Bogotá D.C., 11 de noviembre de 2021

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

DE: Oficina de Control Interno

Asunto: Evaluación del Modelo de Seguridad y Privacidad de la Información 2021

Apreciado Ingeniero Beltrán:

De conformidad con el Plan Anual de Auditorías 2021, 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 de implementación de este se concluye que la implementación paso de estado "EFECTIVO a GESTIONADO" respecto de la implementación del mismo, 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 diciembre de 2020 pasando de 54% a un 63% en escala de calificación, dando avance a los lineamientos de la Resolución 500 del MinTIC de 2021. Es importante continuar avanzando con los Dominios que aún se encuentran con avance inferior.

Igualmente, en cuanto al modelo de operación del PHVA **se evidencia avance pasando del 51% en la vigencia 2020 al 67% en esta vigencia 2021.** 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.

Por su parte, dentro de las mejores prácticas de Ciberseguridad (NIST) se observa un avance de esta perspectiva lo cual permite que la UAESP haya avanzado de un 35% a un 52% con base en las mejores prácticas en ciberseguridad definidas por el NIST. Sobresale la puntuación obtenida en las funciones PROTEGER e INDENTIFICAR cuyos porcentajes fueron 67% y 63% respectivamente. Sin embargo, para las funciones DETECTAR, RESPONDER y RECUPERAR la puntuación obtenida en promedio fue de 42,5%, lo cual se ve reflejado en los Dominios A.10, A14, A16, A17, de los cuales también son importantes para la gestión de TI, y se deben ahondar esfuerzos para avanzar en las funciones más débiles.

De otra parte, si bien es cierto que hay un avance con referencia a la evaluación anterior, aún sigue siendo bajo con referencia a la implementación total del modelo. Es así que se

Bogotá D.C., 11 de noviembre de 2021

deben emprender esfuerzos para continuar avanzando; por lo tanto, es importante que se valide y se contemple si continúan con las mismas acciones y/o adicionar nuevas con base en los hallazgos de esta auditoría para que sean más eficaces y efectivas de tal manera que permitan llegar a buen término en el proceso de implementación total del modelo.

En el informe anexo (virtual) podrá detallar y analizar junto con su equipo de trabajo la reiteración de la No Conformidad. Así mismo, podrán pormenorizar sobre las cinco (5) fortalezas, las catorce (14) observaciones agregadas, catorce (14) recomendaciones de los Dominios y diez (10) recomendaciones generales del MSPI en el marco de esta auditoría interna.

Por último, estaremos atentos para concertar una reunión virtual de socialización de los resultados y detalles del proceso de auditoria llevado a cabo. De esta manera quedamos atentos a la construcción de un plan de mejoramiento de los hallazgos de acuerdo con lo establecido en el procedimiento “PC-03 PM acciones correctivas preventivas y de mejora V9”, el cual se debe entregar 10 días hábiles después de recibido el presente informe

Cordialmente,

ANDRES PABON SALAMANCA
Jefe Oficina de Control Interno
e-mail: andres.pabon@uaesp.gov.co

Elaboró: Ligia Marlén Velandia León – PE.224-22 OCI.
Anexo: 2 archivos virtuales (Informe y anexo instrumento evaluación)

Informado: Dirección General.

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 EVALUACION DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2021 - UAESP**			
PROCESO, PROCEDIMIENTO, Y/O DEPENDENCIA	OFICINA DE TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES			
RESPONSABLE Y/O AUDITADOS	Ing. Cesar Beltrán, Paola Murcia, Osbaldo Cortés, 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) e ISO 27001.**			
ALCANCE	Sistema de Gestión de Seguridad de la Información vigente a octubre de 2021, teniendo en cuenta los controles que según auditoría anterior generaron porcentaje menor o igual a 60 en puntaje.			
PERIODO DE EJECUCIÓN	Del 06/10/2021 al 16/11/2021			
EQUIPO AUDITOR	Andrés Pabón Salamanca – APS, Ligia Marlén Velandia León – LMVL			
DOCUMENTACIÓN ANALIZADA (4)	- **DECRETO 1008 DE 2018 -** POLITICA DE GOBIERNO DIGITAL - **CONPES 3995 JULIO DE 2020 –** POLITICA 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 G10. - **PROCEDIMIENTOS OTIC** - VIGENTES - **DOCUMENTACIÓN MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN** – MSPI VIGENTE EN LA UAESP. - **PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN -** VIGENTE EN LA UAESP. - **PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA**			

	INFORMACIÓN – VIGENTE EN LA UAESP - **INVENTARIO DE APLICATIVOS** – VIGENTE EN LA UAESP - **NORMA ISO 27001** - **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

En el Plan Anual de Auditorías de 2021, la Oficina de Control Interno dando cumplimiento al Plan, procedió a planificar y desarrollar la auditoria de MSPI con radicado 20211100049793 del 07 de octubre de 2021, cuyo propósito consistió en realizar la evaluación de los controles que de la auditoría de 2020 tuvieron una puntuación de 60 o menor. Por tanto, los que se encontraban por encima de esta calificación se les asignó el valor de la evaluación anterior, por lo cual se evaluaron 22 controles administrativos y 50 controles técnicos para un total de 72 controles de 114 que corresponden al modelo del 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 Ministerio de TIC e ISO 27001:2013. Su ejecución comprendió el período comprendido entre octubre 6 y noviembre 16 de 2021.

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 puntuables 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 anteriores 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 del instrumento de medición frente a las mejores prácticas en ciberseguridad definidas por el NIST, lo cual permitió generar un diagnóstico de cinco (5) funciones básicas (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.

Finalmente, la evaluación producto de esta auditoria fue comparada con la evaluación realizada en la vigencia de 2020 con el fin de determinar los criterios con los cuales se ha identificado avance y también aquellos que suponen emprender acciones de mejora.

