MEMORANDO

Al contestar, por favor cite el radicado:
No.:**20211100000303**

Bogotá D.C., 08 de enero de 2021

PARA: **CÉSAR MAURICIO BELTRÁN LÓPEZ**
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 2020

Respetado Ingeniero Beltrán:

La Oficina de Control Interno dando cumplimiento al Plan Anual de Auditorías vigencia 2020, planificó el desarrollo de la auditoria con radicado 20201100057693 cuyo propósito consistió en realizar la evaluación del Sistema de Gestión de la Seguridad de la Información operante en la UAESP, conforme a lineamientos del Modelo de Seguridad y Privacidad de la información (MSPI) e ISO 27001:2013. Su ejecución comprendió el periodo a partir del 10 de diciembre de 2020 al 5 de enero de 2021 proceso que permitió concluir lo siguiente:

1. Resultado de la evaluación efectuada al Modelo de Seguridad y Privacidad de la Información se obtuvo una calificación cuantitativa promedio de 54% frente al 47% obtenido en la evaluación vigencia 2019.

   El avance de 7 puntos porcentuales es bajo frente a la calificación objetivo (100%), este avance es atribuible en gran parte a que el 29% de los Dominios que componen el sistema se encuentran en etapas muy tempranas de su desarrollo que incluyen la construcción y/o planificación de productos y lineamientos que en este punto ya deberían estar en evaluación de su desempeño y mejora.

2. Según la escala de valoración de efectividad de controles SI diseñada por el MINTIC se puede concluir que el sistema implementado se clasifica como EFECTIVO, lo cual significa que buena parte de los procesos y controles se documentan y se comunican. Sin embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.

3. La evaluación de la perspectiva de ciberseguridad permitió concluir que la UAESP cumple en un 35% con las mejores prácticas en ciberseguridad definidas por el NIST. Sobresale la puntuación obtenida en las funciones PROTEGER e INDENTIFICAR cuyos porcentajes respectivamente fueron 59% y 52%. Sin embargo, para las funciones DETECTAR, RESPONDER y RECUPERAR, la puntuación obtenida en promedio es del 22%. Esta valoración se puede explicar por el bajo desempeño identificado en los Dominios del sistema A.10, A.14, A.16 y A.17 (referenciados en la Observación 3.1 del presente informe) ya que son una base importante en la gestión de TI planteada por la entidad para el trabajo remoto / semipresencial.

Bogotá D.C., 08 de enero de 2021

Dadas las condiciones y dinámicas de trabajo modificadas por la emergencia sanitaria COVID-19 se hace urgente emprender las acciones que permitan avanzar rápida y consistentemente con los Dominios anteriormente señalados. Se insiste en la necesidad de construir y poner en marcha el plan de continuidad de servicios de TI el cual permita identificar con claridad los conductos y actividades que se activarán para atenuar la eventual materialización de riesgos de seguridad de la información.

4. La OCI hizo análisis detallado del autodiagnóstico ejecutado por la OTIC en junio de 2020. La siguiente gráfica permite visualizar los Dominios en los cuales se identificaron diferencias significativas entre el autodiagnóstico y la evaluación realizadas en junio y diciembre de 2020 respectivamente.

   A pesar de que las calificaciones en varios de los Dominios fueron distintas, se evidencia una tendencia similar para la evaluación y el autodiagnóstico, lo cual permite concluir que la OTIC conoce con anterioridad aquellos aspectos en los que el sistema presenta debilidades y ha trabajado en varios de los controles rezagados.

En el informe anexo (virtual) podrán detallar y analizar junto con su equipo de trabajo la No Conformidad que requiere tratamiento según los procedimientos vigentes en el SIG. Así mismo, podrán pormenorizar sobre las dos (2) fortalezas, una (1) conformidad, las once (11) observaciones agregadas y nueve (9) recomendaciones de auditoría interna.

Finalmente, estamos atentos para concertar una reunión virtual de socialización de los resultados y detalles del proceso de auditoria llevado a cabo.

