de servicios con sus correspondientes documentaciones a lugar, es decir no solo del "**que"** se hace sino del "**cómo"** se hace; igualmente, complementar la GC con lo que establece los literales b) y c) de este control.
	AD.5.1.3: Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	A pesar de contar con avances, aún se observa debilidad respecto de la implementación oficial de un Plan de Continuidad del Negocio y pruebas correspondientes, (incluyendo procesos, procedimientos, protocolos ante incidentes, análisis y mitigación de riesgos, y demás variables)
AD6. CUMPLIMIENTO.	AD.6.1.2: Derechos de propiedad intelectual.	Se observa debilidad en el protocolo de instalación de equipos y software, y contemplar una política de propiedad intelectual que abordaría el control numeral 1.

3. OBSERVACIONES

	AD.6.1.4: Protección de los datos y privacidad de la información relacionada con los datos personales.	No se evidencia el desarrollo del ciclo de vida de los lineamientos de la Superintendencia de Industria y Comercio - SIC, máxime cuando en el marco de la auditoría se evidenció materialización de riesgo de datos personales, donde se pone en riesgo a la Entidad a sanciones legales y reclamaciones de usuarios.
AD7. RELACIONES CON LOS PROVEEDORES	AD.7.1: Seguridad de la información en las relaciones con los proveedores	Falta complementar el control, estableciendo acuerdos de confidencialidad y ANS – Acuerdo Nivel de Servicio, para proveedores que tengan acceso a los activos de información, con el objetivo de prevenir y tratar las fugas de información.
	AD.7.2: Gestión de la prestación de servicios de proveedores	No se evidencia el cumplimiento del numeral 1, en el sentido de realizar seguimientos, auditorías o revisiones a la seguridad de la información a la que tienen acceso los proveedores. De la misma manera el numeral 2 de cómo se gestionan y comunican los incidentes sufridos por los proveedores. Para ello se deben tener en cuenta los acuerdos de confidencialidad y privacidad de la información en los contratos.

Tabla 2 Descripción Observaciones Controles Administrativos – Fuente: Elaboración propia

3.2. OBSERVACIONES A CONTROLES TÉCNICOS:

DOMINIO	CONTROL	OBSERVACIÓN
T1. CONTROL DE ACCESO	T.1.2.4: Gestión de información de autenticación secreta de usuarios.	La Entidad no cuenta con un sistema para la gestión autónoma de contraseñas (single sign on). **NOTA:** La OCI ratifica que no se ha evidenciado el avance en un 100% frente a la implementación de dicho sistema; aunado a que de acuerdo al seguimiento del Plan de acción del MSPI de la OTIC la actividad "Realizar prueba concepto para implementación de un sistema de autogestión de contraseñas integrando el Directorio Activo.", se encuentra en proceso y se evidencia adicional otra actividad de "Implementar mecanismo de autogestión de contraseñas", lo que confirma que aún no se encuentra la implementación en un 100% al respecto
	T.1.4.2: Procedimiento de ingreso seguro	No se ha configurado una advertencia general acerca de que sólo los usuarios autorizados pueden acceder al computador, literal b) del control.
T2. CRIPTOGRAFIA	T.2.12. Gestión de llaves	En el Manual de Políticas de la Información se evidencian lineamientos de controles criptográficos, pero no se observa el desarrollo en protección y tiempo de vida de las llaves criptográficas, como lo describen los ítems del control en mención.
T3. SEGURIDAD FISICA Y DEL ENTORNO	T.3.1.2. y T.3.1.4 Controles físicos de entrada - Protección contra amenazas externas y ambientales	Con base en la visita en sitio se evidenció en el cuarto eléctrico que faltan acondicionamiento del aseo, y presenta un riesgo latente de condiciones ambientales que se pueden dar por lluvias y presentar cortos eléctricos, generando riesgos de seguridad, y a su vez, actualmente no cuenta con seguridad para ingreso, aun cuando esta situación se evidenció como materialización