1. DESCRIPCIÓN GENERAL DEL DESARROLLO DE LA AUDITORIA

LIMITACIONES DE AUDITORÍA: La auditoría bajo modalidad de trabajo en casa pudo haber restringido las observaciones en sitio de las evidencias de aplicación de los controles para aplicación del MSPI. No obstante, se programaron reuniones en plataformas tecnológicas para hacer entrevistas tanto en sitio como virtualmente que permitieron hacer aclaraciones a las evidencias presentadas con las limitaciones propias del trabajo remoto. Así mismo, uno de los auditores reubicados a la Oficina, luego de solicitud de recursos, dada su calidad de pre-pensionado, solicito renuncia a partir del 2 de noviembre de los corrientes.

2. CONFORMIDADES Y FORTALEZAS

2.1. **Conformidad: Dominios con incremento en el nivel de efectividad de controles.** Luego de realizar la evaluación de efectividad de los controles contemplados en el anexo A de la norma ISO 27001:2013, se evidenciaron incrementos en los niveles de valoración para seis (6) Dominios del sistema referenciado. En los seis (6) dominios que incrementaron su nivel de calificación, se evidencia que los controles se monitorean verificando el cumplimiento de los procedimientos para tomar acción cuando no funcionan eficientemente. La calificación resultante de la evaluación de esta auditoría se resume en la tabla que sigue:

No.	DOMINIO	Calificación Seguimiento diciembre 2020	Calificación Seguimiento octubre 2021	EVALUACIÓN DE EFECTIVIDAD DE CONTROL 2020	EVALUACIÓN DE EFECTIVIDAD DE CONTROL 2021	AVANCE
1	A.5 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	80	80	GESTIONADO	GESTIONADO	**IGUAL**
2	A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	58	61	**EFECTIVO**	**GESTIONADO**	**AVANZO**
3	A.7 SEGURIDAD DE LOS RECURSOS HUMANOS	71	71	GESTIONADO	GESTIONADO	**IGUAL**
4	A.8 GESTIÓN DE ACTIVOS	62	69	GESTIONADO	GESTIONADO	**IGUAL**
5	A.9 CONTROL DE ACCESO	75	76	GESTIONADO	GESTIONADO	**IGUAL**
6	A.10 CRIPTOGRAFÍA	30	60	**REPETIBLE**	**EFECTIVO**	**AVANZO**
7	A.11 SEGURIDAD FÍSICA Y DEL ENTORNO	69	71	GESTIONADO	GESTIONADO	**IGUAL**
8	A.12 SEGURIDAD DE LAS OPERACIONES	41	61	**EFECTIVO**	**GESTIONADO**	**AVANZO**
9	A.13 SEGURIDAD DE LAS COMUNICACIONES	63	68	GESTIONADO	GESTIONADO	**IGUAL**
10	A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	40	42	**REPETIBLE**	**EFECTIVO**	**AVANZO**
11	A.15 RELACIONES CON LOS PROVEEDORES	60	70	**EFECTIVO**	**GESTIONADO**	**AVANZO**

2. CONFORMIDADES Y FORTALEZAS

12	A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	17	43	**INICIAL**	**EFECTIVO**	**AVANZO**
13	A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	26,5	33,5	REPETIBLE	REPETIBLE	**IGUAL**
14	A.18 CUMPLIMIENTO	61	71	GESTIONADO	GESTIONADO	**IGUAL**
	PROMEDIO EVALUACION DE CONTROLES	**54**	**63**	**EFECTIVO**	**GESTIONADO**	**AVANZO**

2.2. **Fortaleza: Dominios con avance significativo.** La siguiente tabla resume los Dominios en los cuales se observó que, aunque mantienen el nivel de efectividad respecto a la evaluación de 2020, reflejan aumento porcentual significativo en la evaluación de 2021.

No.	DOMINIO	Calificación Seguimiento diciembre 2020	Calificación Seguimiento octubre 2021	EVALUACIÓN DE EFECTIVIDAD DE CONTROL 2020	EVALUACIÓN DE EFECTIVIDAD DE CONTROL 2021	EFECTIVIDAD
1	A.10 CRIPTOGRAFÍA	30	60	REPETIBLE	EFECTIVO	AVANZO
2	A.12 SEGURIDAD DE LAS OPERACIONES	41	61	EFECTIVO	GESTIONADO	AVANZO
3	A.15 RELACIONES CON LOS PROVEEDORES	60	70	EFECTIVO	GESTIONADO	AVANZO
4	A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	17	43	INICIAL	EFECTIVO	AVANZO

2.3. **Fortaleza: Documentación, Gestión y Aprobación de Política de Seguridad, Procedimiento Gestión de Incidentes; en proceso Manual de Políticas de Seguridad de la Información y demás procedimientos e instructivos.** Se evidencian esfuerzos importantes con la realización de documentación; es decir, se ha evolucionado en la construcción de los procedimientos, guías, formatos e instructivos del MSPI.

2.4. **Fortaleza: Seguimiento 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 de los colaboradores de la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC, y a su vez se evidencia un Talento Humano competente y comprometido para desarrollar las diferentes actividades que contribuyen al logro de objetivos institucionales.

2.5. **Fortaleza: Resolución 446 de 2021.** Por la cual se determina un delegado responsable del MSPI, 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. CONFORMIDADES Y FORTALEZAS

2.6. Fortaleza: Plan de Sensibilización de MSPI – Matriz de Activos de Información. Durante el desarrollo de la auditoría se evidenció que la OTIC ha demostrado su compromiso y esfuerzo por propender en la UESP por "*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. Se demuestra un importante avance en la documentación del Sistema de Gestión de Seguridad de la Información - SGSI, la que se ha venido perfeccionando y complementando de manera alineada con la aplicación de los controles definidos dentro del modelo de seguridad y privacidad de la información, quedando pendiente algunas mejoras que se identifican en este informe.

3. OBSERVACIONES

Dominios con bajos niveles de efectividad en los controles. La siguiente tabla resume los Dominios del sistema que se mantienen en niveles tempranos (Repetible y Efectivo) de la implementación del MSPI. Si bien es cierto que se presentó avance en su evaluación de los cuales dos (2) Dominios pasaron de nivel Repetible a nivel Efectivo, aún hay un Dominio continúa en nivel Repetible.