Cordialmente,

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

Elaboró: Javier Alfonso Sarmiento Piñeros, Profesional Contratista Oficina de Control Interno.
Anexo: 3 archivos virtuales (Informe y anexos)

Informado: Dra. Luz Amanda Camacho Sánchez, Directora General.

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 2020 - UAESP**			
PROCESO, PROCEDIMIENTO, Y/O DEPENDENCIA	OFICINA DE TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES			
RESPONSABLE Y/O AUDITADOS	Ing. Cesar Beltrán, Rubén Buitrago y equipo de trabajo de la OTIC			
OBJETIVO	**Evaluar el Sistema de Gestión de la Seguridad de la Información operante en la UAESP, conforme a 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 diciembre de 2020.			
PERIODO DE EJECUCIÓN	Del 10/12/2020 al 05/01/2021			
EQUIPO AUDITOR	Andrés Pabón Salamanca – APS, Javier Alfonso Sarmiento Piñeros – JASP			
DOCUMENTACIÓN ANALIZADA (4)	- **LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD** - **PROCEDIMIENTOS OTIC** - VIGENTES - **DOCUMENTACIÓN MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN** – MSPI VIGENTE EN LA UAESP. - **DOCUMENTACIÓN MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN** – MSPI EN CONSTRUCCIÓN. - **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 - **CUESTIONARIO AUDITORIA DE APLICACIONES –** ORFEO – SI CAPITAL - **MATRIZ PAI –** VIGENTE			

(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

La Oficina de Control Interno dando cumplimiento al Plan Anual de Auditorías vigencia 2020, planificó el desarrollo de la auditoria con radicado 20201100057693 cuyo propósito consistió en realizar la evaluación del Sistema de Gestión de la Seguridad de la Información operante en la UAESP, conforme a lineamientos del Modelo de Seguridad y Privacidad de la información (MSPI) e ISO 27001:2013. Su ejecución comprendió el periodo a partir del 10 de diciembre de 2020 al 5 de enero de 2021.

Para realizar la evaluación fueron contempladas dos (2) perspectivas principales:

La primera correspondió a la evaluación de la efectividad de 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.

La segunda perspectiva, tuvo como objetivo determinar el estado de la UAESP frente a las mejores prácticas en ciberseguridad definidas por el NIST[1], 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 aplicados a una muestra de dos (2) aplicativos actualmente en operación en la UAESP.

Finalmente, la evaluación producto de esta auditoria fue contrastada respecto a la evaluación realizada en la vigencia 2019 con el fin de determinar los criterios en los cuales se ha identificado avance y también aquellos que suponen emprender acciones de mejora.

1.1. LIMITACIONES DE AUDITORÍA: La auditoría bajo modalidad de trabajo en casa, que pudo haber limitado la perspectiva respecto a trabajos analíticos, sustantivos y de cumplimiento en visita en sitio. No obstante, se programaron reuniones en plataformas tecnológicas para hacer entrevistas. Así mismo, el manejo de tiempo dado el contexto de trabajo en casa y las dinámicas que implicaron laboralmente la emergencia ambiental y sanitaria por el Covid-19.

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 cinco (5) Dominios del sistema.

Cuatro (4) de ellos incrementaron su nivel, pasando de *Efectivo* a *Gestionado* lo cual significa que los controles se monitorean y además se mide el cumplimiento de los procedimientos permitiendo tomar acción donde los procesos no funcionan eficientemente.

[1] Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés, National Institute of Standards and Technology)

2. CONFORMIDADES Y FORTALEZAS

El Dominio *A.15 Relaciones con los proveedores* incrementó su nivel pasando de *Repetible* a *Efectivo*, lo cual significa que en este Dominio los procesos y los controles se documentan, se comunican y se aplican casi siempre.

La calificación y nivel actual resultado de la evaluación se detalla en la tabla a continuación:

DOMINIO	Calificación Seguimiento 2019	Calificación Seguimiento Actual 2020	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	60	**80**	100	**GESTIONADO**
A.8 GESTIÓN DE ACTIVOS	47	**62**	100	**GESTIONADO**
A.13 SEGURIDAD DE LAS COMUNICACIONES	56	**63**	100	**GESTIONADO**
A.15 RELACIONES CON LOS PROVEEDORES	40	**60**	100	**EFECTIVO**
A.18 CUMPLIMIENTO	54	**61**	100	**GESTIONADO**

2.2. Fortaleza: Dominios con avance significativo. La siguiente tabla detalla los Dominios en los cuales se observó que, aunque mantienen el nivel de efectividad respecto a la evaluación 2019, reflejan aumento porcentual significativo en la evaluación 2020.

