ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HÁBITAT
Unidad Administrativa Especial de Servicios Públicos

MEMORANDO

Al contestar, por favor cite el radicado:
No. **20191100062033**

Bogotá D.C., 09 de octubre de 2019

PARA: **MARTHA CECILIA MURCIA CHAVARRO**
Jefe Oficina Asesora de Planeación

ANGIE ALEXANDRA HERNÁNDEZ CASTAÑO
Subdirectora de Servicios Funerarios y Alumbrado Público

MARTHA PATRICIA PINZON DURAN
Subdirectora de Aprovechamiento

DIEGO IVÁN PALACIOS DONCEL
Subdirector de Asuntos Legales

MARTHA JANETH CARREÑO LIZARAZO
Subdirectora Administrativa y Financiera

GUSTAVO ADOLFO PALACIOS ROJAS
Jefe Oficina de Tecnologías de la Información y las Comunicaciones

CAROLINA ALEJANDRA MARÍN MARTÍNEZ
Jefe Oficina Asesora de Comunicaciones.

DE: Oficina de Control Interno

ASUNTO: Resultados Auditoria al Sistema Integrado de Gestión en la UAESP - 2019

Respetados(as) doctores(as):

De conformidad con el Plan de Auditoria Interna que desarrolló el equipo de trabajo de la Oficina de Control Interno, el cual tiene como objetivo verificar la eficacia del Sistema Integrado de Gestión en la UAESP, de forma integral en concordancia con las Normas NTC ISO 9001:2015 y NTC ISO 14001:2015, envío informe final de auditoria con los

ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HÁBITAT
Unidad Administrativa Especial de Servicios Públicos

MEMORANDO

Al contestar, por favor cite el radicado:
No.:**20191100062033**

Bogotá D.C., 09 de octubre de 2019

resultados obtenidos presentados y validados por el equipo auditor, así:

- Identificación de 24 conformidades
- Presentación para análisis de 24 observaciones
- Formulación de 3 No Conformidades

Conforme con lo anterior y producto del análisis por parte de los gestores y líderes de proceso, y con especial atención en las No Conformidades, se solicita el envío correcciones y acciones correctivas dentro de los diez (10) días siguientes a la radicación de la presente.

Así mismo, remitimos informe de forma virtual con el fin de facilitar la consulta, junto con anexos.

Cordialmente,

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

Anexos: Informe de auditoría y Seis anexos al informe (22 folios)

Elaboró: Edgar Andrés Ortiz Vivas, Profesional OCI

Con copia a Dirección

ENFOQUE DE LA AUDITORIA INTERNA	**GESTIÓN Y RESULTADOS** (1)	**ANÁLISIS FINANCIERO Y CONTABLE** (1)	**LEGAL** (1)	**SISTEMA DE GESTIÓN** (2)
			Resolución No. 312 de 2019 - Mintrabajo	MIPG y MECI NTC ISO 9001:2015; NTC ISO 14001:2015
INFORME (3)	Resultados Auditoría al Sistema Integrado de Gestión en la UAESP			
PROCESO, PROCEDIMIENTO, Y/O DEPENDENCIA	TODOS LOS PROCESOS			
RESPONSABLE Y/O AUDITADOS	Líderes de Proceso y/o Equipos de trabajo designados			
OBJETIVO	Verificar la eficacia del Sistema Integrado de Gestión en la UAESP, de forma integral en concordancia con las Normas NTC ISO 9001:2015 y NTC ISO 14001:2015**.**			
ALCANCE	Todos los procesos de la Unidad, Sede Administrativa y Sede gestión documental, y de las actividades desarrolladas con corte agosto 31 de 2019.			
PERIODO DE EJECUCIÓN	16 de septiembre al 15 de octubre de 2019			
EQUIPO AUDITOR	Andrés Ortiz – AO, José Pinzón – JP Javier Sarmiento – JS, Iván Sierra -IS, Daniela Gordillo – DG (observadora), Harold Puentes - HMP, Martha Olaya – MO.			
DOCUMENTACIÓN ANALIZADA (4)	Manual Operativo SIG, Listado Maestro de documentos, matriz caracterización grupos de interés, matriz mapa de Riesgos, Portafolio de Servicios, Plan Institucional de Gestión Ambiental (PIGA), Plan de Seguridad y salud en el Trabajo (PSST), Acuerdo de Gestión (según muestra); Plan Institucional de Capacitación; Modelo de Seguridad y Privacidad de la Información; Normograma de procesos según Listas de Verificación; registros de PQRSD; y otros documentos presentados durante las visitas en sitio y referenciados en listas de verificación.			

(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

1.1. Descripción Metodológica

De conformidad con el Plan Anual de Auditorías PAA 2019 se planificó verificar el estado y avance del Sistema de Control Interno conforme con el MECI y el MIPG, la cual fue modificada para el segundo ciclo según solicitud de la Oficina Asesora de Planeación para el mes de octubre de 2019, la cual fue aprobada por el Comité Institucional de Coordinación de Control Interno de la UAESP. De acuerdo con lo anterior y considerando la iniciativa prevista por la Oficina de Control Interno según Plan de Acción Institucional (Auditorías Internas con enfoque integrado realizados en la Entidad), se preparó, planificó y ejecutó la presente auditoría con los presentes resultados, así:

- El líder de auditoría verifica competencia basado en educación, formación o experiencia laboral respecto del equipo de trabajo disponible, seleccionando equipo auditor y definiendo roles.

- Realización de jornadas de entrenamiento al equipo auditor referentes acciones para fortalecer la ejecución de auditoría, recordar de la información documentada del procedimiento, y requisitos relacionados con el MECI y MIPG versus NTC ISO 9001, 14001, 27001 y 45001, entre otros.

- Análisis del PAA 2019 la ejecución de las Auditorías de forma integrada (Auditoria combinada), considerando las siguientes:

    - Ciclo 2 de la auditoría número 3, con alcance a todos los procesos: verificar el estado y avance del Sistema de Control Interno conforme con al MECI y el MIPG.

    - Ciclo 2 de la auditoría número 6, con alcance a Procesos Gestión Tecnológica y de Información, Gestión de Apoyo Logístico, Gestión Financiera, y Gestión Documental: Gestión de elementos de hardware, software y derechos de Autor; y verificar cumplimiento de las directrices para prevenir conductas irregulares relacionadas con el incumplimiento de los manuales de funciones y de procedimientos y la pérdida de elementos y documentos públicos

    - Único ciclo de la auditoría número 9, con alcance al proceso Gestión Humana: Verificar el Sistema de información SIGEP (SIDEAP) y gestión de procedimientos 02, 03, 04, 07, 12 y 13.

    - Único ciclo de la auditoría número 10, con alcance a todos los Procesos: Auditoría de cumplimiento del sistema de gestión de la seguridad y salud en el trabajo. SG-SST

    - Único ciclo de la auditoría número 12, con alcance al proceso gestión tecnológica y de la información: verificar aspectos tecnológicos y de sistema de Información de la UAESP en concordancia con la política nacional y distrital de gobierno digital.

1. DESCRIPCIÓN GENERAL DEL DESARROLLO DE LA AUDITORIA

- Único ciclo de la auditoría número 13, cuyo alcance refiere a los procesos gestión de la innovación y gestión del conocimiento: verificar documentación y desempeño de los procesos.

- Único ciclo de la auditoría número 15, con alcance al Proceso de Gestión Ambiental: Evaluar el desempeño del PIGA y gestión ambiental de la UAESP.

- Preparación de los papeles de trabajo (listas de verificación) en virtud de objeto, alcance y criterios definidos para la presente auditoría, por proceso, precisando que las asociadas con 27001 y 45001 son marcos de referencia para la mejora del SIG. El líder de auditoría presenta papeles de trabajo por proceso para que el equipo auditor los analice y ajuste.

- Análisis de la documentación publicada en dirección virtual destinada para el SIG (Micrositio SIG), por parte del equipo auditor, con el objetivo de completar y complementar papeles de trabajo.

- Designación de auditores según temáticas; solicitud de información primaria; comunicación del Plan de Auditoría (Orfeo y email institucional).

- Ejecución de visitas en sitio, según planificación y concertación con los líderes y equipos de trabajo de los procesos.

- Análisis de resultados y presentación de informe. En términos generales, se trabajó de la siguiente forma:

    - Definición de métodos y estructura de documento de presentación para reunión de cierre, e informe final, presentado por el líder de auditoria y validado con el equipo auditor.

    - Listas de verificación, evidencias y otros papeles de trabajo digitalizados en carpeta virtual en OneDrive, y en físico, liderado por líder de Auditoría y Edgar Ortiz.

    - Realización de mesas de trabajo para aclaración y definición de dudas frente hallazgos de auditoría, y definición de auditores líderes de consolidación de información (Fortalezas: Javier Sarmiento; Conformidades, Daniela Gordillo; Observaciones: José Pinzón; No Conformidades Edgar Ortiz; anexos 5 y 6 Harold Puentes e Iván Sierra).

    - Presentación para reunión de cierre y preparación de informe final.

1.2. Limitaciones de Auditoría: a continuación, se citan algunos aspectos que pudieron impactar el desarrollo de la presente auditoría:

1. DESCRIPCIÓN GENERAL DEL DESARROLLO DE LA AUDITORIA

- La Auditoría se hubiese potenciado en virtud de complementar el equipo con auditores con perfil en la gestión ambiental y/o con licencia en seguridad y salud en el trabajo, no obstante, miembros del actual equipo de trabajo participaron en la auditoría al Sistema de Gestión y Seguridad en el Trabajo - SG SST y apoyaron labores en el Sistema de Gestión Ambiental – SGA durante la vigencia 2018, además de que gran parte del equipo cuentan con la capacitación virtual de 50 horas del SG SST, brindado por el actual operador de ARL para la UAESP.

- Formación al equipo auditor de la Oficina, según solicitud, respecto a *Papeles de trabajo el éxito de una buena auditoría* y *alta redacción de informes de auditoría y control interno*, la cual fue analizada por la Comisión de Personal (Rad. Uaesp 20197000038553 de mayo de 2019) pero dado el impacto y esfuerzo de inversión fue descartada, recomendando formación de auditores internos, el cual y según radicado UAESP No. 20197000057263 del mes de septiembre de los corrientes, se encuentra en curso de contratación.

- El proceso de evaluación y mejora realizó un ejercicio de autoevaluación, con el fin de aproximarse a la metodología cuantitativa descrita en los anexos del presente informe.

2. CONFORMIDADES Y FORTALEZAS

2.1. Conformidad: Documentación de la Política, Objetivos, Alcance y otros documentos del Sistema de Gestión operante en la UAESP. Se evidenció información documentada en micrositio del Sistema Integrado de Gestión - SIG referente a la Política de Calidad y alcance del Sistema de Gestión. En algunos procesos auditados (Direccionamiento Estratégico, Alumbrado Público, Servicios Funerarios, Gestión de Asuntos Legales y Gestión Documental) se observó que identifican la Política de Calidad en el desarrollo del respectivo proceso.

Así mismo, se evidenció la identificación por parte de los procesos auditados la consulta en el micrositio, los objetivos del SIG, y la relación de aplicación de cada uno de estos.

El proceso Direccionamiento estratégico evidencia el cumplimiento de los criterios como definición de responsabilidades, procedimientos establecidos, medidas de control e indicadores de desempeño.

Los procesos Alumbrado Público, Servicios Funerarios, Gestión Integral de Residuos Sólidos (Línea de servicio de Aprovechamiento), Gestión de las Comunicaciones, Gestión Financiera, Servicio al Ciudadano, Gestión de la Innovación y Gestión del Conocimiento realizaron la consulta en el micrositio del SIG identificando la cadena de valor, describiendo la operación del proceso (proveedores, las entradas, el ciclo de actividades, los productos, los grupos de interés, los resultados y los impactos).

2.2. Conformidad: Información de los Servicios Ofertados. De acuerdo con las evidencias aportadas por los procesos Alumbrado Público y Servicios Funerarios, se evidenció que se brinda información de los servicios ofertados por medios virtuales, por ejemplo, la ventanilla VUC lo referente

2. CONFORMIDADES Y FORTALEZAS

a Alumbrado Público. De manera general, se evidenció que, mediante asesorías personalizadas, página WEB, operadores (contratistas), Ferias del Servicio al Ciudadano y a través de publicidad se informa de los servicios.

El proceso de Gestión Integral de Residuos Sólidos (Línea de servicio de Aprovechamiento), indicó que la información relativa del servicio se proporciona a través de la página Web, y en el punto de atención al ciudadano de la sede administrativa principal.

2.3. Conformidad: Controles asociados con la prestación del servicio suministrado por proveedores externos a nombre de la UAESP. Se observó documentación de los controles aplicados a la gestión operada por el Contratista, por ejemplo, a los Hornos Crematorios en visitas de campo por parte de la UAESP e interventoría.

Se presentó documento (matriz) con corte a abril de 2019, en el que se evalúan características de la presentación del servicio, con la cual se mide la satisfacción del ciudadano. Así mismo, se informó que a través de la Gestión Social y encuentros Comunitarios son mecanismos para interactuar con los usuarios/ciudadanos.

2.4 Conformidad: Análisis de contexto en la Unidad: La Entidad cuenta con un análisis de "*contexto*" donde se identifican las cuestiones internas y externas pertinentes al sistema de Gestión. Según evidencias y análisis del auditor, se encuentra documentado e integrado con otros objetos y campos de aplicación asociados con la Gestión Ambiental y Seguridad de la Información.