3. OBSERVACIONES

		del riesgo en al marco de esta auditoría por falta de control de acceso y por condiciones del cuarto eléctrico de la Entidad.
	T.3.2.2. Servicios de suministro	Aún no se evidencia actualización de cableado estructurado de casitas, y a su vez puntos de red certificados en la Entidad toda vez que en esta área la prestación del servicio de red en ocasiones es intermitente.
	T.3.2.4. Mantenimiento de equipos	Actualmente se encuentra *"Help People"* sin funcionamiento. Es decir, la nueva herramienta para mesa de ayuda aún no se ha socializado a funcionarios y en cuanto al mantenimiento preventivo de equipos no se evidenció un cronograma y ejecución de este.
	T.3.2.9. Política de escritorio y pantalla limpios	Contar con un mecanismo para evitar el uso no autorizado de periféricos (ej. impresoras), ítem c) del control.
T4. SEGURIDAD DE LAS OPERACIONES	T.4.1.3. Gestión de capacidad	No se cuenta aún con un *Capacity Planning* que tenga en cuenta las variables del control y que contemple gestión de capacidad con análisis de desempeño, historial, planes de expansión de servicios, migraciones a nube, ancho de banda, etc., donde esta categoría de la planificación tenga más preponderancia.
	T.4.4.1. Registro de eventos	Falta ampliar el correlacionador de eventos SIEM a todos los sistemas de la Entidad.
T5. SEGURIDAD DE LAS COMUNICACIONES	T.5.1.1. Controles de redes	Falta validar la aplicación de las políticas de contraseñas toda vez que, para algunos usuarios de la OCI, no está solicitando actualización de contraseñas y las políticas de actualización por ejemplo de *Wallpaper*, no se cumplen igual para todos.
	T.5.1.2. Seguridad de los servicios de red	Debilidad en los mecanismos de requerimientos técnicos para la conexión segura como lo establece los ítems del control del modelo.
	T.5.2.1. Políticas y procedimientos de transferencia de información	Contar con bloqueo de puertos USB, para dar cumplimiento al literal b) del control, es decir que pase de pruebas a ejecución en la totalidad de los equipos de la UAESP, salvo las excepciones que se desprendan del estudio realizado por la OTIC.
	T.5.2.3. Mensajería electrónica	De acuerdo con el literal: "d) definir las consideraciones legales, los requisitos para firmas electrónicas"; no se evidencian lineamientos técnicos o administrativos para uso de firma electrónica.
T6. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	T.6.1.1. Análisis y especificación de requisitos de seguridad de la información	En cumplimiento del literal: "f) establecer los requisitos exigidos por otros controles de seguridad, (interfaces con el ingreso o seguimiento, o los sistemas de detección de fuga de datos)", la entidad aún no cuenta con DLP *(Data Lost Protection)* en producción que permita detectar las posibles fugas de información.

3. OBSERVACIONES

	6.1.3. Protección de transacciones de los servicios de las aplicaciones	No se evidencian los lineamientos de autorización de firmas digitales o electrónicas; igualmente, falta la implementación de la Intranet institucional para aplicar control descrito en los literales a) y e).
	6.2.2. Procedimientos de control de cambios en sistemas	No se evidencia consolidado de las solicitudes, análisis y aprobación de los cambios, al igual que la aprobación de estos por parte de los usuarios. No se evidenció controles de integridad en el despliegue de ORFEO.
	6.2.5. Principios de construcción de sistemas seguros	No se evidencia consolidado de las solicitudes, análisis y aprobación de los cambios, al igual que la aprobación de estos por parte de los usuarios y cumplimiento de los cronogramas establecidos. (Ej. ODO, Orfeo).
	6.2.7. Desarrollo contratado externamente	Se observa la supervisión de contratos de prestación de servicios para apoyar el desarrollo de sistemas de información; no obstante, se deben definir niveles de calidad, seguridad y técnicos esperados en los requerimientos contractuales, minutas de contrato o mecanismos apropiados, en especial acuerdos de licenciamiento, propiedad de los códigos y derechos de propiedad intelectual como lo establece el control.
	6.2.9. Prueba de aceptación de sistemas	Se evidencia la realización de pruebas funcionales a ORFEO 7, no obstante, se deben definir criterios de aceptación para cada plan de pruebas de los sistemas de información antes de aceptar su paso a producción.
	6.3.1. Protección de datos de prueba	No se observa evidencia de las autorizaciones para el acceso a datos de prueba con base en los literales a), b), c) del control, en especial cuando haya pruebas con datos personales para cuando se accede a información sensible.
T7. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	7.1.5. Respuesta a incidentes de seguridad de la información	Se observan los reportes de eventos desde sistemas de seguridad como antivirus y firewall, mesa de Ayuda, SIEM; no obstante, falta el análisis e investigación de los reportes, recomendaciones o notificaciones de estos sistemas, así como pertinencia de ampliar el alcance de los controles, con el objetivo de cubrir los operadores externos.
	7.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información	Aún no se evidencia un protocolo de atención y respuesta a incidentes de seguridad de la información por tipo de incidente una vez clasificados o categorizados.

Tabla 3 Descripción Observaciones Controles Técnicos – Fuente: Elaboración propia

o

4. SOLICITUD DE CORRECCIÓN Y ACCIONES CORRECTIVAS

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

5. CONCLUSIONES

5.1. EVALUACIÓN DE EFECTIVIDAD DE CONTROLES MSPI 2022:

5.1.1. **RESULTADO:** Como resultado de la evaluación efectuada al Modelo de Seguridad y Privacidad de la Información – MSPI se obtuvo una calificación cuantitativa promedio de 78% frente al 63% obtenido en la evaluación de la vigencia 2021. El avance de 15 puntos porcentuales está dado con base en la verificación de controles que se evaluaron en su totalidad. 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.