DOMINIO	Calificación Seguimiento 2019	Calificación Seguimiento Actual 2020	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS	64	**71**	100	**GESTIONADO**
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	24	**40**	100	**REPETIBLE**

2.3. Fortaleza: Política Seguridad de los Información y seguridad de los Recursos Humanos. Se evidencian esfuerzos importantes con la implementación de nuevos controles en los últimos 6 meses que permitieron obtener una calificación superior en la evaluación realizada a los Dominios señalados frente al autodiagnóstico realizado por la OTIC en junio de 2020.

3. OBSERVACIONES

3.1. Observación: Dominios con bajos niveles de efectividad en los controles. La siguiente tabla muestra los Dominios del sistema que se mantienen en niveles tempranos (inicial y repetible) de la implementación del MSPI.

DOMINIO	Calificación Seguimiento 2019	Calificación Seguimiento Actual 2020	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.10 CRIPTOGRAFÍA	30	**30**	100	**REPETIBLE**
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	24	**40**	100	**REPETIBLE**
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	20	**17**	100	**INICIAL**
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	23,5	**27**	100	**REPETIBLE**

Tres (3) de los Dominios identificados se encuentran en el nivel *Repetible*, que implica la no formación ni comunicación formal sobre los procedimientos y estándares, caracterizado por un alto grado de confianza en los conocimientos de cada persona, aumentando la probabilidad de errores.

El Dominio *A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO* se encuentra en nivel ***Inicial*** se caracteriza, porque la implementación de controles depende de cada individuo y es principalmente reactiva en algunos casos se cuenta con procedimientos documentados, pero no son conocidos y/o no se aplican.

3.2. Observación. Actualización de normatividad y referentes en la Política de SI. El documento es susceptible de actualización para tener en cuenta normatividad vigente Ej.: Ley 1915 de 2018 disposiciones en materia de derechos de autor, Resolución N° 001519 de 24 de 2020.

3.3. Observación. Responsabilidades y Organización de la Seguridad de la Información. En revisión de documento Manual de políticas de seguridad de la información actualizado versión 2 - marzo de 2020 se observa que el documento publicado no está firmado**.**

3.3.1. Se evidencia uso indistinto de los conceptos seguridad informática y seguridad de la información lo cual puede dar lugar a interpretaciones erróneas del alcance o de la función (roles).

3.3.2. No se cuenta un procedimiento establecido para el contacto y reporte de incidentes de Seguridad de la Información que especifiquen cuándo y a través de que aprobaciones se debería contactar a las autoridades competentes.

3. OBSERVACIONES

3.4. Observación. Gestión de Activos. El documento PC-13 Cifrado de información V1 no especifica dentro de sus actividades la identificación del formato, medio y gestión de backup de la información.

3.4.1. Existen controles de TI asociados a la devolución de activos asignados. Se evidencia el funcionamiento de un flujo de procesos mediante la herramienta Runmyprocess para la generación de Paz y salvos. Sin embargo, en entrevista con el administrador del sistema ORFEO se evidencian debilidades en los controles asociados a la gestión de aplicativos al finalizar la vinculación de funcionarios y contratistas (usuarios persistentes).

3.4.2. No se evidencia un lineamiento o protocolo que permita determinar la aplicabilidad o no de medidas de protección de medios que contienen información.

3.5. Observación. Control de Acceso. Se evidencian debilidades en el método para asignación de contraseñas. Actualmente no asegura la confidencialidad de accesos mediante usuario y contraseña, al compartirse con personas que, aunque pertenecen a la misma oficina o dependencia no deberían tener acceso.

3.5.1. Se evidencia que el aplicativo ORFEO muestra en pantalla luego del logueo la información de usuario y contraseña en texto, aumentando significativamente la probabilidad de acceso no autorizado a otros sistemas sobre los cuales el usuario tenga privilegios a través de LDAP.