2.5 Conformidad: Liderazgo y compromiso por la Alta Dirección: Se evidenció actividades de liderazgo y compromiso, como la revisión por la Alta dirección, seguimiento a los planes, Informe de gestión, Informe de Rendición de Cuentas. Así mismo mediante los comités directivos la Alta Dirección gestiona el seguimiento en temas concernientes con el Sistema Integrado de Gestión. Como evidencia se valida acta de reunión realizado el 27/02/2019.

2.6 Conformidad. Responsabilidad y Autoridades en el SIG: Se evidencia la definición de responsabilidades, como, por ejemplo, mediante la Resolución No 696 de 2017. Adicionalmente se valida el seguimiento que se realiza en los diferentes comités, evidenciando Acta del comité del Modelo de Transformación Organizacional realizado el 24/09/2019, actas del Comité PIGA del 10/06/2019 y 08/07/2019, actas de comité COPASST del 05/03/2019 y 08/05/2019, y actas de comité SGSI del 28/02/2019 y 26/08/2019.

2.7. Conformidad: Propiedad del cliente o partes interesadas pertinentes en la prestación del servicio: Se verifica documento que contiene la caracterización de las partes interesadas. El cual se revisó y se aprobó en el Comité de responsabilidad social de fecha 18/06/2019. Esta gestión contó con la participación de todos los procesos de la unidad. Como evidencia se toma la participación del proceso de Gestión de Asuntos Legales, mediante acta de reunión de 15/08/2019.

2. CONFORMIDADES Y FORTALEZAS

Así mismo se evidencia el documento “portafolio de servicios de la unidad”, donde se encuentra la descripción de los servicios de la Unidad. Este documento se encuentra publicado en la página web en el micrositio del SIG, Modelo de Transformación Organizacional en la Dimensión relacional.

Alumbrado Público y Servicios Funerarios tiene identificada propiedad del cliente, existe una base de datos de proyectos Fotométricos y es manipulada por una sola persona (funcionario) y cuenta con los permisos de TIC.

2.8. Conformidad: Satisfacción del cliente con el servicio ofertado: La Unidad tiene definido el instrumento “Encuesta” para medir la satisfacción del usuario/ciudadano y cumplimiento de necesidades y expectativas. La construcción se realizó tomando el modelo de encuestas aplicado por las Dependencias Misionales y Servicio al Ciudadano. Por lo anterior se evidencia formato con el modelo de “Encuesta” para aplicar en los meses de octubre, noviembre y diciembre. En la construcción de este formato, participaron las Dependencias Misionales, la Oficina Asesora de Planeación, Subdirección Administrativa y Financiera, y Oficina de Control Interno.

Con relación a los ejercicios de medición individuales, los procesos de Alumbrado Público y Servicios Funerarios, informó, el último registro se realizó para el mes de abril de 2019, a través de encuestas, las cuales permitieron evidenciar el nivel de satisfacción del usuario/ciudadano.

2.9. Conformidad: Medición del desempeño del proceso: Se evidenciaron en Alumbrado Público y Servicios Funerarios los indicadores Publicados con la información consolidada hasta el mes de agosto de 2019 (mes de agosto) correspondiente a la medición del desempeño del proceso.

Se permitió evidenciar que, en las últimas mediciones de satisfacción y medición de desempeño, los resultados obtenidos, estuvieron entre bueno y excelente y se han tomado acciones sobre el servicio ofertado, como registros, base de datos, ficha técnica y análisis de encuestas.

La Gestión Integral de Residuos Sólidos (Línea de servicio de Aprovechamiento) informó que miden el desempeño del proceso con los indicadores de gestión y los indicadores de seguimiento establecidos en el plan de inclusión. La última medición para el indicador de gestión se realizó en septiembre de 2019 y para los indicadores del plan de inclusión en junio de 2019.

2.10. Conformidad: Recursos de seguimiento y medición: Al Indagar si cuentan con equipos, maquinaria o instrumentos para medición, pesaje, entre otros**,** para el proceso de Servicios Funerarios se evidenció que, cuentan con equipos propios para medir por ejemplo la emisión de gases de los Hornos Crematorios y de los cuales existe un Programa de mantenimiento elaborado por el concesionario, teniendo en cuenta el Manual de Operaciones entregado por la UAESP.

La Gestión Integral de Residuos Sólidos (Línea de servicio de Aprovechamiento), informó que el proceso cuenta con basculas de pesaje como equipos de medición, estos equipos requieren de

2. CONFORMIDADES Y FORTALEZAS

calibración la cual se realiza trimestral y anualmente, así mismo se toman acciones en resolución de fallas de acuerdo con los tiempos establecidos en el contrato No. 420 de 2018.

Alumbrado Público, Servicios Funerarios, Gestión de las comunicaciones, Servicio al ciudadano, Gestión de la Innovación y Gestión del Conocimiento, informaron que el proceso no requiere de equipos, maquinaria o instrumentos para medición o pesaje.

2.11. Conformidad: Objetivos del SG-SST: De los Objetivos del SST, en la Gestión de Talento Humano se evidenció la última medición realizada y disponible, se verificó el registro, los ciclos de seguimientos y la documentación relacionada, identificando su comunicación y la comprobación de registros.

Se identificó la base con que se planifico el SST para el 2019 en la entidad, se solicitó y se tuvo conocimiento del documento que contiene el plan anual de trabajo 2019 del SST. Se permitió evidenciar que el Plan Estratégico de Seguridad Vial – PESV se encuentra en construcción y se articula con la asesoría técnica que presta la Política de SST.

En relación con las mediciones ambientales de los riesgos prioritarios, provenientes de peligros químicos, físicos y/o biológicos, se evidenciaron en el Informe de Confort Térmico de Sonometric, niveles bajos, por lo que no requirieron de un Plan de Acción.

En la medición de los indicadores, se evidenciaron mediciones anuales, relacionados con la prevalencia y enfermedad laboral (incidencia de enfermedad laboral). Los mensuales, ausentismo y frecuencia de accidentes de trabajo y se determinó el cumplimiento de los indicadores mínimos.

2.12. Conformidad: Comunicación de la Política del Sistema de Gestión de Seguridad y Salud en el trabajo - SG-SST: De acuerdo con las evidencias aportadas por la Gestión de Talento Humano, la Política del SST se publicó a través de Pantallas, carteleras físicas, Intranet, Socialización piso a piso (actas de participación de mayo de 2019) y a través de piezas comunicativas, se permitió evidenciar que la política del SG-STT fue comunicada en la entidad.

2.13. Conformidad: Accidentes de trabajo y enfermedades laborales: Se evidenció que la Gestión de Talento Humano**,** diligencia esta información en el formato establecido y de acuerdo con el procedimiento. Se revisó con el COPASST, el procedimiento que se realiza al momento de presentarse accidentes de trabajo o enfermedades laborales, el cual se realiza mediante correo electrónico, por medio del cual se envía registro del accidente (radicados 4477616 y 4413568), y el reporte del accidente de trabajo y enfermedades laborales a la ARL y EPS.

2.14. Conformidad: Archivo o retención documental del Sistema de Gestión en Seguridad y Salud en el Trabajo SG-SST: Se evidenció en la Gestión de Talento Humano, la tabla de retención

2. CONFORMIDADES Y FORTALEZAS

documental – TRD, asociada con el proceso, y se identificó Serie, subserie o tipo documental, de una muestra documental solicitada, las cuales fueron indicadas por el profesional encargado.

Se evidenció en la muestra documental, que el jefe de la unidad de personal verificó el cumplimiento de la presentación de la declaración y los formatos de Hoja de Vida se encontraron firmados por la jefe de personal; en este caso la Subdirectora Administrativa.

2.15. Conformidad: Consulta partes interesadas: En relación con la disponibilidad para la realización de la consulta por parte de partes interesadas, se identificó que se realiza a través de la intranet y de la ARL Positiva, conforme se verificó con la Gestión de Talento Humano.

La Gestión tecnológica y de la información, determinó que se observa el repositorio destinado para la documentación del MTO definido por la UAESP, al cual se puede acceder sin restricción desde internet, por lo cual se entiende que la política de seguridad informática está disponible para las partes interesadas.

2.16. Conformidad: Aspectos Ambientales: Alumbrado Público y Servicios Funerarios, identificaron como desarrollo del Proceso, la emisión de gases de los Hornos Crematorios, los cuales cuentan con los permisos ambientales requeridos. Se evidenció que se realizan monitoreos de emisiones de Monóxido de Carbono y cada horno Crematorio cuenta con su equipo de Monitoreo (Res. 3267/18 de la SDA). Este servicio de Monitoreo es contratado con un laboratorio debidamente acreditado por el IDEAM.

La Gestión de Apoyo Logístico, informó que se han identificado aspectos ambientales en el desarrollo del proceso en cuanto a los vehículos indicadores de huella de carbono, en la disposición final de los residuos, como aceites, lubricantes y repuestos. La acción para abordarlos se encuentra plasmada dentro de los contratos de mantenimiento y se evidenció el Contrato No. 458 de 2019 numerales 14, 15 y 17 de la Obligaciones específicas del contratista.

2.17. Conformidad: Identificación de peligros con la participación de todos los niveles de la UAESP: Alumbrado Público y Servicios Funerarios, informó que se identifican riesgos de accidentes biológicos y físicos y la verificación de aplicación de las medidas, se realiza con las visitas de inspección, para lo cual aportan como registros, las actas e informes de supervisión y control.

La Gestión de Talento Humano aportó como evidencia, la Matriz de identificación y valoración de riesgos elaborada por la Subred Norte en cumplimiento de la ISO NTC 45 de 2012, lo cual permitió evidenciar en el informe de abril la identificación del origen de los peligros y riesgos:

1. Físico
2. Químico
3. Psicosocial

2. CONFORMIDADES Y FORTALEZAS

4. Biomecánicos
5. Seguridad
6. Rendimientos naturales
7. Mecánico
8. Biológico

Se evidenció en la Matriz de identificación y valoración de riesgos de los EPP, las medidas de Prevención y Control de Peligros se realizan a través de la entrega de los EPP; formatos y fichas y las medidas se encuentran programadas en el Plan Anual de Trabajo.

La Gestión de Apoyo Logístico, informó que conoce algunos peligros asociados en el proceso como son: lesiones físicas (caídas, enfermados laborales), conoce las medidas de prevención como son los EPP, y manifiesta que las personas que realizan trabajos en alturas se les capacita y sensibiliza.

2.18. Conformidad: Plan de prevención y preparación ante emergencias: La Gestión de Talento Humano, aportó como evidencia, el Plan de Prevención, Preparación y Respuesta ante Emergencias (Estándar 46 de la Res.) de la sede Administrativa, Bodegas y Archivos, en el cual se evidenció:

- La divulgación se realizó a través de los Brigadistas, capacitaciones y a través de correos masivos institucionales.
- Que este plan no se encuentra articulado con otro Plan de Emergencias.
- La identificación de las salidas de emergencia en los planos de las instalaciones de la entidad.
- La señalización de las instalaciones, las cuales no son fotoluminiscentes.
- La conformación de la brigada de la UAESP, con la hoja de vida de cada uno de los integrantes, para lo cual se aportó como evidencia en un documento en Excel.
- Los soportes de las capacitaciones y las actas en temas de Neuro seguridad laboral (primeros auxilios - psicológicos) del 08/04/2019 y manejo de extintores del 20/02-2018.
- El Plan de Emergencias y los procedimientos operativos normalizados.

2.19. Conformidad: Verificación normativa: Alumbrado Público y Servicios Funerarios, al Consultar el Normograma publicado en la página de la Entidad, se observó que este ha sido actualizado conforme lo requerido y se evalúa en el Comité Primario, el cual se realiza para el Proceso – Actas del Comité.

Se evidenció en la Gestión de Asuntos Legales, que por medio del comité primario se socializan las normas a incluir y mensualmente solicitan a TICS la publicación del Normograma.

Al realizar la verificación con el publicado se evidenció que es coherente y posee seguimiento mensual, en las actas de comité primario de 26-08-2019 y del 19-09-2019 se observó el seguimiento y actualización al Normograma.

2. CONFORMIDADES Y FORTALEZAS

2.20. Conformidad: Atención a Derechos de Petición y PQRS: En la Gestión de Asuntos Legales se observó el procedimiento para las denuncias de actos de corrupción, el cual se encuentra publicado en la página web de la Unidad en el enlace de atención al ciudadano, enlace trasparencia y acceso a la información pública.

Desde septiembre de 2018 a septiembre de 2019 se recibieron cuatro (4) denuncias por casos de corrupción, denuncias anónimas, las cuales no cuentan con un fundamento legal sólido, al no tener la determinación de tiempo, modo y lugar, lo que impide la vinculación de un sujeto determinado a un proceso en particular. Razón por la cual se profirieron autos inhibitorios, los cuales no hacen tránsito a cosa juzgada, se informó que el anónimo puede complementar la información inicialmente suministrada a efectos de dar curso o tramite a la averiguación de forma pertinente.