No.	DOMINIO	Calificación Seguimiento diciembre 2020	Calificación Seguimiento octubre 2021	EVALUACIÓN DE EFECTIVIDAD DE CONTROL 2020	EVALUACIÓN DE EFECTIVIDAD DE CONTROL 2021	AVANCE
1	A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	40	42	**REPETIBLE**	**EFECTIVO**	**AVANZO**
2	A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	17	43	**INICIAL**	**EFECTIVO**	**AVANZO**
3	A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	26,5	33,5	**REPETIBLE**	**REPETIBLE**	**IGUAL**

3.1. Observación. Adquisición, Desarrollo y Mantenimiento de Sistemas. El manual de adquisición, desarrollo y mantenimiento seguro de software aún se encuentra en etapa de desarrollo; por lo tanto, es importante garantizar que se implementen sistemas y aplicaciones en el marco de un desarrollo seguro. Sería importante considerar la metodología de desarrollo basado en Scrum.

3.1.1. No se cuenta aún con definición de un documento o política complemento de la minuta de contrato de prestación de servicios SECOP II, donde se tengan en cuenta las diferentes sanciones al contratista que no acate la seguridad de la información de la entidad. Con base

3. OBSERVACIONES

en la reunión del 23 de noviembre se realizó claridad para interpretación. **Observación: 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.** Al respecto el equipo de OTIC solicita involucrar en esta observación a la SAL quien es la líder del proceso de contratación. Una vez analizada la observación de OTIC, la OCI recomienda que este sea claro, conciso, que si se puede hacer un anexo mucho mejor del tema evitando interpretaciones inequívocas; es así que se concluye que se debe realizar un trabajo articulado entre OTIC y SAL para que se determine la mejor forma para las partes, pero con especial atención para la UAESP frente a los posibles incumplimientos más allá de establecerlo de manera complementaria en la minuta, recomendamos se detalle en el anexo de conformidad con el servicio, producto, o contrato de prestación de servicios. (ejemplo: fichas azules – áreas misionales).

3.1.2. Tampoco se cuenta con lineamientos, o una directriz documentada, aprobada, socializada para que la adquisición de software sea siempre validada por la OTIC, como los requerimientos técnicos a lugar (infraestructura, controles de seguridad, tipos de licenciamientos, mantenimientos posteriores, entre otros). Y a su vez que OTIC entregue un concepto técnico de la evaluación respectiva.

3.1.3. Para los servicios de seguridad de servicios de las aplicaciones que utilizan redes públicas con base en los mismos lineamientos que se proponen en el control, el avance está en etapa inicial. Dada la reunión del 23 de noviembre/21 para esta observación OTIC manifiesta contar con el control planteado dentro del Manual; sin embargo, es importante que se complemente este punto para redes públicas por el uso masivo de las mismas (por teletrabajo) en las aplicaciones (ejemplo contar con doble autenticación cuando no se use VPN). **Observación: Para los servicios de seguridad de las aplicaciones que utilizan redes públicas que están en los objetivos descritos en el Manual de PSI, 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**.

3.1.4. 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).

3.1.5. Para realizar pruebas de seguridad controladas no se evidencia un procedimiento que establezca los pasos a seguir. Al verificar con el equipo el día 23 de noviembre/21 al reevaluarla en esta reunión se concluye que se cumple y se levanta esta observación por cuanto esta hace referencia según el control es a desarrollo de software. Por lo tanto, se describe así**: Observación: En las pruebas de seguridad para desarrollo de software se observa el procedimiento proyectado, pero aún en proceso de aprobación; por lo tanto, es necesaria su formalización para que se consolide su aplicabilidad en atención al instrumento del MinTIC**.

3.1.6. 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.

3.2. Observación. Gestión de Incidentes de Seguridad de la Información. 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.

3.2.1. No se evidencia un consolidado, matriz, bitácora o instrumento donde se reflejen los

3. OBSERVACIONES

incidentes de seguridad y clasificación de estos, pues en la herramienta de Help People, no sólo se ingresan los incidentes de seguridad, sino la solicitud de soporte y requerimientos de usuarios. Con base en reunión del 23 de noviembre/21 se amplía el contexto de la observación respectiva. **Observación: No se evidencia un consolidado, matriz, bitácora o instrumento donde se reflejen todos los incidentes de seguridad presentados en el período, solo los de carácter masivo de gran afectación más no los particulares que se han notificado por diversos medios, sin utilizar la herramienta de mesa de ayuda Help People para tener su trazabilidad y análisis**. Mediante correo de noviembre 26/21, OTIC solicita aclarar la frase "los particulares que se han notificado por diversos medios", ya que la OTIC tiene dispuestos los siguientes canales de atención para recibir los incidentes: Herramienta HelpPeople y Correo de Soporte, y a partir del reporte se da la atención correspondiente. La OCI aclara que la expresión "los particulares que se han notificado por diversos medios" se refiere al conocimiento manifestado en las reuniones de que hubo incidentes no registrados en las herramientas dispuestas por la OTIC ni en la bitácora, pero que, si se informaron por correo diferente al de soporte, por mensaje de WhatsApp o verbalmente, sin quedar en la bitácora como analizados y atendidos, así se haya determinado que no eran propiamente incidentes, pero si afectaron a usuarios particulares. Es así que, aunque se cuenta con mecanismos establecidos por la entidad como la herramienta de Help People y correo se recomienda que se integren o vinculen otros mecanismos o medios de comunicación para reporte de posibles incidentes (ejemplo: WhatsApp, línea de contacto celular, etc.) y posteriormente estos sean registrados con la atención dada, toda vez que se pueden presentar incidentes que requieren solución prioritaria propias del ejercicio, y dada la dinámica actual de trabajo en casa.

3.2.2. No se evidencia contar con un plan de respuestas para los diferentes incidentes que se presenten una vez clasificados o categorizados.

3.2.3. No se evidencia documentación o consolidación de información que permitan determinar lecciones aprendidas para mitigar incidentes futuros.

3.2.4. No se comprueban lineamientos para recolección de evidencias; que faciliten la implementación de un archivo o instrumento de lecciones aprendidas.

3.2.5. Si lo anterior se puede gestionar en la herramienta de HelpPeople, no se evidencian estos registros con: responsables, la descripción del incidente, acciones correctivas y de contención, lecciones aprendidas y posibles vulnerabilidades.