3.5.2. No existe un procedimiento para la gestion de códigos fuente, Sin embargo, se evidenció que el sistema ORFEO aplica algunas buenas prácticas mediante la implementación de un repositorio para la gestión del código fuente lo cual permite tener trazabilidad y versionamiento así como realizar rollback en caso de ser necesario.

3.6. Observación. Criptografía. No hay evidencia que permita establecer que se han definido lineamientos para la aplicación de controles criptográficos en la UAESP.

3.6.1. No se evidencia un procedimiento para la gestion de llaves y sistemas criptográficos.

3.7. Observación. Seguridad de las Operaciones. Se evidencia procedimiento de gestion de cambios aun en borrador. Actualmente no se realiza un seguimiento formal de los cambios a los sistemas de información o aplicativos gestionados por la UAESP.

3.7.1. Se evidencia la ejecución de la herramienta para generación de copias de seguridad. Sin embargo, en entrevista se evidencian fallas en los sistemas de respaldo y generación de copias de seguridad de sistemas y ubicaciones de red.

3.7.2. En entrevista se afirma que existen backups en la nube sin embargo no se ven reflejado en los procedimientos.

3. OBSERVACIONES

3.7.3. No se evidencia ejecución regular y sistemática de pruebas de restauración de backups.

3.7.4. En revisión, no se evidencian lineamientos que permitan documentar en detalle la separación de ambientes para el desarrollo de sistemas.

3.8. Observación. Adquisición, Desarrollo Y Mantenimiento De Sistemas. La política de desarrollo seguro se enmarca dentro de la política de requerimiento de seguridad de los sistemas. Sin embargo, no cuenta con los elementos mínimos para garantizar que se implementan sistemas y aplicaciones en el marco de un desarrollo seguro.

3.8.1. Se evidencia que los sistemas objeto de revisión (ORFEO y SI CAPITAL) no cuentan con documentación estructurada en el marco del desarrollo seguro.

3.8.2. No se evidencia consistencia en los procesos de conocimiento de deberes y responsabilidades con la seguridad de la información por parte de los responsables de sistemas y/o aplicativos de la UAESP.

3.8.3. No se evidencia la definición de riesgos relacionados con cambios en el software.

3.8.4. Para los aplicativos objeto de revisión en entrevista se afirma que no se ejecutan pruebas de seguridad.

3.9. Observación. Gestión de Incidentes de Seguridad de la Información. No se cuenta con un procedimiento para la gestion de incidentes de seguridad. Sin embargo, en el plan operativo MSPI se observa reporte de avance del 50% en la construcción del documento. En el seguimiento de 2019 se contaba con un borrador de este documento con elementos ya construidos, se sugiere revisar el documento actual frente al construido en 2019.

3.9.1. No se evidencia clasificación de los incidentes de SI reportados y tampoco un plan de respuesta frente a dichos incidentes.

3.9.2. Se observa que los reportes de incidentes de SI no son significativos en términos de cantidad. Sin embargo, no es posible afirmar que los pocos reportes se deban a que no se presentan incidentes de seguridad.

3.9.3. No se evidencia una recopilación de evidencias soporte de incidentes de SI que permita concluir que se adquiere conocimiento para reducir el impacto futuro.

3.10. Observación. Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio. No se evidencia el establecimiento de plan de contingencia SGSI.

3.10.1. Se evidencia ocurrencia de situaciones de emergencia para las cuales no se ha definido un conducto o manejo contingente (copias de seguridad, ambientales) por ende no se han

3. OBSERVACIONES

realizado pruebas de la funcionalidad de los procedimientos y controles de continuidad de la seguridad de la información.

3.10.2. Se evidencia que la Entidad cuenta servicios redundantes. Sin embargo, actualmente no se encuentra dispuestos, organizados o documentados de forma tal que pueda considerarse como parte de una arquitectura. se evidencian fallos con la gestion de copias de seguridad y respaldo en la ubicación designada en los equipos de cómputo “Mis documentos”.