Servicio al Ciudadano informó que el registro de entradas de PQRS por los diferentes medios se puede observar en los informes que se remiten a la veeduría. Los canales que se utilizan para la recepción de PQRS son los siguientes: Presencial Avenida Caracas # 53-80, Telefónico (3580400 extensiones 1527 – 1549 – 1529 – 1544 – 1567) El equipo de Servicio al Ciudadano compartió la carpeta por One Drive donde se pueden observar las bases de datos de las PQRS radicadas y los informes remitidos a la veeduría distrital del día 27/09/2019.

2.21. Conformidad: Comunicación externa e interna de la UAESP: La Gestión de las Comunicaciones dio a conocer el Plan Estratégico de Comunicaciones -PEC que esta publicado en la pestaña planes, del proceso Gestión de Comunicaciones, esta es la versión 04 del 30 de noviembre de 2015, el auditado aclara que para la vigencia 2019 se está realizando una modificación, actualización y aprobando una nueva versión del PEC y se aclara por el auditado que esta versión ya está siendo revisada por la Dirección General para la aprobación.

La Gestión de las Comunicaciones dio a conocer los lineamientos de a quien comunican y como comunican en el PEC V4 del 30 de noviembre de 2015, así mismo se observa en el borrador PEC 2019, el porqué, el para qué y cómo se deben implementar estas instrucciones. La gestión auditada aclaró que las actividades se desarrollan basados en el PEC V4 del 30 de noviembre de 2015, hasta tanto se apruebe el PEC 2019 por la Dirección General.

2.22 Conformidad: Seguimiento, medición, análisis y evaluación del desempeño del Sistema de Gestión. La unidad realiza el seguimiento, medición y análisis de los resultados mediante el monitoreo y control de los diferentes planes y matrices definidos para tal fin. Se evidencia este seguimiento en las herramientas (Plan de acción Institucional, SEGPLAN-Metas plan de Desarrollo, Plan anticorrupción y atención al Ciudadano, Matriz de riesgos, Matriz de indicadores de gestión y Planes de Mejoramiento).

Los resultados del Desempeño Ambiental lo realizan los Gestores de cada proceso con el Profesional encargado de la Oficina Asesora de Planeación. Se evidencia ultimo seguimiento realizado mediante acta de reunión del mes de julio de 2019.

2. CONFORMIDADES Y FORTALEZAS

Así mismo, los resultados de la última evaluación de desempeño y eficacia del Sistema Integrado de Gestión se realizaron en la revisión por la Alta dirección correspondiente a los resultados de la vigencia 2018. Se evidencia acta con fecha 22/11/2018.

2.23. Conformidad: Planificación de los cambios al Sistema Integrado de gestión. Se evidencia la planificación e identificación de los cambios, mediante el Plan mantenimiento del Modelo de Transformación Organizacional (MTO), donde en los comités trimestrales se realiza el seguimiento respectivo, identificando cambios al sistema con relación al MIPG, por ejemplo, la actualización de los riesgos, y el desarrollo de los nuevos procesos de Innovación y gestión del conocimiento. El último seguimiento se realizó a junio de 2019.

La Unidad planifica e identifica los cambios en el sistema mediante el seguimiento y cumplimiento del Plan de mantenimiento del MTO. Se evidencia seguimiento a junio de 2019

2.24. Fortaleza: Mejoras en el método para recolección, categorización y visualización de información.

Se evidencia que el proceso de Gestión de Talento Humano ha efectuado mejoras en el método para recolección y categorización de la información (Matriz de Excel) correspondiente a Absentismos laborales.

De igual manera se evidencian mejoras implementadas por el proceso de direccionamiento estratégico en cuanto al método para organización y presentación de la información mediante la herramienta Power BI, la cual facilita la compresión y visualización del avance de los objetivos estratégicos que toman como insumo el Plan de Acción Institucional de la UAESP.

3. OBSERVACIONES

3.1. Observación: Comunicación frente a la prestación del servicio ofertado y suministrado por proveedores externos a nombre de la UAESP. Se informó que los procesos Alumbrado Público y Servicios Funerarios los servicios son prestados por terceros (Contratistas), y que los requisitos asociados al servicio ofertado se comunicaron a través del Convenio 766 de 1997, para el caso del Servicio de Alumbrado Público, el Contrato 311 de 2013 para Servicios Funerarios. Sin embargo, no se aportaron durante la ejecución de la Auditoría registros actualizados que evidenciaran la comunicación de las actuales características de los servicios ofertados.

3.2. Observación: Documentación de Servicios Ofertados como No Conformes: Se observo para los procesos Alumbrado Público, Servicios Funerarios y Gestión Integral de Residuos Sólidos (Línea de servicio de Aprovechamiento)**,** que a la fecha de ejecución de auditoria no se presentaron registros de salidas no conformes.

3. OBSERVACIONES

Para el proceso Servicios Funerarios informó que los Servicios Ofertados No Conformes, se presentan cuando no se da respuesta a una solicitud en los tiempos de respuesta establecidos en el procedimiento (no mayor a 10 días), y se evidencia que cuenta o maneja un formato en Excel de la Salida No Conforme (ECM- PCCPSNC -FM-01).

El proceso de Alumbrado Público informa que se aplica el procedimiento de Revisión, verificación, y aprobación de Diseños fotométricos DES-FM-16 v3.

El procedimiento data como última versión 06/12/2013. Al respecto, se informó que la actualización del procedimiento se contempló como compromiso de revisión por la Dirección del 2018 y está aún en proceso de actualización.

3.3. Identificación de la Política del Sistema Integrado de Gestión.

Frente a la identificación de la Política del SIG por parte de los auditados, no se pudo evidenciar que en los procesos de Apoyo Logístico y Gestión Financiera ubicaran la Política del SIG, lo que evidencia el desconocimiento de esta.

La política del SIG, esta publicada en la página WEB, en el micrositio del MTO; sin embargo, no se evidencia que se hayan utilizado otros medios para su comunicación.

Por lo anterior, se evidencia que la “Política del SIG”, no está integrada con los otros sistemas de gestión, dado que no se identifica el cumplimiento de los requisitos de estos. Se valida su disponibilidad para consulta en la página web, pero no ha sido comunicada o socializada.

3.4. Procesos Necesarios para el Sistema de Gestión.

En lo que tiene que ver con los requisitos del Cliente, se observa que no hay claridad para identificar los requisitos pertinentes de las Partes Interesadas, lo que reduce el enfoque del Cliente, Numeral 4.2. de la NTC ISO 9001 2015.

De igual manera, falta claridad para identificar el diseño y desarrollo del Producto y/o servicio ofertados (se llevan a cabo a través de planes Maestros y Plan de Desarrollo para los procesos de Alumbrado Público y de Servicios Funerarios). Numeral 8.3 de NTC ISO 9001 2015.

Se observa una limitación de Servicios Ofertados, especialmente los asociados con el Proceso de Aprovechamiento, en el cual se documenta el servicio del RURO y en la página web, se ofrecen los servicios de ECAs y el desarrollo de los PRA (que para el ciudadano se llama “Reciclar Transforma”), los cuales no están referenciados como servicios.

3.5. Identificación de los Procesos

Al Solicitar a los auditados la Consulta de los procesos, se logró evidenciar que los identifican en el Micrositio, sin embargo, para el proceso de Gestión del Conocimiento, no fue posible determinar con

3. OBSERVACIONES

certeza, que la operación del proceso es conforme dado que, no existen procedimientos, instructivos documentados aprobados o en proceso de aprobación que den cuenta de la definición de un flujo u orden determinado en la ejecución de actividades. Para el Proceso de Apoyo Logístico, se observa que en el menú del SIG aparece como Gestión de Asuntos Logísticos, pero en el proceso aparece como Gestión Apoyo Logístico.

3.6. Abordaje de Oportunidades

Se evidencia que la metodología de riesgos que se conoce se enfoca en riesgos negativos o adversos y de cómo mediante acciones correctivas se puede disminuir el impacto para la UAESP. sin embargo, el tema del abordaje de oportunidades, no se identifica en forma clara, no se logra evidenciar un lineamiento para determinar, planificar y abordar oportunidades.

3.7. Identificación de Objetivos del SIG

En general, todos los procesos logran ubicar los objetivos del SIG, mediante enlace disponible en el micrositio. En revisión se observa que los objetivos planteados carecen de relación con el SST y MSPI, lo cual genera que la Toma de Conciencia por parte de funcionarios y contratistas no sea efectiva dado que se referencian elementos (política, objetivos) desde la perspectiva del SGC, sin incluir los sistemas SST, Ambiental y SGSI.

Adicionalmente, se logró evidenciar que Los objetivos Ambientales no cuentan con ciclos de medición documentados.

3.8. Establecimiento de Planes de Prevención y Preparación de Emergencias

En relación con la realización de los Simulacros, se pudo evidenciar que éstos se comunican y socializan a través de la Oficina Asesora de Comunicaciones – OAC de la entidad (correos masivos) y se lleva a cabo en la fecha establecida por el Distrito. Se aporta como registro, el Certificado de Participación de la UAESP en el Simulacro realizado en octubre de 2019, emitido por el IDIGER. No obstante, no se aportaron registros del Simulacro realizado en la vigencia 2018, como tampoco el análisis de resultados.

No se evidencia un plan de prevención, preparación y respuesta a situaciones emergentes en términos del MSPI. Sin embargo, GTI allegó como evidencia los documentos *"Documento BIA"* y "*Guía de Continuidad del Negocio*" En ambos casos se observa que los documentos solamente cuentan con un bosquejo de la estructura propuesta. El desarrollo de estos documentos es fundamental para dar un tratamiento a situaciones emergentes que se presentan actualmente evidenciando debilidades en la proyección de recursos tecnológicos (correos electrónicos, servicios de impresión, herramienta antimalware y firewall de la UAESP)

3. OBSERVACIONES

3.9. Estructura para el Seguimiento y Evaluación del PETI

En revisión del documento PETI de la UAESP se observan debilidades en identificación y caracterización de servicios dado que el propósito principal de esta fase es "identificar *cuáles son los servicios institucionales de la entidad, a quién se los ofrece, cuáles son los canales por los que se ofrecen"* en general, las descripciones incluidas en el documento no cumplen las características requeridas. En revisión del documento complementario del MSPI *"Catalogo de servicios"* se observan elementos acordes con lo requerido por la guía *"G.ES.06 - Construcción del PETI - Planeación de la Tecnología para la Transformación Digital" emitida por MinTIC a la luz del modelo IT4+."* . Sin embargo, es necesario hacer una revisión de los servicios listados en ambos documentos pues se evidencian diferencias.

Se evidencia debilidades en la "*Evaluación y compresión de servicios de TI"* dado que el documento no contiene una identificación y clasificación de los servicios institucionales de mayor impacto en términos de complejidad, criticidad, costos, niveles de satisfacción del servicio entre otros.

Se evidencia debilidades en el establecimiento de indicadores que permita evaluar el grado de avance del PETI, en la sección "8.1. Sesión 20: Definir el seguimiento y control del PETIC" se enuncian los tipos de indicadores que deben ser definidos, como por ejemplo un indicador asociado a los gastos de TI "G.ES.06 - Construcción del PETI - Planeación de la Tecnología para la trasformación digital"

3.10. Actualización de Inventario de Activos de Información

Se evidencia que el inventario de activos se encuentra en proceso de ajuste dado que en la versión actual el instrumento allegado como soporte está orientado según la resolución 3564 de 2015 del MINTIC "Transparencia y acceso a la información pública" cuyo alcance es limitado, es necesario la relación y clasificación de los elementos de la infraestructura tecnológica de la UAESP de forma tal que permita establecer una valoración del riesgo asociado.

3.11. Planificación del Modelo de Seguridad y Privacidad de la Información

Con base en la evidencia aportada por GTI se observa documento "*Plan operativo MSPI*" que contiene las actividades documentadas que soportan la implementación del Modelo se seguridad y privacidad de la información. Sin embargo, el documento no hace referencia a la fase a la cual corresponden los documentos planteados y se evidencia que falta incluir el "*plan de transición IPV4-IPV6*".

Según lo definido por MINTIC mediante el Decreto único reglamentario 1078 de 2015 - MSPI se establece la fase *"Evaluación de desempeño"* En la cual se hace especial énfasis en el Monitoreo, medición, análisis y evaluación, No se observa un lineamiento que dé cuenta de cómo se planea dar seguimiento y revisión al MSPI.

3. OBSERVACIONES

3.12. Gestión de Incidentes de Seguridad

Se evidencia mediante correo del 25 de Julio de 2019, reporte de incidente de seguridad enviado por un contratista de la UAESP referente a la exposición de datos sus personales en la plataforma SECOP. El responsable se de seguridad de la información consulta a la SAL para que emita el concepto acerca de la procedencia de supresión u ocultación de la información. La SAL argumenta que en el documento de la propuesta de prestación de servicio se firma la autorización para el tratamiento y publicación de la información relacionada con el contrato. Se sugiere revisar en detalle el caso a la luz de la ley 1581 de 2012 – tratamiento de datos clasificados como sensibles y la ley 1712 de 2014 ley de transparencia la cual especifica la siguiente información de obligatoria publicación para funcionarios y contratistas:

a. Nombres y apellidos completos.
b. País, Departamento y Ciudad de nacimiento.
c. Formación académica.
d. Experiencia laboral y profesional.
e. Empleo, cargo o actividad que desempeña (En caso de contratistas el rol que desempeña con base en el objeto contractual).
f. Dependencia en la que presta sus servicios en la entidad o institución
g. Dirección de correo electrónico institucional.
h. Teléfono Institucional.
i. Escala salarial según las categorías para servidores públicos y/o empleados del sector privado.
j. Objeto, valor total de los honorarios, fecha de inicio y de terminación, cuando se trate contratos de prestación de servicios.