3.3. **Observación. Aspectos de Seguridad de la Información y de la Gestión de la Continuidad del Negocio.** 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.

3.3.1. 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 DRP (BCP-DR) en alta disponibilidad para contar con una solución de restablecimiento de servicios de manera ágil.

3.3.2. 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

3. OBSERVACIONES

planeación de la implementación del DRP, sin haber validado en su momento estas situaciones.

3.3.3. 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.

3.4. Observación: Dominios con niveles promedio de efectividad en los controles. La siguiente tabla muestra el resumen de los Dominios del sistema que pasan a niveles promedios (Efectivo y Gestionado) de la implementación del MSPI.

No.	DOMINIO	Calificación Seguimiento diciembre 2020	Calificación Seguimiento octubre 2021	EVALUACIÓN DE EFECTIVIDAD DE CONTROL 2020	EVALUACIÓN DE EFECTIVIDAD DE CONTROL 2021	AVANCE
1	A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	58	61	**EFECTIVO**	**GESTIONADO**	**AVANZO**
2	A.10 CRIPTOGRAFÍA	30	60	**REPETIBLE**	**EFECTIVO**	**AVANZO**
3	A.12 SEGURIDAD DE LAS OPERACIONES	41	61	**EFECTIVO**	**GESTIONADO**	**AVANZO**

3.5. Observación. Organización de la Seguridad de la Información. Una vez verificada la documentación y validada en reuniones se observa que:

3.5.1. 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. En cuanto al ingreso de aplicaciones se encuentra ORFEO integrado con LDAP, mientras que SI CAPITAL se realiza manual. Con base en el correo de 26 de noviembre/21 la OTIC solicita dividir la observación, ya que las acciones de mejora serian diferentes. La OCI valida este punto y se procede a independizar las observaciones a lugar: **Observación 1: 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. Observación 2: En cuanto al ingreso de aplicaciones se encuentra ORFEO integrado con LDAP, mientras que SI CAPITAL se realiza manual**.

3.5.2. 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.

3.5.3. Dada la emergencia sanitaria los funcionarios y contratistas tienen en su mayoría modalidad de teletrabajo y con modalidad BYOD *(del inglés Bring Your Own Device)* con dispositivos de uso personal, para los cuales no se evidencia suficientes controles de

3. OBSERVACIONES

acceso sino únicamente VPN *(del inglés Virtual Private Network)* para que algunos usuarios puedan acceder a aplicativos críticos específicos de su rol.

3.6. Observación. Criptografía.

3.6.1. 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.

3.6.2. 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.

3.6.3. No se evidencia aún un procedimiento para la gestión de llaves y sistemas criptográficos, una vez quede en firme el Manual de Política de Seguridad de la Información desarrollado.

3.7. Observación. Seguridad de las Operaciones. Se evidencia un procedimiento de gestión de cambios aún en borrador. Por lo tanto, no se observa seguimiento formal y documentado de los cambios a los sistemas de información, aplicativos o bases de datos de la Entidad.

3.7.1. 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.

3.7.2. 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.

3.7.3. 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.

3.7.4. Si bien es cierto que se realizan análisis de vulnerabilidades (página web), según reunión, no se evidencia gestión en auditorías preventivas a los sistemas de información. 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. Con base en reunión del 23 de noviembre/21 se complementa la observación. **Observación**: **Si bien es cierto que se realizan análisis de vulnerabilidades (página web, ORFEO), según reunión, no se evidencia 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**.

3. OBSERVACIONES

3.8. Observaciones. Dominios con niveles de efectividad más alta en los controles. La siguiente tabla muestra los Dominios del sistema que se mantienen en niveles promedio (Gestionado) de la implementación del MSPI.

No.	DOMINIO	Calificación Seguimiento diciembre 2020	Calificación Seguimiento octubre 2021	EVALUACIÓN DE EFECTIVIDAD DE CONTROL 2021	OBSERVACIONES
1	A.5 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	80	80	GESTIONADO	1. Aún pendiente acto administrativo que adopta la Política General de Seguridad y Privacidad de la Información.
2	A.7 SEGURIDAD DE LOS RECURSOS HUMANOS	71	71	GESTIONADO	1. El Manual de Política de Seguridad de la Información aún en proceso de formalización y adopción. 2. No se evidencian los acuerdos de confidencialidad que deben diligenciar y firmar todos los servidores públicos y contratistas que ingresen a la Entidad, en donde se incluye el cumplimiento y conocimiento de las políticas de seguridad de la información. Ello es independiente de la minuta de contrato de SECOP II.
3	A.8 GESTIÓN DE ACTIVOS	62	69	GESTIONADO	1. 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). 2. 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. 3. 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. 4. Según reunión se evidencia debilidad en la gestión del directorio, en particular, en el aplicativo ORFEO por

3. OBSERVACIONES

					cuanto cuenta aún con debilidades al finalizar vinculación de funcionarios y contratistas no se desactivan ágilmente.
4	A.9 CONTROL DE ACCESO	75	76	GESTIONADO	1. 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. 2. Aunque en reunión el líder de infraestructura y el DBA manifestaron el control y gestión de contraseñas, en el aplicativo KeePass no se evidencia lineamientos o procedimientos de gestión de contraseñas sensibles; es decir, de administradores para servicios de red, bases de datos, sistemas de información, periféricos, donde se defina nivel de responsabilidad, periodicidad, custodia, criticidad, etc.
5	A.11 SEGURIDAD FÍSICA Y DEL ENTORNO	69	71	GESTIONADO	1. 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. 2. En visita al centro de datos *(DC Data Center)* se evidencia desorganización del cableado estructurado. 3. 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.
6	A.13 SEGURIDAD DE LAS COMUNICACIONES	63	68	GESTIONADO	1. 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. Con base en el correo de 26 de noviembre/21 la OTIC solicita respetuosamente ampliar el contexto. La OCI, precisa que se trata de los acuerdos sobre transferencia de información; es decir, los asuntos de seguridad que se hayan convenido con las entidades con las que se intercambia información para garantizar su integridad, confidencialidad y disponibilidad.