3.10.3. Se evidencian fallos en la gestión de backup de aplicativos como ORFEO y nuevas implementaciones como el sistema de gestion de planes de mejoramiento de la UAESP.

3.11. Observación. Cumplimiento. No se evidencia la ejecución estructurada de un plan de pruebas de seguridad manuales o automatizadas para los servicios, sistemas y/o aplicaciones de la UAESP.

4. SOLICITUD DE CORRECCIÓN Y ACCIONES CORRECTIVAS

No.	DESCRIPCIÓN DE LA NO CONFORMIDAD	REQUISITO QUE INCUMPLE
1.1.	En la evaluación realizada al Modelo de Seguridad y Privacidad de la Información operante en la UAESP se evidencia que el avance verificado a la fecha (54%) es bajo respecto a la calificación objetivo (100%) definida por el MINTIC e insuficiente respecto a los plazos fijados normativamente para la implementación del sistema (para entidades del orden territorial a partir del 2018 el sistema se debe mantener según el ciclo PHVA en Mejora continua).	Decreto 1078 de 2015, en el Titulo 9, Capitulo 1, Sección 3. (Política de Seguridad Digital, MIPG)

5. CONCLUSIONES

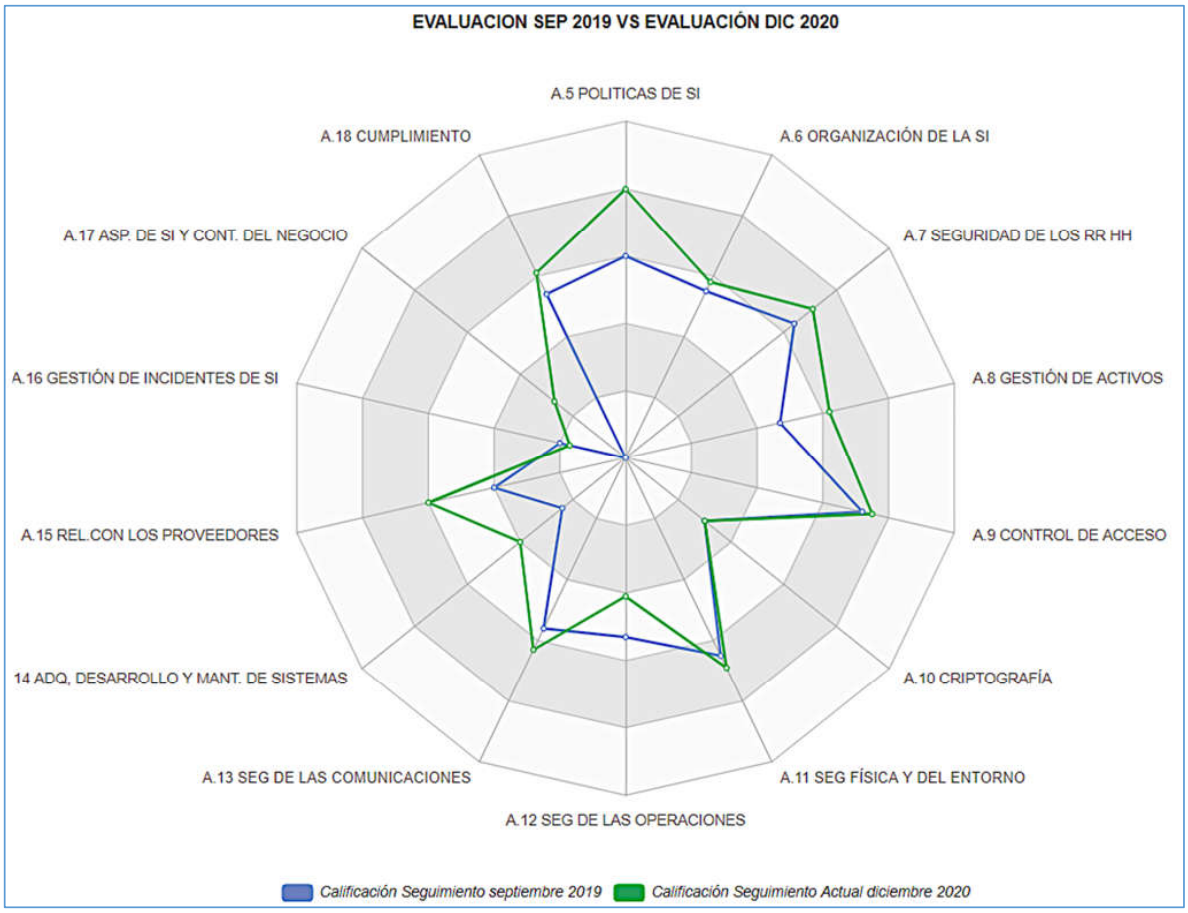
EVALUACIÓN DE EFECTIVIDAD DE CONTROLES MSPI 2020