En la plataforma se evidencia que se cargan documentos que contiene datos sensibles que permiten identificar unívocamente a las personas “contratistas”, entre ellos exámenes médicos, documento de identidad, certificaciones bancarias, dirección y teléfonos personales.

3.13. Comunicación y Control en el Desarrollo de Proyectos.

Se evidencian actas de reunión con los procesos de Gestión del conocimiento, Gestión de Comunicaciones, Gestión TIC y Gestión de la Innovación en las cuales se definieron acuerdos y compromisos para desarrollar el proyecto “Escuela Corporativa”, del cual no se allegaron soportes acerca de su estructuración (fases, tiempos) que permitan determinar el grado de avance de este.

En la verificación del enlace enviado por el proceso de Gestión del conocimiento http://moodle.sistemafenix.co/ se observa que la plataforma basada en el LMS (Learning Management System) Moodle se encuentra en un servicio de alojamiento externo a los servidores de Prueba o Producción de la UAESP y bajo un dominio de igual manera externo, en indagación no se evidencia solicitud al proceso de GTIC para validar que los requerimientos técnicos plataforma sean cubiertos por la infraestructura tecnológica de la UAESP ante un eventual publicación del servicio.

3. OBSERVACIONES

3.14. Información Documentada.

Para el Proceso de Direccionamiento Estratégico, Del Listado maestro de Documentos – LMD, se tomó como muestra el procedimiento "Indicadores de Gestión", última actualización del 2015 (El procedimiento se encuentra en revisión y actualización), verificando los registros del Procedimiento se valida el registro de la actividad No.1 actas de reunión de la revisión de los indicadores, se evidencia acta con el Proceso de innovación de junio de 2019, Direccionamiento Estratégico de marzo de 2019 y Gestión de Asuntos Legales de marzo de 2019. Se valida la Actividad No. 4, evidenciando el "tablero general de indicadores" con seguimiento al mes de agosto de 2019. Por último, se revisó los registros de la actividad No 5, los cuales no se están ejecutando y que corresponden a el Informe de autoevaluación de la gestión y el acta de reunión de Comité Directivo. De acuerdo con la muestra tomada, el procedimiento de "Indicadores de gestión" está en proceso de actualización. Verificando los registros de las actividades que se deben mantener documentadas, se evidenció que la actividad No. 5 no se ha documentado y no se cuentan con registros de esta.

Para la identificación y control de la información documentada de origen externo, se observó que El Manual Operativo SIG se actualizó con fecha 25/09/2019, el cual no presenta su actualización en el LMD, en el cual esta referenciado y vigente el manual de calidad anterior. Este documento que se requiere para el SIG, la Unidad debe asegurarse de cumplir con los criterios de los numerales 7.5.2 (creación y actualización), y 7.5.3 (Control de la Información documentada).

3.15. Revisión por la Alta Dirección.

Se evidencia la última revisión por la Alta Dirección el 22/11/2018, con los resultados de la vigencia 2018. De los cuatro compromisos adquiridos se han cumplido tres;

- Continuidad en el cierre de hallazgos
- Presentación al comité MTO el Balance del Plan de Trabajo y
- Continuar con la actualización de criterios de control de las salidas "No Conforme".

La actividad de actualización del procedimiento de las salidas No Conforme está en proceso de actualizarse. Es decir, el compromiso no se ha cumplido. Así mismo, en las entradas para la revisión no se evidencia temas relacionados con los otros subsistemas que permitan identificar una revisión integral.

3.15. Competencia.

3.15.1. Se seleccionaron 48 expedientes (14 correspondientes a profesionales especializados, 19 Profesionales Universitarios, 5 Técnicos, 3 secretarios, 5 Auxiliar Administrativo y 2 conductores; en los cuales se revisó uno a uno el último registro de bienes y rentas y hoja de vida, verificando los requisitos de suscrito, fechas y diligenciamiento. Evidenciándose lo siguiente:

3. OBSERVACIONES

- El 87,5%, Cuarenta y dos (42) funcionarios actualizaron y diligenciaron correctamente los formatos de Hojas de Vida y Bienes y Rentas. De estos 42 funcionarios 3 realizaron su actualización el 1 de agosto de 2019, un día después de la fecha establecida.

- El 12,5% (6 funcionarios) no presentaron la actualización física de sus Hoja de vida ni Bienes y rentas. Al respecto se evidenció solicitud por parte del proceso en espera de actualización o de renuencia, para proceder a trámite administrativo correspondiente (disciplinario).

Al realizar la verificación en el SIDEAP se verifico que 3 de los funcionarios que no habían allegado los formatos al área de talento humano, realizaron su actualización con posterioridad a la fecha establecida.

3.15.2. En la visita realizada a la Gestión de Talento Humano, se verifica la base de datos de Absentismo Laboral, base de datos en la cual se registra todo lo relacionado con la solicitud de permisos laborales PC-04 _Solicitud_permisos_laborales_V2, esta base está clasificada e identificada por tipo de permiso. Se tomo una muestra de 10 solicitudes, lo cual permitió evidenciar, que estos permisos tienen firma de aprobación, son registrados en la base datos y del mismo modo son anexados al expediente laboral del funcionario.

Ahora bien, frente al cumplimiento del procedimiento PC-04 _Solicitud_permisos_laborales_V2, se evidenció que no se está realizando la actividad No. 3 del procedimiento en atención a: ““Cuando es un permiso, se envía escaneado por el medio tecnológico destinado para tal fin; para la aprobación del(a) director(a) de la Unidad.”, no se cuenta con este registro escaneado.

Del mismo modo, no se encuentra registro de la actividad No. 4 del procedimiento: “Informar la aprobación o negación del permiso o ausentismo. Una vez sea evaluada la solicitud, envía el resultado por correo electrónico al solicitante”, no se cuenta con los registros de correo electrónico.

Se informó por parte de los profesionales que atendieron la visita, que se va a presentar un ajuste en el procedimiento en atención a que en la practica el procedimiento que están llevando a cabo es más eficaz y permite tener las evidencias físicas y digitales de los permisos con mayor celeridad.

Por tal razón, a la fecha se deja la observación de que el procedimiento no se está llevando conforme lo establecido en el procedimiento actual.

3.15.3. Se verifica el documento asociado con los acuerdos de gestión, Concertación, Seguimiento y Evaluación de los Acuerdos de Gestión PC-07. En la intranet, en SAF, Talento Humano, se encuentran los acuerdos de gestión de los subdirectores de la Entidad.

En la página web de la Entidad, en donde debe estar publicada la evaluación de desempeño de los gerentes públicos por medio del acuerdo de gestión, se evidencia el enlace en transparencia/3. Estructura orgánica numeral 7. Evaluación desempeño/documento desempeño 2018-2019. Se precisa frente a este enlace que, No abre el documento señalado, abre un documento denominado “Directorio de funcionarios públicos”. Lo cual no permite verificar la actividad No. 3 del procedimiento de los acuerdos de gestión de la unidad PC-07. En la visita de auditoria el día 26 de septiembre de 2019, se

3. OBSERVACIONES

realizó esta observación y se determinó que se iba a verificar el día 30 de septiembre de 2019, ese día no se cumplió con la asistencia de verificación.

Se realizó la evidencia del seguimiento a dos acuerdos de gestión de fecha 23 de agosto de 2019, de la Subdirectora Administrativa y Financiera y del Subdirector de Asuntos Legales.

Se debe precisar que no se evidencio en la visita de auditoria, el cumplimiento del procedimiento en atención a la designación por medio de resolución a los pares que participan en la evaluación de los gestores públicos.

Se informa que se encuentran las evaluaciones de acuerdos de gestión 2018 en una carpeta, porque la dirección los había solicitado para realizar el seguimiento 2019, por esa razón no se encontraban en el expediente del gerente público. Paso seguido, se iban a incorporar a los expedientes, pero no se permitió evidenciar esta actividad. Se informa por parte del profesional que atendió la visita, que en la entidad no hay incentivos pecuniarios para los gerentes públicos, se han realizado comunicaciones y reconocimientos públicos.

3.15. Conocimientos de la Organización: Se verificó el cronograma de capacitación el cual cuenta con indicadores y seguimiento trimestral, y está clasificado por temáticas. Se informa en la visita por parte del profesional encargado que las capacitaciones no reprogramadas dependían de otras entidades, en atención a que son capacitaciones que no tienen costo.

- Frente a las capacitaciones asociadas con SIG, Calidad, Seguridad de la Información y Gestión Ambiental, se observó la realización de la sensibilización de seguridad de la información, de la cual se tomó muestra como evidencia del cumplimiento de estas capacitaciones.

- En relación con las capacitaciones de Gestión ambiental, se tomó evidencia de la sensibilización del PIGA y la realización de la semana ambiental que se realizó en la entidad en el mes de junio.

- Frente a las capacitaciones asociadas con aspectos generales y específicos de las actividades o funciones a realizar que incluían entre otros la identificación de peligros y control de los riesgos en el trabajo y la prevención de accidentes de trabajo y enfermedades laborales, se tomó muestra de la socialización política y objetivo del sistema del mes de mayo 2019, se hace precisión que frente a esta socialización se permiten evidenciar los listados de asistencia y no se informa del contenido de esta.

- Frente la capacitación para el uso de los elementos de protección personal, se anexan 3 muestras de formatos de entrega de elementos de protección personal, informó el profesional encargado que atendió la visita, que en estas entregas se da información relacionada con la identificación de peligros y control de los riesgos en su trabajo y la prevención de accidentes de trabajo.

- Frente a las capacitaciones a los funcionarios de la Unidad respecto de la perdida de documentos – Gestión Documental (DD3), en la visita se tomó evidencia de la sensibilización

3. OBSERVACIONES

de instrumentos archivísticos, del mes de mayo 2019, se debe precisar que la sensibilización cuenta con el listado de asistencia, y no hay contenido de esta.

Del mismo modo se tomó evidencia de la socialización de instrumentos archivísticos, del mes de agosto 2019, la cual cuenta con listados de asistencia, pero no con información del contenido socializado.

- En relación con las capacitaciones a los funcionarios de la Unidad respecto del Manual de Funciones, se informa por parte del profesional que atendió la visita, que no se han realizado dichas capacitaciones, que el manual de funciones se encuentra en la intranet de la entidad, para su verificación, se han realizado las actualizaciones de acuerdo con los ajustes que se han realizado.

Por otro lado, se debe precisar que frente a cada uno de los temas a auditar se identificaron capacitaciones, sensibilizaciones y socializaciones, de las cuales se cuenta los listados de asistencia, pero no se evidencia el contenido de estas, lo cual permite evidenciar una observación al cumplimiento parcial de estas capacitaciones.

Ahora por otro lado, se manifestó, por parte del profesional encargado que atendió la visita, que de las capacitaciones externas no se cuenta con registros de asistencia, ni con el contenido, evidenciando una observación al control del cumplimiento de estas.

4. SOLICITUD DE CORRECCIÓN Y ACCIONES CORRECTIVAS

No.	DESCRIPCIÓN DE LA NO CONFORMIDAD	REQUISITO QUE INCUMPLE
1	En el proceso de Direccionamiento Estratégico, no se evidenció acciones o lineamientos para determinar, planificar y abordar las oportunidades para el logro de los resultados, en el marco del Sistema integrado de Gestión.	Según lo dispuesto en el numeral 6.1.1. y literal a) del numeral 6.1.2 de la NTC ISO 9001:2015 (6.1. NTC ISO 14001:2015)

4. SOLICITUD DE CORRECCIÓN Y ACCIONES CORRECTIVAS		
2	Al verificar las actividades descritas en el Procedimiento Normograma (PC 04 V6) se evidencia que para los procesos Gestión de Apoyo Logístico, Gestión Financiera, Gestión de la Innovación, Gestión de Comunicaciones y Gestión del Conocimiento, no presentan evidencias objetivas respecto de las actividades 1 y 4. Así mismo, al consultar el ultimo Normograma publicado en página WEB (septiembre 2019), se evidencia casillas vacías en la columna "fecha" y "descripción", relacionadas con "seguimiento interno"; en otros casos, se evidencia seguimiento que datan de la vigencia 2018.	Actividades 1 y 4 del Procedimiento Normograma (PC 04 V6)
3	Se evidenciaron los siguientes eventos relacionados con Información Documentada del Sistema Integrado de Gestión, así: • El Proceso de Gestión de la Innovación presenta procedimientos y registros en borrador, pero se evidenció que se usa el procedimiento y algunos formatos. La cadena de valor publicada en el micrositio del SIG en algunos apartes es ilegible. • El proceso de gestión de conocimiento no cuenta con otros documentos que permitan evidenciar la operación de este. La cadena de valor publicada en el micrositio del SIG en algunos apartes es ilegible. • La denominación del Proceso de Gestión Apoyo Logístico es difiere en el micrositio del SIG, lugar disponible de los documentos del Sistema de Gestión, en algunos casos se denomina Gestión de Asuntos Logística o Apoyo Logístico. La cadena de valor publicada en el micrositio del SIG en algunos apartes es ilegible. • La política del Sistema Integrado de Gestión en el micrositio del SIG en algunos apartes se denomina Política de Calidad; y, por ejemplo, al compararla con la contenida y publicada en el documento PIGA, difiere en cuanto a contenido. • El soporte presentado para el Control Documentos (listado maestro de documentos) por el Proceso	Según lo dispuesto en el numeral 7.5 de la NTC ISO 9001:2015 (a) 7.5.2; a) 7.5.3.1; a) y c) 7.5.3.2).