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

No.	Evaluación de Efectividad de controles				ESCALA DE CALIFICACIÓN	
	DOMINIO	Calificación Seguimiento OCI_Octubre 2021	Calificación Seguimiento OCI_noviembre 2022	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL 2022	EVALUACIÓN DE EFECTIVIDAD DE CONTROL 2021
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	80	100	100	OPTIMIZADO	GESTIONADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	61	82	100	GESTIONADO	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	71	77	100	GESTIONADO	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	69	77	100	GESTIONADO	GESTIONADO
A.9	CONTROL DE ACCESO	76	83	100	GESTIONADO	GESTIONADO
A.10	CRIPTOGRAFÍA	60	70	100	EFECTIVO	EFECTIVO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	71	76	100	GESTIONADO	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	61	82	100	GESTIONADO	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	68	72	100	GESTIONADO	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	42	73	100	EFECTIVO	EFECTIVO
A.15	RELACIONES CON LOS PROVEEDORES	70	80	100	GESTIONADO	GESTIONADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	43	77	100	OPTIMIZADO	EFECTIVO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	34	70	100	EFECTIVO	REPETIBLE
A.18	CUMPLIMIENTO	71	76	100	OPTIMIZADO	GESTIONADO
	PROMEDIO EVALUACIÓN DE CONTROLES	**63**	**78**	**100**	GESTIONADO	GESTIONADO

Ilustración 1 Avance efectividad de controles MSPI – Fuente: Elaboración propia

En la gráfica siguiente se ilustra el progreso que se ha tenido en las diferentes evaluaciones que se han venido desarrollando.

5. CONCLUSIONES

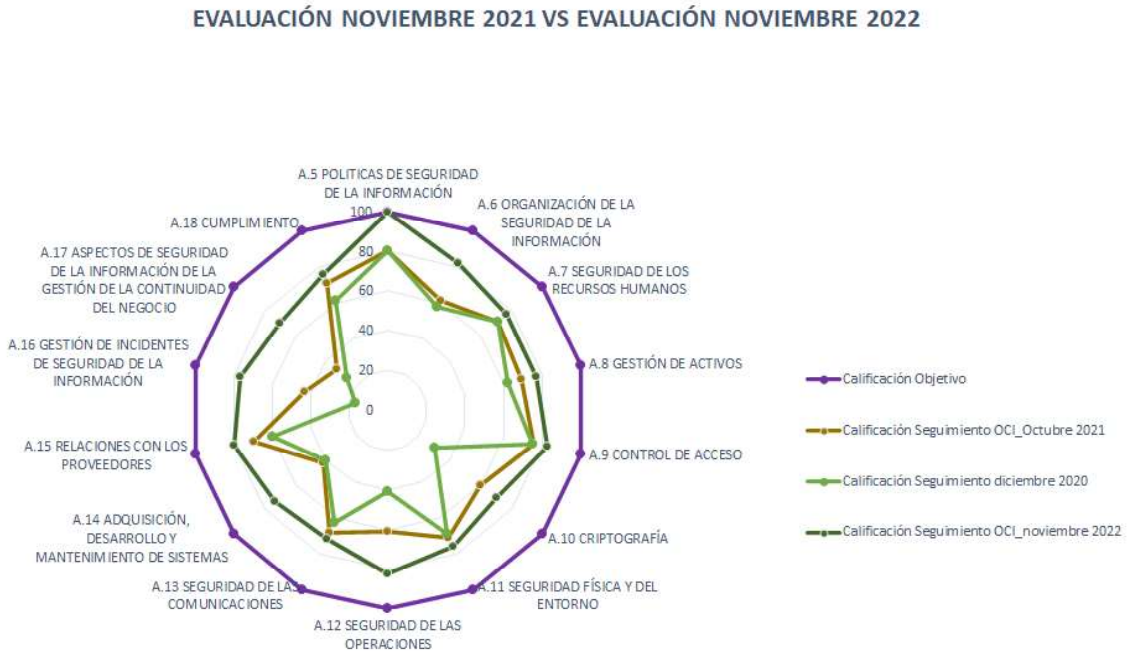

Ilustración 2 Gráfica de avance en la implementación -MSPI-2022

5.2. NIVEL DE AVANCE: Según la escala de valoración de efectividad de controles diseñada por el MinTIC se puede concluir que el sistema implementado evidencia un avance en la calificación desde la evaluación anterior en todos los dominios respectivos, lo cual demuestra que la OTIC ha mejorado en la implementación de los controles del modelo MSPI cuyo objetivo es la correlación entre los instrumentos documentados y las configuraciones en los activos de información, además de la gestión de la operación con la aplicación de los controles a los riesgos. Lo anterior aunado a que se han atendido la mayoría de las recomendaciones emitidas en la auditoría anterior que se corrobora con el avance demostrado

5.3 AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA). La correcta implementación del modelo establece la articulación del ciclo de Planear, Hacer (implementar), Verificar (evaluar) y Actuar (mejorar) – PHVA, como la estrategia para la construcción y mantenimiento del MSPI. Es así como, con base en la evaluación se puede evidenciar lo siguiente:

5.3.1 Se determina avance de 67% a 83% con base en la calificación otorgada. Si bien es cierto que se ha avanzado en construcción de diferentes documentos e instrumentos, aún se encuentran varios en proceso de elaboración, otros en proceso de aprobación y socialización para implementar, verificar y realizar su mejora continua.