3. OBSERVACIONES

					Durante la auditoría no se presentó documento alguno de formalización de acuerdos si los hay.
7	A.15 RELACIONES CON LOS PROVEEDORES	60	70	GESTIONADO	1. No se evidencia acuerdos de niveles de servicio - ANS para proveedores que tengan acceso a los activos de información, formalizados en la minuta o anexos del contrato que indique criticidad, tiempos de atención, tiempos de solución y descuentos por incumplimientos. Solo aparece un tope para atender llamada y de solución sin considerar la criticidad y nivel de afectación de los servicios tecnológicos (ej. ETB). Un ANS debe tener tiempos de atención y solución conforme criticidad, protocolo de escalamiento en caso de superar tales tiempos y sanción o descuentos por incumplimiento de estos, entre otros. Con base en el correo de noviembre 26/21 la OTIC manifiesta los siguiente: De las modalidades de selección previstas en la Ley 1150 de 2007, la Contratación directa es el procedimiento mediante el cual la entidad estatal contrata directamente con una persona natural o jurídica, para el caso con la empresa ETB la prestación de servicios de conectividad y telecomunicaciones. Esta modalidad contractual no es competitiva, es decir, se planea para la contratación directa con el proveedor directo y exclusivo que cumple con la necesidad en todos sus entornos, él debe presentar la oferta técnico-económica con los detalles de la prestación del servicio, esta oferta es pre-requisito obligatorio para legalizar el contrato y proceder a la firma del mismo previo cumplimiento a todo los requisitos técnicos, legales, financieros. De acuerdo con lo anterior la ETB presenta oferta económica en la cual se detalla la prestación del servicio con sus ANS, matriz de escalabilidad, porcentajes de disponibilidad e indisponibilidad del servicio, así como su respectiva tasación en caso de interrupción o afectación del servicio. Con lo anterior OTIC precisa que el documento no está dentro de la minuta del contrato sino dentro del documento denominado oferta económica. La OCI al verificar este documento encuentra los ANS y la OTIC acepta que este documento hace parte del contrato en virtud de la normatividad. De acuerdo con lo anterior, se evidencia cumplimiento del requisito. En todo caso es importante complementar con lo que se está desarrollando en el Manual PSI, en lo que hace referencia a relación con proveedores, y sería importante considerar contar con un anexo

3. OBSERVACIONES

					técnico al contrato que trate específicamente los ANS. 2. 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.
8	A.18 CUMPLIMIENTO	61	71	GESTIONADO	1. 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. 2. 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.

o

4. SOLICITUD DE CORRECCIÓN Y ACCIONES CORRECTIVAS

No.	DESCRIPCIÓN DE LA NO CONFORMIDAD	REQUISITO QUE INCUMPLE
1	Se mantiene la No Conformidad que se generó en la auditoría anterior, por cuanto se obtiene una calificación de 63% en la implementación del MSPI en la UAESP, siendo su objetivo el 100% con base en los lineamientos del MinTIC. Es decir, se evidencia avance pasando a una escala de calificación de EFECTIVO, aunque debiendo estar en OPTIMIZADO. Por tanto, es importante reforzar las acciones a tomar para completar la implementación total del modelo de acuerdo con lo establecido en la normatividad.	Decreto 1078 de 2015, en el Titulo 9, Capitulo 1, Sección 3. (Política de Seguridad Digital, MIPG). Resolución 500 de 201 del MinTIC. Directiva Presidencial 03 de 2021.

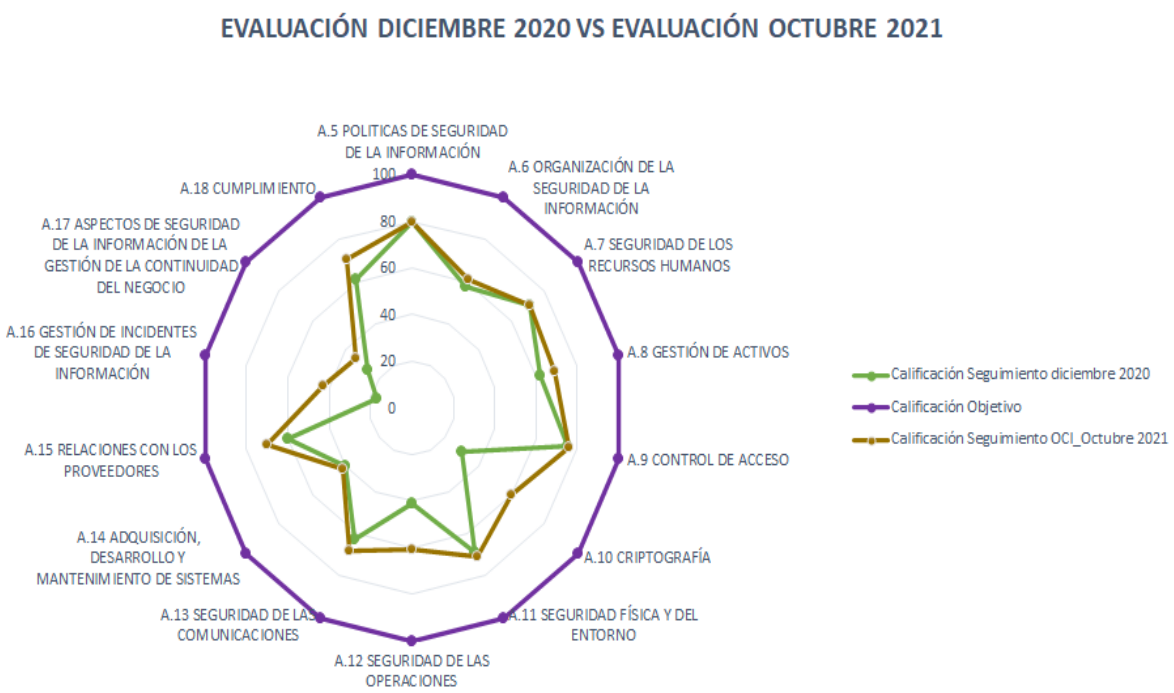
5. CONCLUSIONES

5.1. **EVALUACIÓN DE EFECTIVIDAD DE CONTROLES MSPI 2021:**

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 63% frente al 54%

5. CONCLUSIONES

obtenido en la evaluación de la vigencia 2020. El avance de 9 puntos porcentuales está dado con base en la verificación de controles que se encontraban bajos con una calificación de 60 o menor frente a la calificación objetivo (100%). 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 encuentran aún en etapas tempranas de avance mientras que los de puntaje que se encontraban mayores a 60 ya se encuentran en niveles más avanzados de implementación.