5.1. Resultado de la evaluación efectuada al Modelo de Seguridad y Privacidad de la Información se obtuvo una calificación cuantitativa promedio de **54%** frente al 47% obtenido en la evaluación vigencia 2019.

El avance de 7 puntos porcentuales es bajo frente a la calificación objetivo (100%), este avance es atribuible en gran parte a que el 29% de los Dominios que componen el sistema se

5. CONCLUSIONES

encuentran en etapas muy tempranas de su desarrollo que incluyen la construcción y/o planificación de productos y lineamientos que en este punto ya deberían estar en evaluación de su desempeño y mejora.



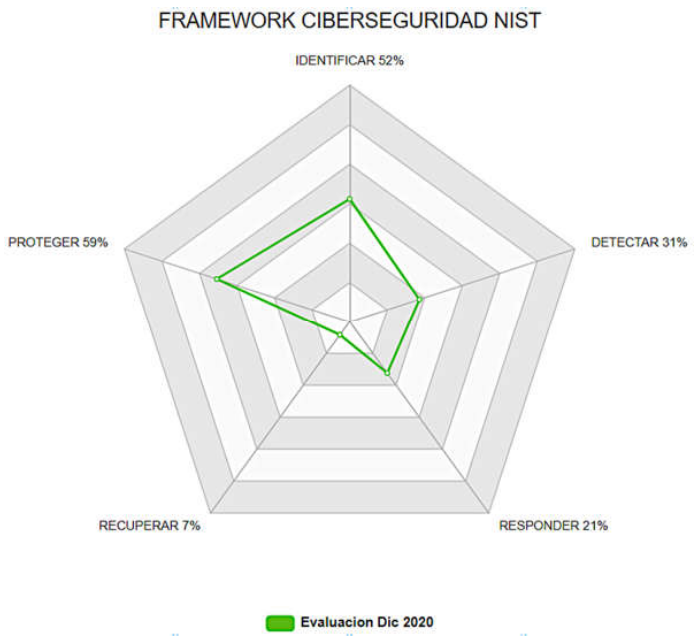
5.2. Según la escala de valoración de efectividad de controles SI diseñada por el MINTIC se puede concluir que el sistema implementado se clasifica como ***EFECTIVO,*** lo cual significa que buena parte de los procesos y controles se documentan y se comunican. Sin embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.

5. CONCLUSIONES

EVALUACION MEJORES PRACTICAS DE CIBERSEGURIDAD NIST

5.3. La evaluación de la perspectiva de ciberseguridad permitió concluir que la UAESP cumple en un **35%** con las mejores prácticas en ciberseguridad definidas por el NIST. Sobresale la puntuación obtenida en las funciones **PROTEGER** e **INDENTIFICAR** cuyos porcentajes respectivamente fueron 59% y 52%. Sin embargo, para las funciones **DETECTAR, RESPONDER** y **RECUPERAR,** la puntuación obtenida en promedio es del **22%**. Esta valoración se puede explicar por el bajo desempeño identificado en los Dominios del sistema A.10, A.14, A.16 y A.17 (referenciados en la Observación 3.1 del presente informe) ya que son una base importante en la gestión de TI planteada por la entidad para el trabajo remoto / semipresencial.

Dadas las condiciones y dinámicas de trabajo modificadas por la emergencia sanitaria COVID-19 se hace urgente emprender las acciones que permitan avanzar rápida y consistentemente con los Dominios anteriormente señalados. Se insiste en la necesidad de construir y poner en marcha el plan de continuidad de servicios de TI el cual permita identificar con claridad los conductos y actividades que se activarán para atenuar la eventual materialización de riesgos de seguridad de la información.