5. CONCLUSIONES

5.3.2 Como este modelo de operación contribuye al objetivo de la construcción de los instrumentos documentales y su estructuración con el entendimiento del contexto de la organización articulado con el sistema de gestión de calidad, se nota el avance en la implantación del MSPI.

5.3.3 Se han estructurado y formalizado los documentos de Política General de Seguridad y Privacidad de la Información, Plan de Privacidad y Seguridad de la Información, complementado con su plan de operación, que enmarca diferentes actividades las cuales se encuentran en proceso de desarrollo en su mayoría para el año 2023.

En la siguiente gráfica se ilustra el avance que se ha tenido en sus diferentes evaluaciones.

AVANCE PHVA

COMPONENTE	% sep.2019	% junio 2020	% diciembre 2020	% OTIC_autoevaluación 2021	% OCI_octubre 2021	% OTIC_autoevaluación 2022	% OCI_noviembre 2022	% Esperado
Planificación	18%	31%	25%	28%	28%	38%	35%	40%
Implementación	7%	13%	7%	13%	10%	19%	13%	20%
Evaluación de desempeño	0%	11%	11%	15%	12%	16%	17%	20%
Mejora continua	0%	16%	8%	18%	16%	16%	18%	20%
TOTAL	26%	71%	50%	73%	67%	89%	83%	100%

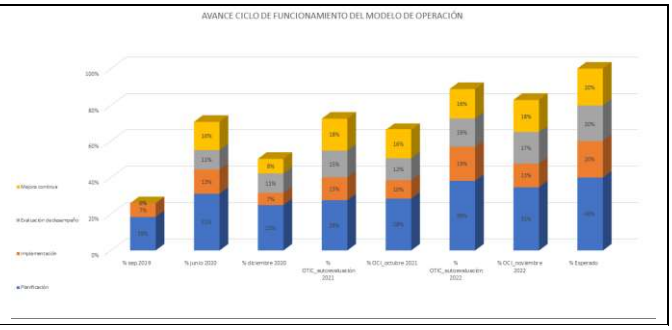

Ilustración 3 Avance de PHVA - Generado del instrumento MSPI

5.4 EVALUACIÓN MEJORES PRACTICAS DE CIBERSEGURIDAD NIST.

5.4.1 La evaluación de la perspectiva de ciberseguridad permitió concluir que la UAESP avanzó de un 52% a un 72% con las mejores prácticas en ciberseguridad definidas por el NIST. Sobresale la puntuación obtenida en las funciones RESPONDER y PROTEGER cuyos porcentajes fueron 78% para ambas.

5.4.2 Para las funciones IDENTIFICAR, DETECTAR y RECUPERAR la puntuación obtenida en promedio fueron de 71%, 76% y 60% respectivamente.

5.4.3 Vale la pena resaltar que con base en la evaluación anterior se presenta un avance en el nivel de Ciberseguridad dando como resultado de pasar en el año 2021 de un nivel “INICIAL” a 2022 con un nivel “DEFINIDO”, como se explica con la siguiente ilustración.