4. SOLICITUD DE CORRECCIÓN Y ACCIONES CORRECTIVAS		
	Direccionamiento Estratégico, no evidencia registro correspondiente a la Cadena de valor de Gestión del Conocimiento; así mismo, en referencia al Formato Proyectos de Inversión FM-04 (V5), no se tiene registro en el *listado maestro de documentos, y por lo contrario* se relaciona y está publicado en el micrositio del SIG. El Manual Operativo publicado y actualizado recientemente en el micrositio del MTO no cuenta con identificación, descripción y versionamiento según lineamientos de la Entidad. De acuerdo con lo anterior, se evidencia incumplimiento frente a la información documentada relacionada con la disponibilidad, preservación de la legibilidad, uso y control de cambios, del cual sugerimos se lidere desde el proceso e Direccionamiento Estratégico el tratamiento correspondiente.	

5. CONCLUSIONES

5.1. La UAESP cuenta con un Sistema de Gestión establecido, en el que se evidencia acciones de planificación, operación y mantenimiento con énfasis en la NTC 9001:2015, sin embargo, es importante fortalecer acciones que promuevan la integración respecto al objeto y campo de aplicación de la Norma Técnica Colombiana (NTC), de 14001, y/o el Sistema de Gestión de SST.

5.2. Se evidencia acciones que promueven la implementación del Sistema de Gestión de Seguridad y Salud en el Trabajo de acuerdo con disposiciones de la Resolución No. 312 de 2019 del Ministerio del Trabajo.

5.3. Se cuenta con plan de trabajo y productos asociados con las dimensiones del Modelo Integrado de Planeación y Gestión – MIPG.

5.4. Continuar fortaleciendo la toma de conciencia frente a los lineamientos estratégicos, y aspectos del Sistema Integrado de Gestión, bajo un enfoque de sentido de pertenencia.

6. RECOMENDACIONES

6.1. La Unidad debe determinar e implementar una metodología que permita identificar y ejecutar acciones con el propósito de establecer oportunidades para el logro de los resultados, en el marco del Sistema integrado de Gestión.

6. RECOMENDACIONES

6.2. Los procesos deben ejecutar y cumplir las actividades establecidas en los procedimientos, formatos, instructivos, manuales, etc.; que son transversales en la Unidad y que permiten mantener y mejorar la eficacia del Sistema Integrado de Gestión.

6.3. Los procesos de la Unidad deben mantener la información documentada, cumpliendo con los criterios de disponibilidad, preservación de la legibilidad, uso y control de cambios. Así mismo asegurar la uniformidad de la información registrada en los documentos del SIG, con relación a la información publicada en los canales de comunicación.

6.4. Para los documentos que componen la estructura del MSPI, se sugiere hacer precisión de los conceptos de *seguridad informática (infraestructura de TI)* y de *seguridad de la información (más amplio pues involucra además de la infraestructura los procedimientos, lineamientos de gestión y uso de información)* en algunas secciones se hace referencia indistinta a estos conceptos.

6.5. Se sugiere definir un cronograma contingente para el desarrollo de las fases 3 y 4 del MSPI faltando poco menos de tres meses para la fecha limite planteada en el PAI y teniendo en cuenta el plazo definido para entidades territoriales tipo A el sistema debería estar en fase de mantenimiento (posterior a la implementación).

APROBACIÓN:

FIRMA	FIRMA(S)
Jefe(s) de Oficina de Control Interno	**Auditor(es) Interno(s)**
FECHA[4]:	**09/OCTUBRE/2019**

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

ANEXO 1

De acuerdo con aplicación de listas de verificación, evidencias recopiladas y analisis realizado por el equipo auditor, los dias 2 y 3 de octubre de 2019 se realizó valoración del Sistema de Gestión, asi:

SISTEMA INTEGRADO DE GESTIÓN

ASPECTOS EVALUADOS:

- **¿SE ESTABLECE?:** Acciones que permiten saber/conocer el qué, cómo, cuándo, quién, entre otros aspectos para la operacionalización.
- **¿SE IMPLEMENTA?:** Acciones que dan cuenta de que lo establecido se aplica o desarrolla en la práctica.
- **¿SE MANTIENE Y MEJORA?:** Acciones relacionadas con proveer, conservar y proseguir con lo establecido.

CRITERIOS DE CALIFICACION: de acuerdo con la evidencias presentadas y verificadas, se evaluará así: SI(10); PARCIAL(5); NO (0)

SEGÚN EVIDENCIA VERIFICADA, DETERMINE LA RELACIÓN FRENTE AL CUMPLIMIENTO DE LA RESPECTIVA NTC

CRITERIOS DE CALIFICACION: Determine la relación entre la evidencia verificada y el objeto y campo de aplicación de la Norma Técnica Colombiana (NTC) correspondiente, permitiendo comprender si existe: RELACIÓN DIRECTA(+10); RELACIÓN INDIRECTA(+0); o NO SE EVIDENCIA RELACIÓN.

	CRITERIOS (ESTANDARES SEGÚN ESTRUCTURA DE ACTO NIVEL DE LA ISO)	¿SE ESTABLECE?	¿SE IMPLEMENTA?	¿SE MANTIENE Y MEJORA?	NTC ISO 9001:2015	NTC ISO 14001:2015	NTC ISO 27001:2013	NTC ISO 45001:2015
4,1	Se determinan las cuestiones externas e internas que son pertinentes	SI	SI	PARCIAL	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
4,1	Se realiza el seguimiento y la revisión de la información sobre estas cuestiones externas e internas.	PARCIAL	SI	PARCIAL	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
RESULTADO DE VERIFICACIÓN COMPRENSIÓN DE LA ORGANIZACIÓN Y SU CONTEXTO					**81,3%**	**81,3%**	**81,3%**	**81,3%**
4,2	Se ha determinado las partes interesadas y los requisitos de estas partes interesadas	SI	PARCIAL	PARCIAL	RELACIÓN DIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA
4,2	Se realiza el seguimiento y la revisión de la información sobre estas partes interesadas y sus requisitos.	SI	PARCIAL	PARCIAL	RELACIÓN DIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA
RESULTADO DE VERIFICACIÓN COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS					**75,0%**	**50,0%**	**50,0%**	**50,0%**
4,3	El alcance del SG, se ha determinado según: Procesos operativos, productos y servicios, instalaciones físicas, ubicación geográfica	PARCIAL	PARCIAL	PARCIAL	RELACIÓN DIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA
4,3	El alcance del SG se ha determinado teniendo en cuenta los problemas externos e internos, las partes interesadas y sus productos y servicios?	SI	SI	PARCIAL	RELACIÓN DIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA
4,3	Se tiene disponible y documentado el alcance del Sistema de Gestion.	SI	SI	SI	RELACIÓN DIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA
4,3	Se tiene justificado y/o documentado los requisitos (exclusiones) que no son aplicables para el Sistema de Gestion?	SI	SI	SI	RELACIÓN DIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA
RESULTADO DE VERIFICACIÓN DETERMINACIÓN DEL ALCANCE					**87,5%**	**62,5%**	**62,5%**	**62,5%**
4,4	Se tienen identificados los procesos necesarios para el sistema de gestión de la Uaesp	SI	PARCIAL	SI	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
4,4	Se tienen establecidos los criterios para la gestion de los procesos teniendo en cuenta las responsabilidades, procedimientos, medidas de control e indicadores de desempeño necesarios que permitan la efectiva operación y control de los mismos.	SI	PARCIAL	SI	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
4,4	Se mantiene y conserva informacion documentada que permita apoyar la operación de estos procesos.	SI	PARCIAL	PARCIAL	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
RESULTADO DE VERIFICACIÓN SISTEMA DE GESTIÓN Y SUS PROCESOS					**83,3%**	**83,3%**	**83,3%**	**83,3%**
CONTEXTO DE LA ORGANIZACIÓN					**83,0%**	**69,3%**	**69,3%**	**69,3%**

PROMEDIO **72,7%**

Nota: Este papel de trabajo y metodologia aplicada por la Oficina de Control Interno, busca aproximarse de forma objetiva y cuantitativamente a los principales aspectos relacionados con la aplicación de la Normas Técnicas Colombianas, ya que los aspectos cualitativos se encuentran en el cuerpo del informe.

ANEXO 1

De acuerdo con aplicación de listas de verificación, evidencias recopiladas y analisis realizado por el equipo auditor, los dias 2 y 3 de octubre de 2019 se realizó valoración del Sistema de Gestión, asi:

SISTEMA INTEGRADO DE GESTIÓN					SEGÚN EVIDENCIA VERIFICADA, DETERMINE LA RELACIÓN FRENTE AL CUMPLIMIENTO DE LA RESPECTIVA NTC			
ASPECTOS EVALUADOS: • **¿SE ESTABLECE?:** Acciones que permiten saber/conocer el qué, cómo, cuándo, quién, entre otros aspectos para la ejecución. • **¿SE IMPLEMENTA?:** Acciones que dan cuenta de que lo establecido se aplica o desarrolla en la práctica. • **¿SE MANTIENE Y MEJORA?:** Acciones relacionadas con proveer, conservar y proseguir con lo establecido. **CRITERIOS DE CALIFICACION:** de acuerdo con la evidencias presentadas y verificadas, se evaluará así: SI(10); PARCIAL(5); NO (0)					**CRITERIOS DE CALIFICACION:** Determine la relación entre la evidencia verificada y el objeto y campo de aplicación de la Norma Técnica Colombiana (NTC) correspondiente, permitiendo comprender si existe: RELACIÓN DIRECTA(+10); RELACIÓN INDIRECTA(+0); o NO SE EVIDENCIA RELACIÓN.			
CRITERIOS (ESTANDARES SEGÚN ESTRUCTURA DE ACTO NIVEL DE LA ISO)		¿SE ESTABLECE?	¿SE IMPLEMENTA?	¿SE MANTIENE Y MEJORA?	NTC ISO 9001:2015	NTC ISO 14001:2015	NTC ISO 27001:2013	NTC ISO 45001:2015
5,1,1	Se demuestra LIDERAZGO Y COMPROMISO por parte de la alta dirección para la eficacia del SGC.	SI	SI	PARCIAL	RELACIÓN DIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA
5,1,2	La Alta Dirección garantiza que los requisitos de los clientes de determinan y se cumplen.	SI	SI	PARCIAL	RELACIÓN DIRECTA	N.A.	N.A.	N.A.
5,1,2	Se determinan y consideran los riesgos y oportunidades que puedan afectar a la conformidad de los productos y servicios y a la capacidad de aumentar la satisfaccion del cliente.	SI	SI	PARCIAL	RELACIÓN DIRECTA	N.A.	N.A.	N.A.
RESULTADO DE VERIFICACIÓN LIDERAZGO Y COMPROMISO					**87,5%**	**62,5%**	**62,5%**	**62,5%**
5,2	La política del SG con la que cuenta actualmente la UAESP está acorde con los propósitos establecidos.	SI	SI	PARCIAL	RELACIÓN DIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA
5,2	La política incluye los minimos compromisos descritos según Norma Tecnica.	SI	SI	PARCIAL	RELACIÓN DIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA
5,2	Se tiene disponible a las partes interesadas pertienentes, se ha comunidado dentro de la organización.	SI	SI	SI	RELACIÓN DIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA
RESULTADO DE VERIFICACIÓN POLÍTICA					**91,7%**	**66,7%**	**66,7%**	**66,7%**
5,3	Se han establecido las responsabilidades y autoridades para los roles pertinentes en toda la organización.	SI	SI	PARCIAL	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
5,3	Se comunican y entienden	SI	SI	PARCIAL	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
5,3	Se informa sobre el desempeño del SG	SI	SI	PARCIAL	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
RESULTADO DE VERIFICACIÓN ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN					**87,5%**	**87,5%**	**87,5%**	**87,5%**
LIDERAZGO					**88,9%**	**58,3%**	**58,3%**	**58,3%**
					PROMEDIO		**66,0%**	

Nota: Este papel de trabajo y metodologia aplicada por la Oficina de Control Interno, busca aproximarse de forma objetiva y cuantitativamente a los principales aspectos relacionados con la aplicación de la Normas Técnicas Colombianas, ya que los aspectos cualitativos se encuentran en el cuerpo del informe.

ANEXO 1

De acuerdo con aplicación de listas de verificación, evidencias recopiladas y analisis realizado por el equipo auditor, los dias 2 y 3 de octubre de 2019 se realizó valoración del Sistema de Gestión, asi:

SISTEMA INTEGRADO DE GESTIÓN

ASPECTOS EVALUADOS:

- **¿SE ESTABLECE?:** Acciones que permiten saber/conocer el qué, cómo, cuándo, quién, entre otros aspectos para la ejecución.
- **¿SE IMPLEMENTA?:** Acciones que dan cuenta de que lo establecido se aplica o desarrolla en la práctica.
- **¿SE MANTIENE Y MEJORA?:** Acciones relacionadas con proveer, conservar y proseguir con lo establecido.