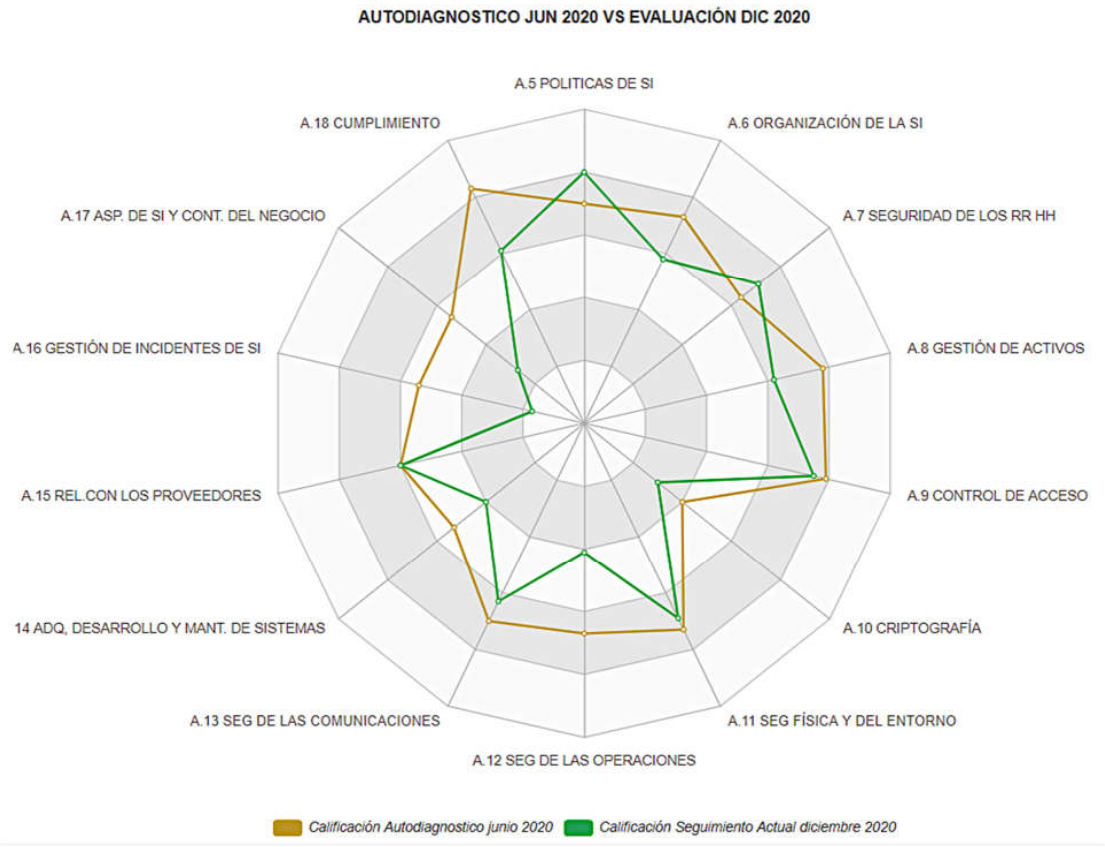


5. CONCLUSIONES

BRECHAS AUTODIAGNOSTICO 2020 VS EVALUACIÓN 2020

5.4. La OCI hizo análisis detallado del autodiagnóstico ejecutado por la OTIC en junio de 2020. La siguiente gráfica permite visualizar los Dominios en los cuales se identificaron diferencias significativas entre el autodiagnóstico y la evaluación realizadas en junio y diciembre de 2020 respectivamente.

A pesar de que las calificaciones en varios de los Dominios fueron distintas, se evidencia una tendencia similar para la evaluación y el autodiagnóstico, lo cual permite concluir que la OTIC conoce con anterioridad aquellos aspectos en los que el sistema presenta debilidades y ha trabajado en varios de los controles rezagados.



6. RECOMENDACIONES

6.1. Recomendación. Política De Seguridad De La Información. Se sugiere definir una 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.