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

2021	
Nivel de madurez alcanzado	INICIAL

2022	
Nivel de madurez alcanzado	**DEFINIDO**

Ilustración 4 Nivel de buenas prácticas de Ciberseguridad

5.5 BRECHAS DE AUTODIAGNÓSTICO OTIC 2022 vs. EVALUACIÓN OCI 2022

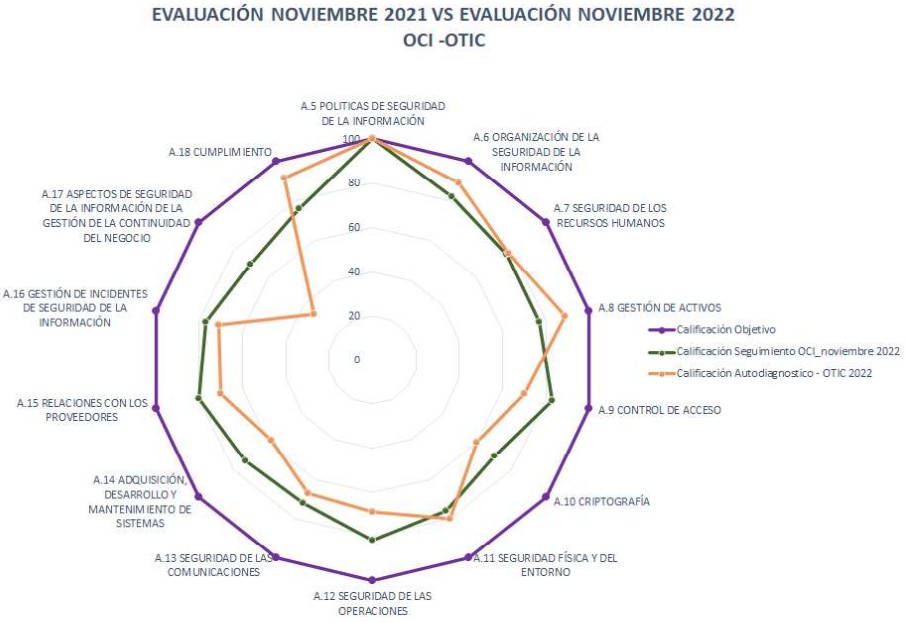

Ilustración 5 Brechas evaluación OCI- OTIC

5.5.1 La OCI hizo análisis detallado del autodiagnóstico ejecutado por la OTIC. La ilustración anterior permite visualizar los Dominios en los cuales se identificaron diferencias entre el autodiagnóstico y la evaluación realizadas este año, arrojando un porcentaje más alto al evaluado por la OCI con un 78% y la OTIC un 73% respectivamente.

5.5.2 A pesar de que las calificaciones en los diferentes dominios fueron distintas, se demuestra una tendencia similar entre la evaluación y el autodiagnóstico, lo cual permite concluir que la OTIC reconoce aquellos aspectos en los que el sistema presenta debilidades y ha trabajado para superarlas.

6 RECOMENDACIONES

A continuación, se presentan las recomendaciones derivadas de las observaciones presentadas por cada uno de los dominios del MSPI, así:

6.1 Dominio AD.1 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

6.1.1 Importante continuar con la socialización y apropiación 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 V3 a funcionarios públicos de la UAESP, a través de estrategias de comunicación que puede ser apoyada por la OACRI.

6.1.2 Continuar con las sensibilizaciones y buscar las estrategias para aumentar la apropiación de los funcionarios a las políticas de seguridad y privacidad de la información.

6.2 Dominio AD.2 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

6.2.1 Definir una metodología o lineamientos para la Gestión de Proyectos que contemple: activos que se involucran en el proyecto, si hay información confidencial, si hay riesgos de seguridad que tengan que ver con el proyecto, entre otras.

6.2.2 Es importante contar con mejores prácticas para el registro y acceso de dispositivos móviles que ingresan a la Entidad más que un registro manual que se hace en la recepción; si es claro, en el manual la política de dispositivos móviles permite el uso de dispositivos móviles de propiedad personal, es importante que se considere que los usuarios tengan un acuerdo de usuario final, en el que se reconocen sus deberes como los establece las condiciones de ítem prueba de este instrumento para este control (AD221).

6.2.3 Incluir en las obligaciones específicas de los contratos las condiciones de seguridad y la obligación de firmar acuerdos de confidencialidad y de niveles de servicio que permitan cumplir con las políticas de seguridad de la información.

6.3 Dominio AD.3 SEGURIDAD DE LOS RECURSOS HUMANOS

6.3.1 Avanzar con un acuerdo de confidencialidad para los servidores públicos que ingresen a la Entidad, en donde se incluye el cumplimiento y conocimiento de las políticas de seguridad y privacidad de la información.

6.3.2 Se recomienda a la Subdirección de Asuntos Legales – SAL, se revise el manual de contratación para evaluar su actualización a la fecha que incluya las firmas correspondientes, ya que el vigente data del año 2020. Así mismo, se complemente o se verifique el cumplimiento del literal h) *"La información sobre todos los candidatos que se consideran para cargos dentro de la organización, se debería recolectar y manejar apropiadamente de acuerdo con la ley de protección de datos personales*". (AD.311).

6.3.3 Considerar la inclusión de socialización y entrega de la política de seguridad y manual de seguridad y su aceptación formal en los procesos de inducción y reinducción con Talento Humano.

6 RECOMENDACIONES

6.3.4 Se recomienda validar con la SAL y Control Interno Disciplinario el procedimiento disciplinario ordinario GDI-PC-02V1 para hacer referencia a las diferentes sanciones tanto a funcionarios o contratistas en caso de poner en riesgo y/o afectar la seguridad de la información de la Entidad por cualquier medio.