CRITERIOS DE CALIFICACION: de acuerdo con la evidencias presentadas y verificadas, se evaluará así: SI(10); PARCIAL(5); NO (0)

SEGÚN EVIDENCIA VERIFICADA, DETERMINE LA RELACIÓN FRENTE AL CUMPLIMIENTO DE LA RESPECTIVA NTC

CRITERIOS DE CALIFICACION: Determine la relación entre la evidencia verificada y el objeto y campo de aplicación de la Norma Técnica Colombiana (NTC) correspondiente, permitiendo comprender si existe: RELACIÓN DIRECTA(+10); RELACIÓN INDIRECTA(+0); o NO SE EVIDENCIA RELACIÓN.

	CRITERIOS (ESTANDARES SEGÚN ESTRUCTURA DE ACTO NIVEL DE LA ISO)	¿SE ESTABLECE?	¿SE IMPLEMENTA?	¿SE MANTIENE Y MEJORA?	NTC ISO 9001:2015	NTC ISO 14001:2015	NTC ISO 27001:2013	NTC ISO 45001:2015
6,1	Se han establecido los riesgos y oportunidades que deben ser abordados para asegurar que el SG logre los resultados esperados.	PARCIAL	PARCIAL	PARCIAL	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN INDIRECTA
6,1,	La Unidad ha previsto las acciones necesarias para abordar estos riesgos y oportunidades y los ha integrado en los procesos del sistema.	PARCIAL	PARCIAL	PARCIAL	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN INDIRECTA
6,1,2	Se han determinado Aspectos e Impactos Ambientales asociados y los significativos. Se han comunicado a los diferentes niveles de la Unidad.	SI	PARCIAL	PARCIAL		RELACIÓN DIRECTA		
6,1,2	Se han Identificado peligros asociados con labores y actividades del SG, se han evaluado y definido acciones de intervención.	SI	PARCIAL	PARCIAL				RELACIÓN DIRECTA
6,1,3	Se mantiene y conserva documentado los requisitos legales asociados con el SG (Ambiental y SST).	SI	SI	PARCIAL		RELACIÓN DIRECTA		RELACIÓN DIRECTA
6,1,4	Se han determinado acciones para abordar los requisitos legales y otros requisitos del SG (Ambiental y SST).	SI	SI	PARCIAL		RELACIÓN DIRECTA		RELACIÓN DIRECTA
RESULTADO DE VERIFICACIÓN ACCIONES PARA ABORDAR RIESGOS Y OPORTUNIDADES					**62,5%**	**75,0%**	**62,5%**	**65,0%**
6,2	Se han definido objetivos del SG	SI	SI	PARCIAL	RELACIÓN DIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA
6,2	Se han comunicado los objetivos del SG	SI	SI	PARCIAL	RELACIÓN DIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA
RESULTADO OBJETIVOS Y PLANIFICACIÓN PARA LOGRARLOS					**87,5%**	**87,5%**	**87,5%**	**87,5%**
6,3	Existe un lineamiento definido para determinar la necesidad de cambios en el SG y la gestión de su implementación?	SI	SI	SI	RELACIÓN DIRECTA		RELACIÓN DIRECTA	
RESULTADO DE VERIFICACIÓN PLANIFICACION DE LOS CAMBIOS					**100,0%**	**0,1%**	**100,0%**	**0,0%**
PLANIFICACIÓN					**80,0%**	**78,6%**	**80,0%**	**71,4%**

PROMEDIO **77,5%**

Nota: Este papel de trabajo y metodologia aplicada por la Oficina de Control Interno, busca aproximarse de forma objetiva y cuantitativamente a los principales aspectos relacionados con la aplicación de la Normas Técnicas Colombianas, ya que los aspectos cualitativos se encuentran en el cuerpo del informe.

ANEXO 1

De acuerdo con aplicación de listas de verificación, evidencias recopiladas y analisis realizado por el equipo auditor, los dias 2 y 3 de octubre de 2019 se realizó valoración del Sistema de Gestión, asi:

SISTEMA INTEGRADO DE GESTIÓN

ASPECTOS EVALUADOS:

- **¿SE ESTABLECE?:** Acciones que permiten saber/conocer el qué, cómo, cuándo, quién, entre otros aspectos para la ejecución.
- **¿SE IMPLEMENTA?:** Acciones que dan cuenta de que lo establecido se aplica o desarrolla en la práctica.
- **¿SE MANTIENE Y MEJORA?:** Acciones relacionadas con proveer, conservar y proseguir con lo establecido.

CRITERIOS DE CALIFICACION: de acuerdo con la evidencias presentadas y verificadas, se evaluará así: SI(10); PARCIAL(5); NO (0)

CRITERIOS (ESTANDARES SEGÚN ESTRUCTURA DE ACTO NIVEL DE LA ISO)		¿SE ESTABLECE?	¿SE IMPLEMENTA?	¿SE MANTIENE Y MEJORA?	NTC ISO 9001:2015	NTC ISO 14001:2015	NTC ISO 27001:2013	NTC ISO 45001:2015
7,1	La Unidad ha determinado y proporcionado los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SG (incluidos los requisitos de las personas, mediambientales y de infraestructura)	SI	SI	SI	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
7,1	Se ha determinado, porporcionado y mantenido el ambiente necesarios para la operación de procesos	SI	SI	PARCIAL	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
7,1,5	Dispone de métodos eficaces para garantizar la trazabilidad durante el proceso operacional.	SI	SI	SI	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
7,1,5	Se calibran o verifican equipos de medición necesarios para la operación del proceso.	SI	SI	SI	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
7,1,6	Ha determinado la UAESP los conocimientos necesarios para el funcionamiento de sus procesos y el logro de la conformidad de los productos y servicios y, ha implementado un proceso de experiencias adquiridas.	SI	PARCIAL	SI	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
RESULTADO DE VERIFICACIÓN RECURSOS					**95,0%**	**95,0%**	**95,0%**	**95,0%**
7,2	Se ha determinado que las personas sean competentes, basandose en la educación, fromación o experiencia .	SI	SI	SI	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
7,2	Se han determinado acciones para adquirir la competencia necesaria y evaluar la eficacia las acciones tomadas	SI	PARCIAL	PARCIAL	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
RESULTADO COMPETENCIA					**87,5%**	**87,5%**	**87,5%**	**87,5%**
7,3	Existe lineamiento o mecanismos que faciliten validar la toma de conciencia referente a los aspectos del SG respecto de las personas que realizan el trabajo.	PARCIAL	PARCIAL	PARCIAL	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
7,3	De los aspectos indagados según listas de verificación (politica, objetivos, contribución, implicaciones de incumplimiento, Aspectos ambientales, peligros, entre otros), se evidenció conciencia por parte de los auditados	SI	PARCIAL	PARCIAL	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
RESULTADO TOMA DE CONCIENCIA					**68,8%**	**68,8%**	**68,8%**	**68,8%**
7,4	Se tiene cuenta con linemientos para las comunicaciones internas y externas del SIG dentro de la organización.	SI	SI	PARCIAL	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
7,4	De los aspectos verificados según listas de verificación (qué, cuándo, a quién, cómo, quien) son claros y conocidos en la Unidad	SI	PARCIAL	PARCIAL	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
RESULTADO COMUNICACIÓN					**81,3%**	**81,3%**	**81,3%**	**81,3%**
7,5	Se ha establecido la información documentada requerida por la norma y necesaria para la implementación y funcionamiento eficaz del SG	SI	PARCIAL	PARCIAL	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
7,5	Los lineamientos para la creación, actualización, y control de la información docuemnntada se desarrolla en la Unidad.	SI	PARCIAL	PARCIAL	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
RESULTADO INFORMACIÓN DOCUMENTADA					**75,0%**	**75,0%**	**75,0%**	**75,0%**
APOYO					**84,6%**	**84,6%**	**84,6%**	**84,6%**

SEGÚN EVIDENCIA VERIFICADA, DETERMINE LA RELACIÓN FRENTE AL CUMPLIMIENTO DE LA RESPECTIVA NTC

CRITERIOS DE CALIFICACION: Determine la relación entre la evidencia verificada y el objeto y campo de aplicación de la Norma Técnica Colombiana (NTC) correspondiente, permitiendo comprender si existe: RELACIÓN DIRECTA(+10); RELACIÓN INDIRECTA(+0); o NO SE EVIDENCIA RELACIÓN.

PROMEDIO	**84,6%**

Nota: Este papel de trabajo y metodologia aplicada por la Oficina de Control Interno, busca aproximarse de forma objetiva y cuantitativamente a los principales aspectos relacionados con la aplicación de la Normas Técnicas Colombianas, ya que los aspectos cualitativos se encuentran en el cuerpo del informe.

ANEXO 1

De acuerdo con aplicación de listas de verificación, evidencias recopiladas y analisis realizado por el equipo auditor, los dias 2 y 3 de octubre de 2019 se realizó valoración del Sistema de Gestión, asi:

SISTEMA INTEGRADO DE GESTIÓN

ASPECTOS EVALUADOS:

- **¿SE ESTABLECE?:** Acciones que permiten saber/conocer el qué, cómo, cuándo, quién, entre otros aspectos para la ejecución.
- **¿SE IMPLEMENTA?:** Acciones que dan cuenta de que lo establecido se aplica o desarrolla en la práctica.
- **¿SE MANTIENE Y MEJORA?:** Acciones relacionadas con proveer, conservar y proseguir con lo establecido.

CRITERIOS DE CALIFICACION: de acuerdo con la evidencias presentadas y verificadas, se evaluará así: SI(10); PARCIAL(5); NO (0)

CRITERIOS (ESTANDARES SEGÚN ESTRUCTURA DE ACTO NIVEL DE LA ISO)		¿SE ESTABLECE?	¿SE IMPLEMENTA?	¿SE MANTIENE Y MEJORA?
8,1,	Se planifican, implementan y controlan los procesos necesarios para cumplir los requisitos para la provision de servicios.	SI	SI	SI
8,1,	La salida de esta planificación es adecuada para las operaciones de la UAESP.	SI	SI	SI
8,1,1	Planifica, implementa, controla y ,mantiene procesos necesariuos para cumplir requisitos del SG SST y SGA	SI	SI	SI
8,1,2	La UAESP cuenta con lineamiento para eliminar peligros y reducir riesgos de SST SGA	SI	SI	SI
8,1,4	La UAESP cuenta con lineamientos para controlar la compra de productos y servicios de forma de asegure la conformidad del SG SST SGA	SI	PARCIAL	PARCIAL
RESULTADO PLANIFICACIÓN Y CONTROL OPERACIONAL				
8,2,1	La comunicación con los clientes incluye información relativa a los productos y servicios.	SI	SI	SI
8,2,1	Se obtiene la retroalimentación de los clientes relativa a los productos y servicios, incluyendo las quejas.	SI	PARCIAL	PARCIAL
8,2,2	Se determinan los requisitos legales y reglamentaarios para los productos y servicios que se ofrecen y aquellos considerados necesarios para la UAESP.	SI	SI	SI
8,2,3	La UAESP se asegura que tiene la capacidad de cumplir los requisitos de los productos y servicios ofrecidos.	PARCIAL	PARCIAL	PARCIAL
8,2,3	La UAESP revisa los requisitos del cliente antes de comprometerse a suministrar productos y servicios a este.	PARCIAL	PARCIAL	PARCIAL
8,2,3	Se confirma los requisitos del cliente antes de la aceptación por parte de estos, cuando no se ha proporcionado informacion documentada al respecto.	PARCIAL	PARCIAL	PARCIAL
8,2,4	Las personas son conscientes de los cambios en los requisitos de los productos y servicios, se modifica la informacion documentada pertienente a estos cambios.	PARCIAL	PARCIAL	PARCIAL
RESULTADO REQUISITOS PARA LOS PRODUCTOS Y SERVICIOS				
8,2	La UAESP ha definido procesos necesarios acerca de como prepararse y responder a situaciones potenciales de emergencia	SI	PARCIAL	PARCIAL
8,2	Se evalua y revisa periodicamente los procesos y acciones de respuesta planificadas	SI	PARCIAL	PARCIAL
RESULTADO PREPARACIÓN Y RESPUESTA ANTE EMERGENCIA				
8,3,1	Se establece, implementa y mantiene un proceso de diseño y desarrollo que sea adecuado para asegurar la posterior provición de los servicios.	PARCIAL	PARCIAL	PARCIAL
8,3,2	La UAESP determina todas las etapas y controles necesarios para el diseño y desarrollo de productos y servicios.	PARCIAL	PARCIAL	PARCIAL
8,3,3	Al determinar los requisitos esenciales para los tipos específicos de productos y servicios a desarrollar, se consideran los requisitos funcionales y de desempeño, los requisitos legales y	PARCIAL	PARCIAL	PARCIAL
8,3,4	Se aplican los controles al proceso de diseño y desarrollo, se definen los resultados a lograr.	PARCIAL	PARCIAL	PARCIAL
8,3,5	Se conserva información documentada sobre las salidas del diseño y desarrollo.	PARCIAL	PARCIAL	PARCIAL
8,3,6	Se identifican, revisan y controlan los cambios hechos durante el diseño y desarrollo de los productos y servicios	PARCIAL	PARCIAL	PARCIAL
RESULTADO DISEÑO Y DESARROLLO DE PRODUCTOS Y SERVICIOS				

SEGÚN EVIDENCIA VERIFICADA, DETERMINE LA RELACIÓN FRENTE AL CUMPLIMIENTO DE LA RESPECTIVA NTC

CRITERIOS DE CALIFICACION: Determine la relación entre la evidencia verificada y el objeto y campo de aplicación de la Norma Técnica Colombiana (NTC) correspondiente, permitiendo comprender si existe: RELACIÓN DIRECTA(+10); RELACIÓN INDIRECTA(+0); o NO SE EVIDENCIA RELACIÓN.