5.1.2. **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 desde la evaluación anterior pasando de *EFECTIVO a GESTIONADO* lo cual significa que buena parte de los dominios, procesos, procedimientos y controles se documentan y se comunican, aunque falten indicadores de gestión. El objetivo del MSPI 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. Se evidencia que la OTIC ha mejorado en la implementación de los controles de seguridad para los activos de información: redes, software base, software aplicativo, archivos y recurso humano. Esto aunado con que se han atendido la mayoría de las recomendaciones emitidas en las auditorías anteriores que se evidencia con el avance demostrado.

5. CONCLUSIONES

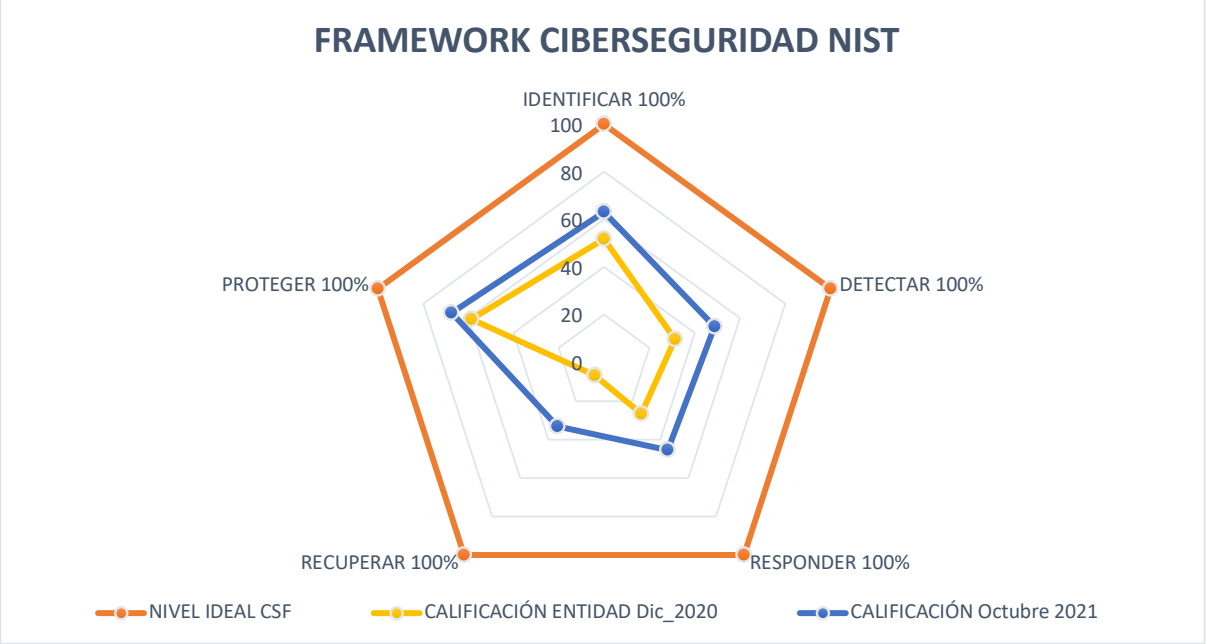
5.2. **AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA).** La correcta implementación del modelo establece la articulación del ciclo de Planear, Hacer (implementar), Verificar (evaluar) y Actuar (mejorar) – PHVA, como la estrategia para la construcción y mantenimiento del MSPI. Es así como,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

5.2.1. Se determina avance de 51% a 67% 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.

5.2.2. 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.

5.2.3. Se han estructurado, los documentos de Política General de Seguridad y Privacidad de la Información, Plan de Privacidad y Seguridad de la información.

5.3. **EVALUACION MEJORES PRACTICAS DE CIBERSEGURIDAD NIST**



5.3.1. La evaluación de la perspectiva de ciberseguridad permitió concluir que la UAESP avanzó de un 35% a un 52% con las mejores prácticas en ciberseguridad definidas por el NIST. Sobresale

5. CONCLUSIONES

la puntuación obtenida en las funciones PROTEGER e INDENTIFICAR cuyos porcentajes fueron 67% y 63% respectivamente.

5.3.2. Sin embargo, para las funciones DETECTAR, RESPONDER y RECUPERAR la puntuación obtenida en promedio fue de 42,5%, lo cual se ve reflejado en los Dominios A.10, A14, A16, A17, de los cuales se identificaron las observaciones respectivas.