6.4 Dominio AD.4 GESTIÓN DE ACTIVOS

6.4.1 Se recomienda actualizar la matriz de activos de información, y a su vez desde la OTIC se cuente con el inventario de activos de hardware (equipos de cómputo y su respectiva hoja de vida actualizada, tema que se evidenció en la evaluación de derechos de autor) y que no solamente se cuente con el inventario de Almacén, con el cumplimiento a los literales de este control que describe el MSPI.

6.4.2 Revisar el Manual GTI-MN-02, para evaluar su posible mejora, ya que se recomienda que se encuentre alineado con la matriz de activos que también incluya activos de hardware.

6.4.3 Definir “lineamiento” o “protocolo” para transferencia de medios físicos que contienen información, donde se contemple un análisis de riesgo de equipos que no se encuentran en la sede principal de la Entidad.

6.4.4 Contar con la “herramienta o solución” para la gestión de medios removibles, para minimizar riesgos de fugas de información por estos medios una vez se cuente con los lineamientos para el etiquetado de información.

6.5 Dominio AD.5 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

6.5.1 Gestionar mayor avance en la estrategia y documentación de continuidad de la operación con el plan de continuidad del negocio y recuperación de desastres – BCP/DRP.

6.5.2 Es importante tener en cuenta la recomendación de la anterior evaluación, en cuanto a la organización y documentación dentro de la parte de arquitectura para los servicios redundantes que se tiene en la Entidad.

6.5.3 Se recomienda contar con el plan de continuidad con su cronograma y pruebas de funcionalidad de los procesos y ejecutarlo.

6.5.4 Se recomienda que los profesionales de la OTIC realicen la respectiva Gestión del Conocimiento (GC) para servicios de misión crítica, lo que implica adquirir, generar, documentar, y transferir en un entorno colaborativo del área, los diferentes procesos que se tienen; ya que el no realizarlo puede generar riesgo de no contar con talento humano que puedan soportar los servicios en caso de ausencia de algún profesional, especialmente en infraestructura. Es decir, se recomienda que se realice no solo del “QUE” se hace sino del “COMO” se hace.

6 RECOMENDACIONES

6.6 Dominio AD.6 CUMPLIMIENTO

6.6.1 Desarrollar de manera general la política de propiedad intelectual con lineamientos, alcance, finalidades y responsables.

6.6.2 Desarrollar el ciclo de vida de la Seguridad y Protección de Datos Personales y su tratamiento como el tema de Habeas Data. Como referencia se puede contar con la guía sobre el tratamiento de datos personales en entidades estatales de la SIC y en la Ley 1581 de 2012.

6.6.3 Gestionar con Gestión Documental la actualización de las Tablas de Retención Documental - TRD, tema que ya se ha evidenciado con otras auditorías.

6.6.4 Contar con una herramienta, metodología, o instrumento donde se evidencie que los lideres de los procesos aseguran el cumplimiento de la política de seguridad de la información.

6.7 Dominio AD.7 RELACIONES CON LOS PROVEEDORES

6.7.1 Implementar un instrumento que contenga los ANS de los diferentes contratos y permita su identificación, consulta y en caso de requerirse solicitar el cumplimiento de manera ágil y de ser necesario, realizar las reclamaciones, devoluciones, descuentos o subsanaciones cómo se hace el seguimiento y cumplimiento del numeral 7.15.2 Lineamientos.

6.7.2 Incluir, verificar y monitorear que en los acuerdos con los proveedores (SIGAB, concesionarios de servicios, ASES-Área de Servicio Exclusivo) se cumpla con los numerales 1 y 2 del control como son: *"1) Indague y solicite evidencia en una muestra de proveedores seleccionada, como la Entidad hace seguimiento, revisa y audita con regularidad de acuerdo con la política la prestación de servicios de los proveedores y el cumplimiento de los compromisos respecto a la seguridad de la información. 2) Indague y evidencie como se gestionan los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, los incidentes de seguridad de la información y la revaloración de los riesgos."* Como lo establece el instrumento del MSPI.

6.7.3 Contar con una sección especial para terceros donde se establezca el acuerdo de confidencialidad cuando se tenga que intervenir con activos de información sensibles y de misión crítica.

6.8 Dominio T.1 CONTROL DE ACCESO

6.8.1 Contar con un lineamiento o procedimiento de gestión de contraseñas sensibles (es decir de administración para servicios de red, bases de datos, sistemas de información, periféricos) donde se defina responsabilidad, periodicidad y custodia.

6.8.2 Establecer mecanismos seguros para la entrega de la primera contraseña manteniendo: "información de autenticación secreta, asegurándose de que no sea divulgada a ninguna otra parte, incluidas las personas con autoridad."

6 RECOMENDACIONES

6.8.3 Se requiere validar la política de expiración de contraseñas, debido a que a algunos usuarios no aplica dicha política.