NTC ISO 9001:2015	NTC ISO 14001:2015	NTC ISO 27001:2013	NTC ISO 45001:2015
RELACIÓN DIRECTA	N.A.	N.A.	N.A.
RELACIÓN DIRECTA	N.A.	N.A.	N.A.
N.A.	RELACIÓN DIRECTA	N.A.	RELACIÓN DIRECTA
N.A.	RELACIÓN DIRECTA	N.A.	RELACIÓN DIRECTA
N.A.	RELACIÓN DIRECTA	N.A.	RELACIÓN DIRECTA
100,0%	**91,7%**	**0,0%**	**91,7%**
RELACIÓN DIRECTA	N.A.	N.A.	N.A.
RELACIÓN DIRECTA	N.A.	N.A.	N.A.
RELACIÓN DIRECTA	N.A.	N.A.	N.A.
RELACIÓN DIRECTA	N.A.	N.A.	N.A.
RELACIÓN DIRECTA	N.A.	N.A.	N.A.
RELACIÓN DIRECTA	N.A.	N.A.	N.A.
RELACIÓN DIRECTA	N.A.	N.A.	N.A.
75,0%	**N.A.**	**N.A.**	**N.A.**
N.A.	RELACIÓN DIRECTA	RELACIÓN INDIRECTA	RELACIÓN DIRECTA
N.A.	RELACIÓN DIRECTA	RELACIÓN INDIRECTA	RELACIÓN DIRECTA
N.A.	**75,0%**	**50,0%**	**75,0%**
RELACIÓN DIRECTA	N.A.	N.A.	N.A.
RELACIÓN DIRECTA	N.A.	N.A.	N.A.
RELACIÓN DIRECTA	N.A.	N.A.	N.A.
RELACIÓN DIRECTA	N.A.	N.A.	N.A.
RELACIÓN DIRECTA	N.A.	N.A.	N.A.
RELACIÓN DIRECTA	N.A.	N.A.	N.A.
62,5%	**N.A.**	**N.A.**	**N.A.**

8,4	La UAESP asegura que los procesos, productos y servicios suministrados externamente son conforme a los requisitos.	SI	SI	PARCIAL	RELACIÓN DIRECTA	N.A.	N.A.	N.A.
8,4	Se determina los controles a aplicar a los procesos, productos y servicios suministrados externamente.	SI	SI	SI	RELACIÓN DIRECTA	N.A.	N.A.	N.A.
8,4	Se determina y aplica criterios para la evaluación, selección, seguimiento del desempeño y la reevaluación de los proveedores externos.	SI	SI	SI	RELACIÓN DIRECTA	N.A.	N.A.	N.A.
8,4,2	Se asegura que los procesos suministrados externamente permanecen dentro del control de su sistema de gestion	SI	SI	PARCIAL	RELACIÓN DIRECTA	N.A.	N.A.	N.A.
8,4,3,	La UAESP comunica a los proveedores externos sus requisitos para los procesos, productos y servicios.	SI	SI	SI	RELACIÓN DIRECTA	N.A.	N.A.	N.A.
8,4,3,	Se comunica las interacciones del proveedor externo con la UAESP.	SI	SI	SI	RELACIÓN DIRECTA	N.A.	N.A.	N.A.
RESULTADO CONTROL DE PRODUCTOS Y SERVICIOS SUMINISTRADOS EXTERNAMENTE					**95,8%**	**N.A.**	**N.A.**	**N.A.**
8,5,1	Dispone de información documentada que defina las características de los productos a producir, servicios a prestar, o las actividades a desempeñar.	SI	SI	PARCIAL	RELACIÓN DIRECTA	N.A.	N.A.	N.A.
8,5,2	Se conserva información documentada para permitir la trazabilidad.	SI	SI	SI	RELACIÓN DIRECTA	N.A.	N.A.	N.A.
8,5,3	La UAESP cuida la propiedad de los clientes o proveedores externos mientras esta bajo el control de la UAESP o siendo utilizada por la misma.	SI	SI	SI	RELACIÓN DIRECTA	N.A.	N.A.	N.A.
8,5,3	Se Identifica, verifica, protege y salvaguarda la propiedad de los clientes o de los proveedores externos suministrada para su utilización o incorporación en los productos y servicios.	SI	SI	SI	RELACIÓN DIRECTA	N.A.	N.A.	N.A.
8,5,5	Se cumplen los requisitos para las actividades posteriores a la entrega asociadas con los productos y servicios.	PARCIAL	PARCIAL	PARCIAL	RELACIÓN DIRECTA	N.A.	N.A.	N.A.
8,5,6	La UAESP revisa y controla los cambios en la producción o la prestación del servicio para asegurar la conformidad con los requisitos.	SI	SI	SI	RELACIÓN DIRECTA	N.A.	N.A.	N.A.
RESULTADO PRODUCCIÓN Y PRESTACIÓN DEL SERVICIO					**91,7%**	**N.A.**	**N.A.**	**N.A.**
8,7	La organización se asegura que las salidas no conformes con sus requisitos se identifican y se controlan para prevenir su uso o entrega.	SI	SI	PARCIAL	RELACIÓN DIRECTA	N.A.	N.A.	N.A.
8,7	La organización toma las acciones adecuadas de acuerdo a la naturaleza de la no conformidad y su efecto sobre la conformidad de los productos y servicios.	PARCIAL	PARCIAL	PARCIAL	RELACIÓN DIRECTA	N.A.	N.A.	N.A.
8,7	Se verifica la conformidad con los requisitos cuando se corrigen las salidas no conformes.	PARCIAL	PARCIAL	PARCIAL	RELACIÓN DIRECTA	N.A.	N.A.	N.A.
8,7	La organización trata las salidas no conformes de una o más maneras	PARCIAL	PARCIAL	PARCIAL	RELACIÓN DIRECTA	N.A.	N.A.	N.A.
8,7	La organización conserva información documentada que describa la no conformidad, las acciones tomadas, las concesiones obtenidas e identifique la autoridad que decide la acción con respecto a la no conformidad.	PARCIAL	PARCIAL	PARCIAL	RELACIÓN DIRECTA	N.A.	N.A.	N.A.
RESULTADO CONTROL DE LOS RESULTADOS DEL PROCESO, PRODUCTO Y SERVICIO NO CONFORME					**67,5%**	**N.A.**	**N.A.**	**N.A.**

OPERACIÓN	**73,2%**	**85,0%**	**50,0%**	**85,0%**

PROMEDIO **73,3%**

Nota: Este papel de trabajo y metodologia aplicada por la Oficina de Control Interno, busca aproximarse de forma objetiva y cuantitativamente a los principales aspectos relacionados con la aplicación de la Normas Técnicas Colombianas, ya que los aspectos cualitativos se encuentran en el cuerpo del informe.

ANEXO 1

De acuerdo con aplicación de listas de verificación, evidencias recopiladas y analisis realizado por el equipo auditor, los dias 2 y 3 de octubre de 2019 se realizó valoración del Sistema de Gestión, asi:

SISTEMA INTEGRADO DE GESTIÓN

ASPECTOS EVALUADOS:

- **¿SE ESTABLECE?:** Acciones que permiten saber/conocer el qué, cómo, cuándo, quién, entre otros aspectos para la ejecución.
- **¿SE IMPLEMENTA?:** Acciones que dan cuenta de que lo establecido se aplica o desarrolla en la práctica.
- **¿SE MANTIENE Y MEJORA?:** Acciones relacionadas con proveer, conservar y proseguir con lo establecido.

CRITERIOS DE CALIFICACION: de acuerdo con la evidencias presentadas y verificadas, se evaluará así: SI(10); PARCIAL(5); NO (0)

SEGÚN EVIDENCIA VERIFICADA, DETERMINE LA RELACIÓN FRENTE AL CUMPLIMIENTO DE LA RESPECTIVA NTC

CRITERIOS DE CALIFICACION: Determine la relación entre la evidencia verificada y el objeto y campo de aplicación de la Norma Técnica Colombiana (NTC) correspondiente, permitiendo comprender si existe: RELACIÓN DIRECTA(+10); RELACIÓN INDIRECTA(+0); o NO SE EVIDENCIA RELACIÓN.

CRITERIOS (ESTANDARES SEGÚN ESTRUCTURA DE ACTO NIVEL DE LA ISO)		¿SE ESTABLECE?	¿SE IMPLEMENTA?	¿SE MANTIENE Y MEJORA?	NTC ISO 9001:2015	NTC ISO 14001:2015	NTC ISO 27001:2013	NTC ISO 45001:2015
9,1	La UAESP determina que necesita seguimiento y medición.	SI	SI	SI	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
9,1	Determina los métodos de seguimiento, medición, análisis y evaluación para asegurar resultados validos.	SI	SI	SI	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
9,1	Determina cuando se lleva a cabo el seguimiento y la medición.	SI	PARCIAL	PARCIAL	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
9,1	Determina cuando analizar y evaluar los resultados del seguimiento y medición.	SI	PARCIAL	PARCIAL	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
9,1	Evalúa el desempeño y la eficacia del SG	SI	SI	PARCIAL	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
9,1,2	La UAESP realiza seguimiento de las percepciones de los clientes del grado en que se cumplen sus necesidades y expectativas.	SI	PARCIAL	PARCIAL	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
9,1,2	Determina los métodos para obtener, realizar el seguimiento y revisar la información.	SI	PARCIAL	PARCIAL	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
9,1,3	La UAESP analiza y evalúa los datos y la información que surgen del seguimiento y la medición.	SI	PARCIAL	PARCIAL	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
RESULTADO SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN					**82,8%**	**82,8%**	**82,8%**	**82,8%**
9,2	La organización lleva a cabo auditorías internas a intervalos planificados.	SI	SI	SI	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
9,2	Las auditorías proporcionan información sobre el SG conforme con los requisitos propios y de norma marco	SI	SI	SI	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
9,2	La organización planifica, establece, implementa y mantiene uno o varios programas de auditoría.	SI	SI	SI	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
9,2	Define los criterios de auditoría y el alcance para cada una.	SI	SI	SI	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
9,2	Selecciona los auditores y lleva a cabo auditorías para asegurar la objetividad y la imparcialidad del proceso.	SI	SI	SI	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
9,2	Asegura que los resultados de las auditorias se informan a la dirección.	SI	SI	SI	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
9,2	Realiza las correcciones y toma las acciones correctivas adecuadas.	SI	SI	SI	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
9,2	Conserva información documentada como evidencia de la implementación del programa de auditoría y los resultados.	SI	SI	SI	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
RESULTADO AUDITORÍA INTERNA					**100,0%**	**100,0%**	**100,0%**	**100,0%**
9,3	La alta dirección revisa el SGC a intervalos planificados, para asegurar su conveniencia, adecuación, eficacia y alineación continua con la estrategia de la organización.	SI	SI	PARCIAL	RELACIÓN DIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA
9,3	Se evidenciaron las Entradas de la revision por la direccion, según listas de verificación aplicadas	SI	PARCIAL	PARCIAL	RELACIÓN DIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA
9,3	Se evidenciaron las Salidas segun revision por la direccion, según listas de verificación aplicadas	SI	SI	PARCIAL	RELACIÓN DIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA
RESULTADO REVISIÓN POR LA DIRECCIÓN					**83,3%**	**58,3%**	**58,3%**	**58,3%**
EVALUACIÓN Y DESEMPEÑO					**90,1%**	**86,2%**	**86,2%**	**86,2%**

PROMEDIO **87,2%**

Nota: Este papel de trabajo y metodologia aplicada por la Oficina de Control Interno, busca aproximarse de forma objetiva y cuantitativamente a los principales aspectos relacionados con la aplicación de la Normas Técnicas Colombianas, ya que los aspectos cualitativos se encuentran en el cuerpo del informe. Las indicaciones asociadas con Auditoria Interna se realizaron bajo un esquema de autoevaluación, con el fin de que el modelo no se afectara.

ANEXO 1

De acuerdo con aplicación de listas de verificación, evidencias recopiladas y analisis realizado por el equipo auditor, los dias 2 y 3 de octubre de 2019 se realizó valoración del Sistema de Gestión, asi:

SISTEMA INTEGRADO DE GESTIÓN

ASPECTOS EVALUADOS:

- **¿SE ESTABLECE?:** Acciones que permiten saber/conocer el qué, cómo, cuándo, quién, entre otros aspectos para la ejecución.
- **¿SE IMPLEMENTA?:** Acciones que dan cuenta de que lo establecido se aplica o desarrolla en la práctica.
- **¿SE MANTIENE Y MEJORA?:** Acciones relacionadas con proveer, conservar y proseguir con lo establecido.