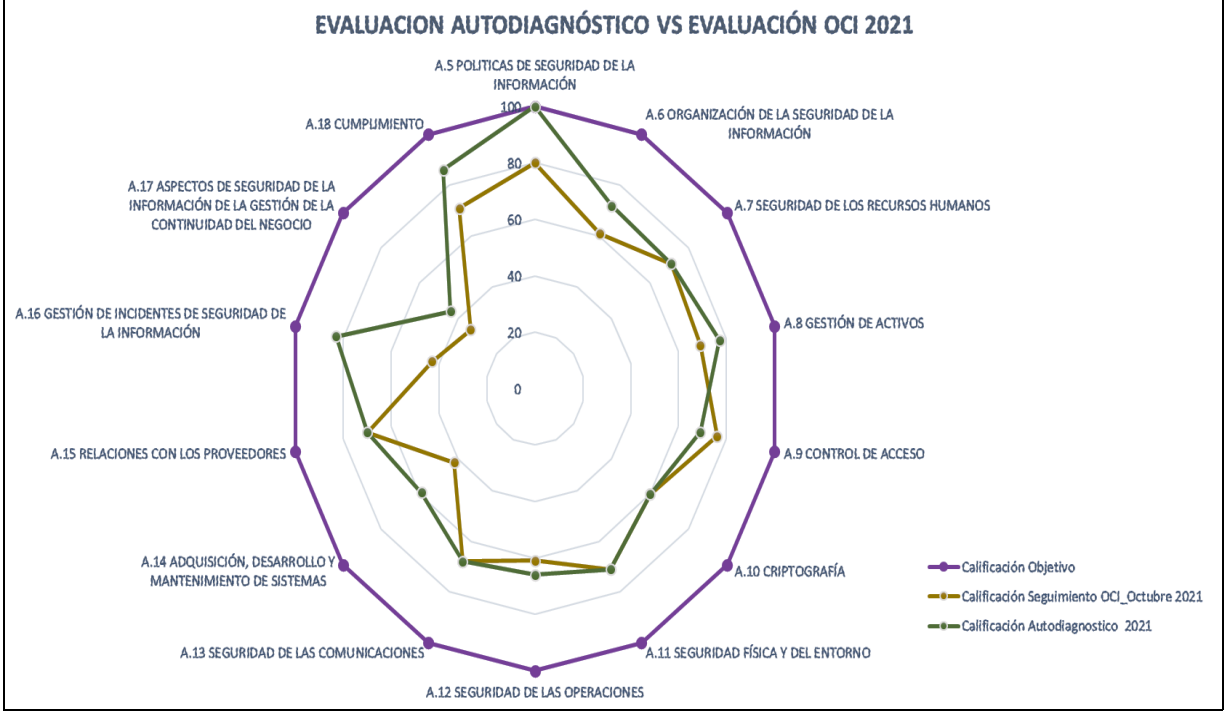
5.3.3. Dadas las condiciones de trabajo por la emergencia sanitaria COVID- 19 se hace urgente emprender las acciones que permitan avanzar con los Dominios anteriormente señalados. De esta manera se presenta la necesidad de avanzar en la formalización y aplicación del plan de continuidad de servicios tecnológicos el cual permita identificar con claridad los protocolos y actividades que se activarían en la eventual materialización de riesgos de seguridad de la información.

5.4. BRECHAS DE AUTODIAGNOSTICO 2021 vs. EVALUACIÓN 2021

5.4.1. La OCI hizo análisis detallado del autodiagnóstico ejecutado por la OTIC. La siguiente gráfica permite visualizar los Dominios en los cuales se identificaron diferencias significativas entre el autodiagnóstico y la evaluación realizadas este año respectivamente.

5.4.2. A pesar de que las calificaciones en los 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.

5. CONCLUSIONES



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 A.5 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

6.1.1. Formalizar mediante acto administrativo la Política General de Seguridad y Privacidad de la Información.
6.1.2. Dar prioridad al desarrollo total del Manual de Seguridad Digital para que se adopten todas las políticas de seguridad digital.

6.2. Dominio A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

6.2.1. Integrar SI Capital igualmente con LDAP, y contar con una herramienta que pueda validar amenazas de seguridad.
6.2.2. Contar con la matriz de Roles y Perfiles para asignación de usuarios a las aplicaciones de acuerdo

6. RECOMENDACIONES

con el manual de funciones institucional.

6.2.3. Que se cuente con los controles necesarios para evitar y minimizar riesgos de seguridad de información para teletrabajo o modalidad BYOD, máxime cuando la mayoría de los dispositivos utilizados actualmente son de uso personal y se pueden compartir con otros usuarios colocando en riesgo el acceso no autorizado a información sensible de la Entidad.

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

6.2.5. 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 A.7 SEGURIDAD DE LOS RECURSOS HUMANOS

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

6.3.2. 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.

6.4. Dominio A.8 GESTIÓN DE ACTIVOS

6.4.1. Adelantar el “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, (ej. equipos que se reasignan).

6.4.2. 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.

6.4.3. Contar con una “herramienta o solución” para la gestión de medios removibles o solución para minimizar riesgos de fugas de información por estos medios.

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

6.5. Dominio A.9 CONTROL DE ACCESO

6.5.1. Implementar un repositorio para versionamiento de código fuente, así mitigar el riesgo de perder la trazabilidad de desarrollos y el Know How de mejoras y desarrollos in house; igualmente para realizar un rollback cuando sea necesario.

6.5.2. 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

6. RECOMENDACIONES

se defina responsabilidad, periodicidad y custodia.

6.5.3. Una vez se tenga el manual de SI, aprobado se puede contemplar desarrollar instrumentos donde se pueda llevar trazabilidades como; solicitud y respuestas a usuarios en cuanto a accesos.

6.6. Dominio A.10 CRIPTOGRAFÍA

6.6.1. 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.

6.6.2. 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 en la realización de firmas escaneadas o digitalizadas que actualmente se está utilizando.

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

6.7. Dominio A.11 SEGURIDAD FÍSICA Y DEL ENTORNO

6.7.1. Validar en conjunto con la SAF, un análisis de identificación de riesgos ambientales para establecer los mecanismos para su mitigación.

6.7.2. Se recomienda la reorganización del cableado estructurado de acuerdo con los requisitos de ICONTEC

6.7.3. Llevar una bitácora de ingresos al centro de datos *(DC Data Center)* de personas externas, (ejemplo, personas de mantenimiento) por visitas esporádicas y/o empresas de mantenimientos.

6.7.4. Una vez aprobado el Manual de Seguridad de la Información, se implemente lo que hace falta en referencia al Capítulo 9.4 sobre Seguridad física y ambiental.

6.8. Dominio A.12 SEGURIDAD DE LAS OPERACIONES

6.8.1. Contar con un instrumento 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.

6.8.2. 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.

6.8.3. Es importante contar con un plan de gestión de backups donde se contemple pruebas de restauraciones que actualmente no se realizan. Es decir, en la política, procedimiento o lineamientos de BackUps documentar el plan y programación de copias de seguridad de la entidad en formato único que permita identificar tiempos, ubicaciones, responsables y medios de todos los respaldos y procedimientos del proceso. Se debería complementar con un formato que

6. RECOMENDACIONES

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.

6.8.4. Realizar gestión de auditorías preventivas a los sistemas de información; es decir, contemplar un plan de realización de auditorías para que no se realicen únicamente cuando se materializa el evento.