6.8.4 Coordinar con la SAF y OAP la actualización el procedimiento PC - 11 Paz y salvo V1, ya que este documento data del año 2017 y contiene conceptos desactualizados como por ejemplo en el ítem 5; donde el aplicativo de correo es "Google APPS", El responsable lo identifican como "usuario" ocasionando confusión de roles, etc.

6.9 Dominio T.2 CRIPTOGRAFÍA

6.9.1 Desarrollar más el tema de desarrollo en protección y tiempo de vida de las llaves criptográficas, dentro del Manual de Política que se encuentra en estructuración, y desarrollar procedimiento para la gestión de llaves y sistemas criptográficos.

6.9.2 Validar la implementación de la firma digital de documentos y correos electrónicos (cuando aplique), de tal manera que se minimice el riesgo que se está generando con el uso de firmas escaneadas o digitalizadas que actualmente se está utilizando.

6.9.3 Contar con una herramienta criptográfica para implementarla en los activos de información clasificados como confidenciales.

6.9.4 Realizar capacitaciones periódicas sobre el cifrado de la información responsabilidad de los usuarios. Igualmente, complementar el ítem de Criptografía con sus respectivos controles del modelo.

6.10 Dominio T.3 SEGURIDAD FÍSICA Y DEL ENTORNO

6.10.1 Validar en conjunto con la Subdirección Administrativa y Financiera - SAF, un análisis de identificación de riesgos ambientales para establecer los mecanismos para su mitigación, y también verificar el cumplimiento de las restricciones de acceso al cuarto eléctrico en tanto que el presente año se materializó el riesgo de corte eléctrico.

6.10.2 Verificar en la sede administrativa de la UAESP que los perímetros cuenten con controles de seguridad verificables en especial el Data Center, centros de cableados de datos, cuarto eléctrico. No hay evidencia de identificación de perímetros de seguridad en ubicaciones (sedes) alternas donde opera la UAESP.

6.10.3 Contar con los directorios y guías telefónicas internas que identifican los lugares de las instalaciones de procesamiento de información confidencial no deben ser accesibles a ninguna persona no autorizada.

6.10.4 Se recomienda dada la materialización de riesgo en el cuarto eléctrico y a su vez lo que se pueda presentar por riesgos eléctricos, realizar la socialización y medición de las directrices de protección para equipos con riesgos y amenazas, peligros del entorno, y las oportunidades para accesos no autorizados y que la Entidad cuente con un profesional que tenga estos conocimientos de electricidad.

6.10.5 Contar con mecanismos configurados para evitar el uso no autorizado de las fotocopiadoras de la Entidad (ejemplo: establecer contraseñas). También importante unificar el papel tapiz de los equipos complementando la política de escritorio limpio.

6 RECOMENDACIONES

6.11 Dominio T.4 SEGURIDAD DE LAS OPERACIONES

6.11.1 Contar con un instrumento (tablero de control) para monitorización de la plataforma donde se registren las acciones realizadas; es decir, detallar el evento, la solución, categoría, incidencia y servicio como insumo para la toma de decisiones en el ciclo de mejoramiento continuo.

6.11.2 Es importante que para medir la gestión de la capacidad futura que se cuente con un lineamiento donde se verifique no solo la capacidad de almacenamiento sino también se tenga el análisis de desempeño, historial, planes de expansión de servicios, migraciones a nube, etc.; es decir, una planificación que proyecte la infraestructura tanto de servidores como de demás dispositivos con base en su mantenimiento preventivo y correctivo.

6.11.3 Es importante que las pruebas de restauraciones de Backups sean de manera más periódica y validar la posibilidad de implementar y/o contemplar un formato que permita identificar rápidamente la disposición final de todas las copias de seguridad de la información respaldada y de esta forma disminuir los tiempos de recuperación.

6.11.4 Incluir pruebas de integridad de los Backups en los informes, y realizar su seguimiento. A su vez se recomienda que se haga análisis de reportes de las herramientas y acciones consecuentes.

6.11.5 Actualizar y fortalecer los informes del SIEM y hacer análisis de los reportes de las herramientas que además permita controles periódicos preventivos e investigaciones a incidentes, como también complementar el SIEM con la totalidad de los sistemas.

6.11.6 Se recomienda validar la efectividad de las actualizaciones del sistema operativo y antivirus.

6.11.7 Se recomienda contar con inventario actualizado tanto del software de usuario final como el de administradores de la(infraestructura).

6.12 Dominio T.5 SEGURIDAD DE LAS COMUNICACIONES

6.12.1 Verificar la actualización de contraseñas y políticas del Directorio Activo - DA, no todos los usuarios tienen esta sincronización.

6.12.2 Verificar y socializar el cumplimiento de: *"Advertencia del tratamiento de la información en la firma de los correos electrónicos"*.

6.12.3 Socializar a la planta de la Entidad sobre *"la capacidad de encriptado de los correos"*

6.12.4 LA OCI recomienda continuar con el plan de bloqueo de los puertos de USB, para mitigar el riesgo de ataque en la Entidad por esta vía.