6.2. Recomendación. Responsabilidades Y Organización Seguridad Información. Se recomienda actualizar documento "*Manual de políticas de seguridad de la información*" para que guarde coherencia con el apartado Matriz de Roles y responsabilidades del documento *"Política de seguridad de la información*".

6.2.1. Se sugiere consolidar el documento "Documento Roles y responsabilidades Seguridad de la Información" dado que dentro del manual de políticas de seguridad de la información hay un apartado que trata la misma temática.

6.2.2. Dada la emergencia sanitaria COVID-19, las tareas y actividades que desarrollan funcionarios y contratistas se ejecutan mediante trabajo en casa en su mayoría haciendo uso de sus dispositivos propios, se recomienda incluir este tipo de escenarios de contingencia en la construcción del plan de continuidad de negocio.

6.2.3. Se recomienda relacionar el procedimiento de cifrado de información con la clasificación de los activos de información para facilitar la identificación de aquella información susceptible a este tipo de control.

6.2.4. Se recomienda retomar construcciones de documentos BIA y BCP que se encontraban en un avance significativo para 2019.

6.3. Recomendación. Seguridad De Los Recursos Humanos. Emprender las acciones pertinentes para solicitar aprobación y publicación del documento "Acuerdo de confidencialidad".

6.3.1. Se recomienda hacer énfasis en las responsabilidades de SI de los funcionarios y Contratistas en los procesos de inducción y reinducción más aun teniendo en cuenta la emergencia sanitaria COVID-19.

6.4. Recomendación. Control de Acceso. Se recomienda habilitar los mecanismos necesarios para la gestión autónoma de contraseñas, y así reducir el riesgo de pérdida de confidencialidad por acceso a información de asignación de usuarios y contraseñas por parte de personal ajeno al autorizado.

6.5. Recomendación. Criptografía. Se sugiere que LA OTIC haga revisión y propuesta de la implementación de controles criptográficos como la firma digital y/o electrónica para manejo de funcionarios y contratistas de forma tal que permita reducir los tramites manuales que se ejecutan en varios procesos.

6. RECOMENDACIONES

6.6. Recomendación. Gestión de Incidentes de Seguridad de la Información. En el seguimiento de 2019 se contaba con un borrador de este documento con elementos ya construidos, se sugiere revisar el documento actual frente al construido en la vigencia anterior.

6.7. Recomendación. Cumplimiento. 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.: Resolución 1519 de 2020.

6.8. Recomendación. Sistemas Y Aplicativos. Para el desarrollo de esta evaluación la OCI parametrizó una prueba automatizada para la identificar vulnerabilidades WEB del aplicativo ORFEO. Se recomienda hacer revisión del Anexo 2 del presente informe.

6.8.1. Se recomienda revisar por parte de los administradores de los sistemas/aplicaciones y de infraestructura tecnológica la viabilidad y aplicación de controles criptográficos que permitan dotar a los sistemas de información de irrenunciabilidad o no repudio mediante la implementación de servicios de seguridad que prueben la participación de las partes en una comunicación de forma tal que se reduzca el trámite y gestion de soportes en sistemas como ORFEO.

6.9. Recomendación. General MSPI Nueva Versión. Se sugiere tener en cuenta el documento Maestro de lineamientos MSPI Versión 4 de septiembre de 2020. A pesar de que es un documento borrador en los próximos meses se prevé entre en vigencia mediante resolución del MINTIC este documento tiene en cuenta normatividad Decreto 2106 de 2019 (interoperabilidad y servicios digitales) así como también establece elementos para la identificación y protección de infraestructura critica al interior de las entidades.

APROBACIÓN:

FIRMA **Jefe(a) de Oficina de Control Interno**	Firmado digitalmente por Javier Alfonso Sarmiento Piñeros DN: C=CO, CN=Javier Alfonso Sarmiento Piñeros, E=jasarmiento101a@gmail.com Razón: Doy fe de la exactitud e integridad de este documento Ubicación: Bogotá, Colombia **Auditor(es) Interno(s)**

FECHA[4]:

08 - 01 – 2021

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