6.9. Dominio A.13 SEGURIDAD DE LAS COMUNICACIONES

6.9.1. 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.

6.9.2. Tener formatos, plantillas o instrumentos para solicitar y configurar los servicios de red que evidencien el cumplimiento de la política y procedimientos. Igualmente, la definición de responsabilidad en seguridad de los proveedores de red y no solo los ANS.

6.9.3. Es importante apoyar la aplicación de la política de acceso a la red con instrumentos, plantillas y formatos para evidenciar su cumplimiento.

6.9.4. Es recomendable que dentro del proceso de OTIC se cuente con profesionales certificados en X-ROAD para el manejo de interoperabilidad que requieran utilizar este recurso del Estado.

6.9.5. Tener evidencias sobre aplicación de la política, los procesos y los procedimientos para uso de los servicios de red.

6.10. Dominio A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

6.10.1. Adelantar con la definición de lineamientos como complemento a la minuta de contrato de SECOP II, con sanciones, o a los funcionarios con acciones disciplinarias, que viole la seguridad de la información definida en la política y se complemente con los temas de propiedad intelectual y derechos de autor.

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

6.10.3. Contar con los tres ambientes independientes para el proceso de mejoras, ajustes, adaptaciones y demás desarrollos como son: desarrollo, pruebas y producción como se establece en el control.

6.10.4. Una vez aprobado el manual de Política de SI, establecer lineamientos para la realización de pruebas de seguridad controladas.

6.10.5. 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.

6.10.6. Contar con una herramienta para el control de la metodología de desarrollo, así como gestionar requerimientos, planeación, tiempos de desarrollo, historia de usuarios, entre otros.

6.10.7. Complementar el procedimiento en desarrollo con algunos formatos o instrumentos para diferenciar desarrollo en tres escenarios: Adquirir software comercial, desarrollo de software de terceros, desarrollo software interno.

6. RECOMENDACIONES

6.11. Dominio A.15 RELACIONES CON LOS PROVEEDORES

6.11.1. Contar con una matriz de Acuerdos de Nivel de Servicio - ANS por terceros y políticas de ANS, para complementar el acuerdo de confidencialidad, en los contratos con terceros que indiquen criticidad de incidentes, tiempos de atención con base en la criticidad, protocolos de escalamiento y sanciones por incumplimiento de los ANS.

6.11.2. 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.

6.12. Dominio A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

6.12.1. Contar con un instrumento donde se registren y consoliden los diferentes incidentes de seguridad y su clasificación.

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

6.12.3. Documentar la gestión para poder consolidar y evidenciar los incidentes de seguridad que permitan establecer lecciones aprendidas para mitigar incidentes futuros.

6.12.4. Definir un indicador de incidentes de seguridad para medir el nivel de incidencias y la efectividad de las respuestas.

6.13. Dominio A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

6.13.1. 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/DR.

6.13.2. Es importante contar con 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.

6.14. Dominio A.18 CUMPLIMIENTO

6.14.1. Desarrollar de manera general la política de datos personales con lineamientos, alcance, finalidades, responsables y 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. Es decir, desarrollar el ciclo de vida para seguridad y PDP con base en la Ley 1581 de 2012.

6.14.2. Validar la observación de la auditoría anterior en cuanto a los protocolos para registro y actualización de Bases de datos con información personal y el cumplimiento de los tiempos y condiciones para actualización del registro ante la SIC.

6.14.3. Incorporar las directrices de la nueva guía de riesgos del DAFP. Esto por cuanto algunas evidencias presentadas son las mismas para más de un control lo que evidencia que el diseño de los controles mitigue riesgos diferentes.

6. RECOMENDACIONES

RECOMENDACIONES GENERALES DEL MSPI

i. En cuanto a los indicadores es recomendable realizar ajustes y contemplar adicionar algunos como: incidentes de seguridad, indicador a seguimiento de riesgos de TI, cobertura de sensibilización, y demás que se consideren pertinentes para la seguridad de la información, validar los contemplados en el Anexo 1. de la Resolución 500 del MinTIC.

ii. Es importante para la matriz de seguridad digital incorporar las directrices de la nueva guía de riesgos del DAFP, por cuanto se evidencia que aún no se ha tenido en cuenta. "*Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5, diciembre de 2020*", a su vez contemplar un documento con el Plan de Tratamiento de riesgos de seguridad de la Información.

iii. 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. De otra parte es recomendable actualizar la información a la SIC como se especifica en el Plan de Seguridad y Privacidad de la información publicado en la web, no se evidencia el cumplimiento de la actividad *"Registrar o actualizar las bases de datos en la plataforma de la SIC teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información*", para el 1 de agosto de los corrientes, evidenciando que la última actualización enviada a la SIC corresponde al año 2019, por lo cual puede generar un riesgo con la información no reportada en este período.

iv. Contemplar un apoyo con 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.

v. Definir periodicidad para la revisión y posibles actualizaciones de las políticas relacionadas con seguridad de la información e integrar en el documento un control de versionamiento que permita identificar los ajustes realizados al documento.

vi. Hacer énfasis en las responsabilidades de seguridad de la información - SI de los funcionarios y contratistas en los procesos de inducción y reinducción más aun teniendo en cuenta la emergencia sanitaria COVID-19.

vii. Conforme 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 de tal manera que por la ausencia de un miembro no se afecte la seguridad de la información y la infraestructura.

viii. Se recomienda actualizar el normograma para tener en cuenta lineamientos emitidos recientemente por el distrito en materia de datos abiertos de Bogotá además de modificaciones emitidas por MinTIC referentes a propiedad intelectual, seguridad digital, estándares de publicación y accesibilidad. Ej.: Resoluciones 1519, 2893 de 2020 y 0500 de 2021, Directiva Presidencial 03 de 2021.

ix. Actualizar el Plan de Seguridad y Privacidad de la Información teniendo la cuenta la Resolución 500 de MinTIC.

6. **RECOMENDACIONES**
x. 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 o 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.

APROBACIÓN:	
FIRMA **Jefe(a) de Oficina de Control Interno**	**Auditor(es) Interno(s)**
FECHA[4]: 10 – 11 – 2021	

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