6.12.5 Contar con un acuerdo de confidencialidad formal con lineamientos de confidencialidad, no divulgación, integridad, disponibilidad, autenticidad, seguridad de la información para cuando se trasmita o consulte información a otras entidades.

6.13 Dominio T.6 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

6.13.1 Avanzar con la definición de lineamientos definida en la política y se complemente con los temas de propiedad intelectual y derechos de autor.

6 RECOMENDACIONES

6.13.2 La OCI recomienda realizar el etiquetado de la información y desplegar los mecanismos de defensa tipo DLP para asegurar la información.

6.13.3 Configurar el MFA *(del inglés Multi Factor Authentication)* en especial para los administradores de sistemas.

6.13.4 Definir unos lineamientos y/o directrices que establezca que todos los requerimientos de TIC sean validados y atendidos por la Oficina de TIC para evitar que algún área realice adquisiciones que pongan en peligro la seguridad de la información.

6.13.5 Una vez aprobado el manual de PSI, contar con un acuerdo o autorización formal para uso de información de pruebas cuando se utilicen datos personales para el desarrollo del ejercicio.

6.13.6 Contar con una herramienta para el control de la metodología de desarrollo, así como gestionar requerimientos, planeación, tiempos de desarrollo, historia de usuarios, etc. Igualmente, se recomienda realizar seguimientos periódicos a los cronogramas de desarrollo y dar cumplimiento de lo proyectado vs lo ejecutado, de ser necesario reprogramar fechas mediante un acta documentada.

6.13.7 Se recomienda contar con controles de integridad en los despliegues (especialmente ORFEO, y a su vez tener presente este control *"evaluar el impacto, si la organización llega a ser responsable del mantenimiento futuro del software como resultado de los cambios"*.

6.13.8 Se recomienda tener lineamientos donde se establezcan programas de pruebas de seguridad de la información y de detección de incidentes realizarlo periódicamente, y no tener que realizar *rollback* como sucedió con ORFEO una vez estaba ya en producción.

6.13.9 La OCI, con relación al literal; "*k) Asegurar que la documentación de operación y los procedimientos de los usuarios experimenten los cambios que les permitan seguir siendo apropiados"*, de lo que pide el instrumento de MSPI, validar la vigencia de los manuales de operación de los aplicativos. el procedimiento en desarrollo con algunos formatos o instrumentos para diferenciar desarrollo en los tres escenarios: Adquirir software comercial, desarrollo de software de terceros, desarrollo software interno.

6.13.10 Se recomienda tener en cuenta aplicativos externos como SIGAB, para el cumplimiento de los controles solicitados.

6.14 Dominio T.7 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

6.14.1 Contar con un plan de respuesta específico para los incidentes que se clasifiquen y categoricen.

6.14.2 Se debe revisar la pertinencia de ampliar el alcance de los controles, con el objetivo de cubrir los operadores externos.

RECOMENDACIONES GENERALES DEL MSPI

i. De otra parte, para el desarrollo del tema de protección de datos personales se sugiere tener presente la *"Guía sobre el tratamiento de datos personales en las entidades estatales 2021"* de la SIC.

6 RECOMENDACIONES

ii. Evaluar contar como apoyo una herramienta o software de gestión para poder validar y gestionar los diferentes controles de MSPI, entre ellos los riesgos, incidentes, reportes, documentación, indicadores, etc.

iii. Conforme a las mejores prácticas, la transferencia de conocimiento es fundamental en la gestión del talento humano. De esta manera tanto funcionarios como contratistas deben contar con conocimiento redundante, que por la ausencia de un miembro no se afecte la seguridad de la información y la infraestructura.

iv. Dentro del proyecto de actualización de la plataforma de gestión documental ORFEO se recomienda que se tenga en cuenta, si no lo tiene o no lo han contemplado, las tres maneras de remitir comunicados: con documento adjunto, formulario de mensaje o mensaje tipo correo electrónico que se puedan firmar de las maneras: digitalizada escaneada, digital, electrónica o con la trazabilidad del sistema. Esto permitirá cumplir de la mejor manera las condiciones de autenticidad y no repudio de los pilares de seguridad de la información.

v. Validar con la actualización de ORFEO, la depuración y gestión del directorio de funcionarios y contratistas una vez finalizada su vinculación.

vi. Se recomienda que se valide prioritariamente la implementación de la Política de Propiedad Intelectual y Derechos de Autor.

APROBACIÓN:

Sandra Beatriz Alvarado Salcedo Firmado digitalmente por Sandra Beatriz Alvarado Salcedo Fecha: 2022.11.25 14:34:40 -05'00' **Jefe(a) de Oficina de Control Interno**	 **Auditor(es) Interno(s)**

FECHA[4]:

24 – 11 – 2022

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