CRITERIOS DE CALIFICACION: de acuerdo con la evidencias presentadas y verificadas, se evaluará así: SI(10); PARCIAL(5); NO (0)

SEGÚN EVIDENCIA VERIFICADA, DETERMINE LA RELACIÓN FRENTE AL CUMPLIMIENTO DE LA RESPECTIVA NTC

CRITERIOS DE CALIFICACION: Determine la relación entre la evidencia verificada y el objeto y campo de aplicación de la Norma Técnica Colombiana (NTC) correspondiente, permitiendo comprender si existe: RELACIÓN DIRECTA(+10); RELACIÓN INDIRECTA(+0); o NO SE EVIDENCIA RELACIÓN.

	CRITERIOS (ESTANDARES SEGÚN ESTRUCTURA DE ACTO NIVEL DE LA ISO)	¿SE ESTABLECE?	¿SE IMPLEMENTA?	¿SE MANTIENE Y MEJORA?	NTC ISO 9001:2015	NTC ISO 14001:2015	NTC ISO 27001:2013	NTC ISO 45001:2015
10,1	La organización ha determinado y seleccionado las oportunidades de mejora e implementado las acciones necesarias para cumplir con los requisitos del cliente y mejorar su satisfacción.	SI	PARCIAL	PARCIAL	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
RESULTADO GENERALIDADES					**75,0%**	**75,0%**	**75,0%**	**75,0%**
10,2	La organización reacciona ante la no conformidad, toma acciones para controlarla y corregirla. (Incidentes en SST)	SI	SI	PARCIAL	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
10,2	Revisa la eficacia de cualquier acción correctiva tomada.	SI	PARCIAL	PARCIAL	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA	RELACIÓN DIRECTA
RESULTADO NO CONFORMIDAD Y ACCIÓN CORERECTIVA					**81,3%**	**81,3%**	**81,3%**	**81,3%**
10,3	La organización mejora continuamente la conveniencia, adecuación y eficacia del SG	SI	SI	PARCIAL	RELACIÓN DIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA	RELACIÓN INDIRECTA
RESULTADO MEJORA CONTINUA					**87,5%**	**62,5%**	**62,5%**	**62,5%**
MEJORA					**81,3%**	**75,0%**	**75,0%**	**75,0%**

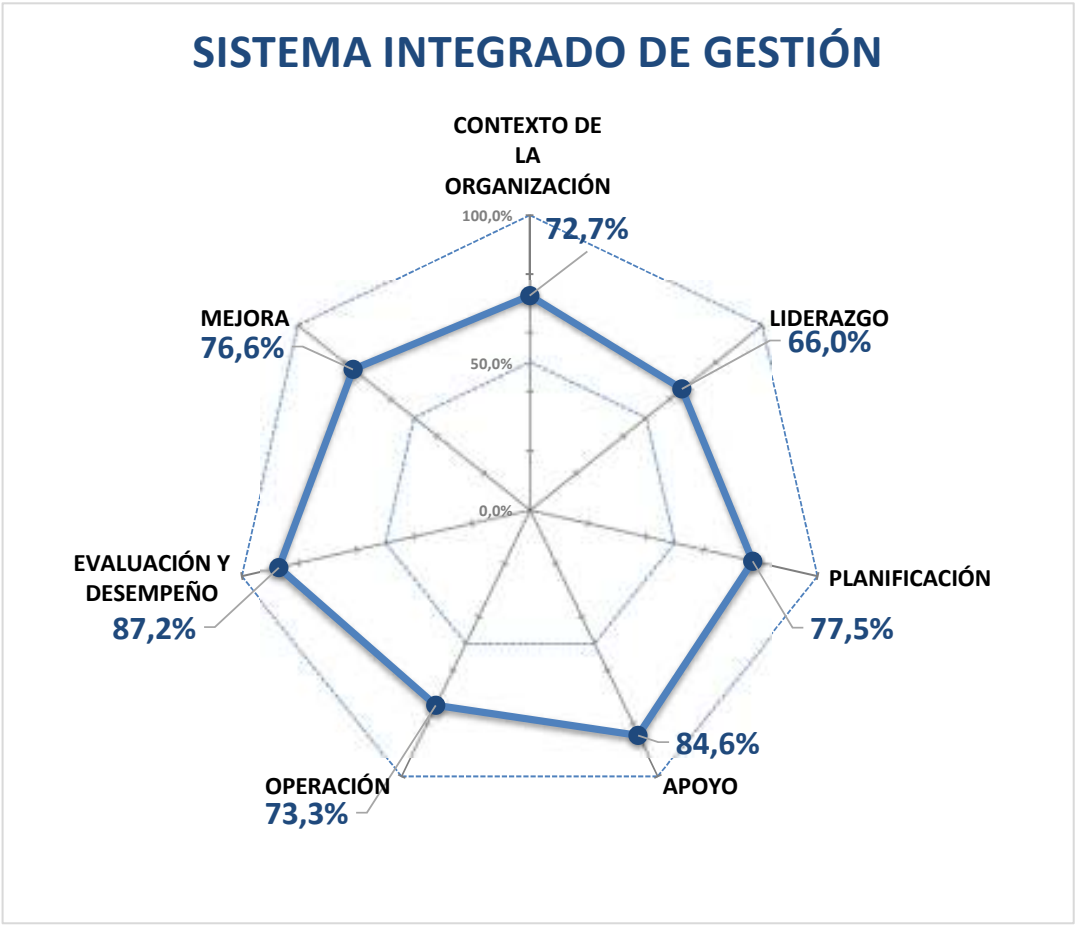
PROMEDIO **76,6%**

Nota: Este papel de trabajo y metodologia aplicada por la Oficina de Control Interno, busca aproximarse de forma objetiva y cuantitativamente a los principales aspectos relacionados con la aplicación de la Normas Técnicas Colombianas, ya que los aspectos cualitativos se encuentran en el cuerpo del informe.

ANEXO 2: Estimación de avance según criterios verificados y metodología descrita en Anexo 1

SISTEMA INTEGRADO DE GESTIÓN

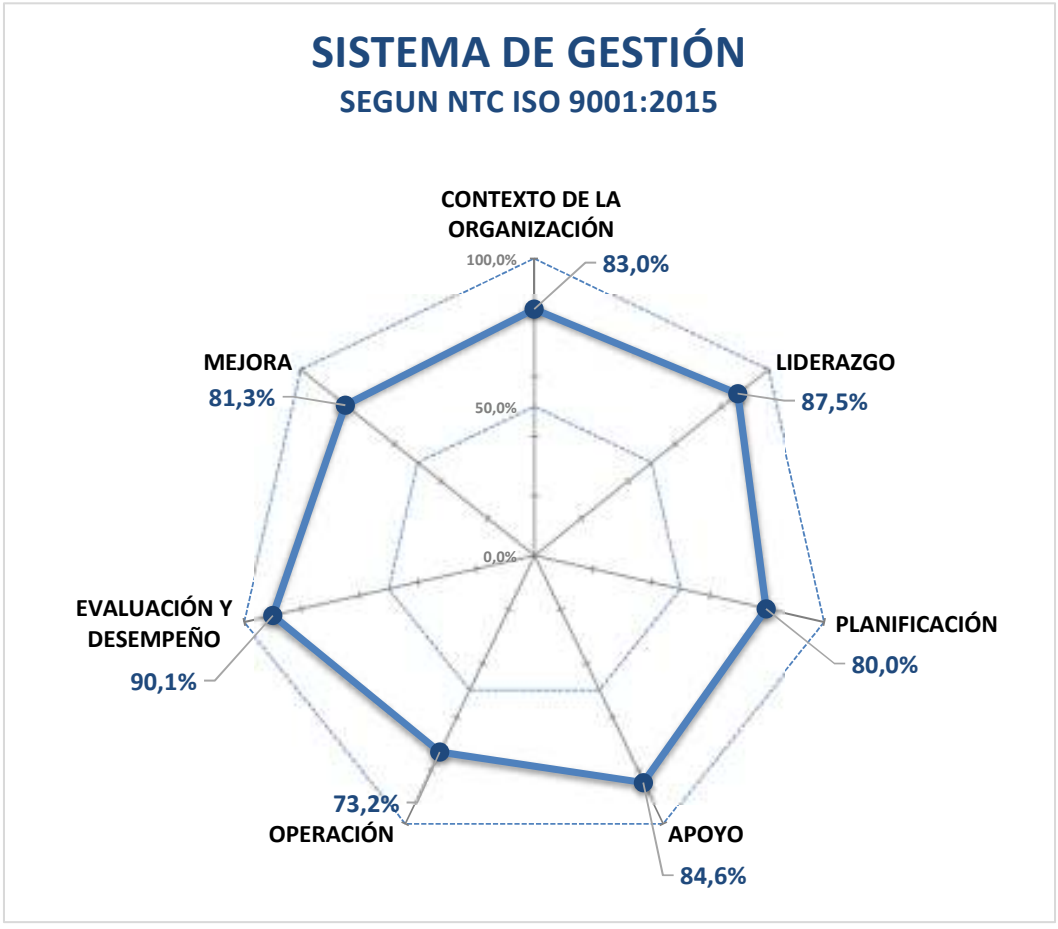
REQUISITOS	Avance Estimado	ACCIONES POR REALIZAR
CONTEXTO DE LA ORGANIZACIÓN	72,7%	MEJORAR
LIDERAZGO	66,0%	MEJORAR
PLANIFICACIÓN	77,5%	MEJORAR
APOYO	84,6%	MEJORAR
OPERACIÓN	73,3%	MEJORAR
EVALUACIÓN Y DESEMPEÑO	87,2%	MANTENER
MEJORA	76,6%	MEJORAR
TOTAL DEL SGI	76,8%	MEJORAR



ANEXO 2: Estimación de avance según criterios verificados y metodología descrita en Anexo 1

SISTEMA GESTIÓN BAJO MARCO 9001

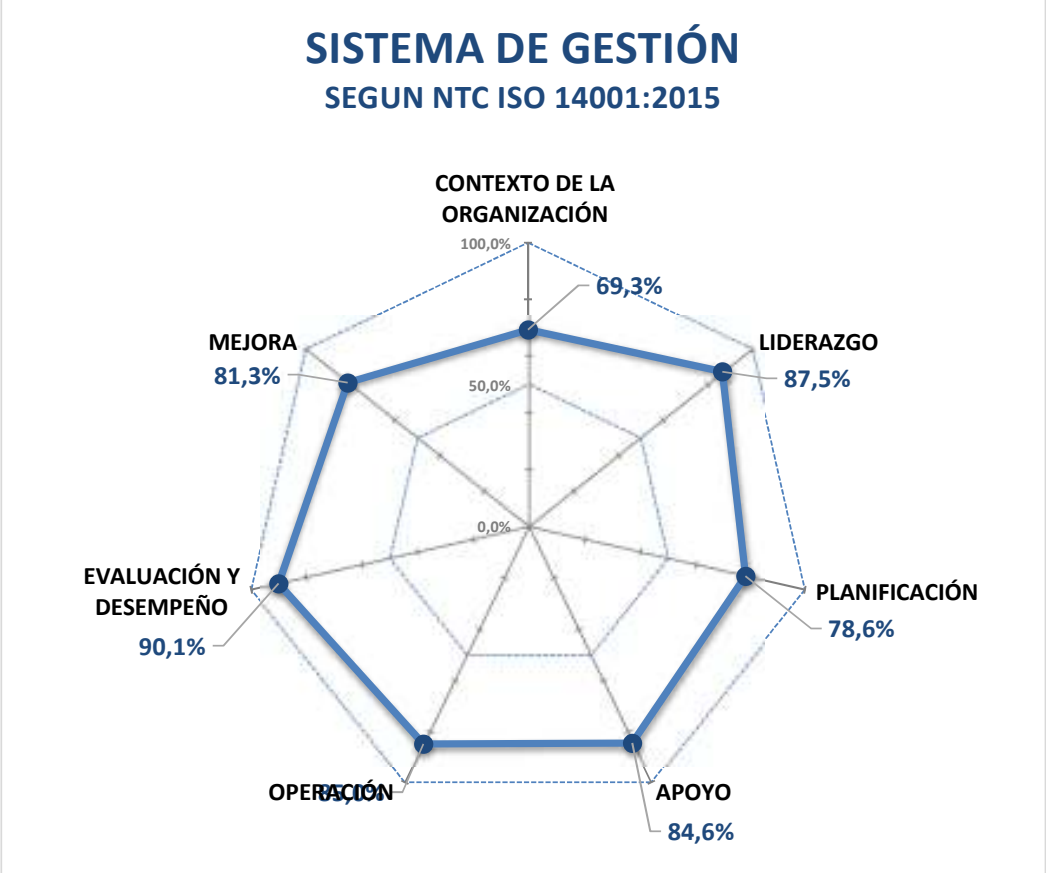
REQUISITOS	Avance Estimado	ACCIONES POR REALIZAR
CONTEXTO DE LA ORGANIZACIÓN	83,0%	MEJORAR
LIDERAZGO	87,5%	MANTENER
PLANIFICACIÓN	80,0%	MEJORAR
APOYO	84,6%	MEJORAR
OPERACIÓN	73,2%	MEJORAR
EVALUACIÓN Y DESEMPEÑO	90,1%	MANTENER
MEJORA	81,3%	MEJORAR
TOTAL DEL SGC	82,8%	MEJORAR



ANEXO 2: Estimación de avance según criterios verificados y metodología descrita en Anexo 1

SISTEMA GESTIÓN BAJO MARCO 14001

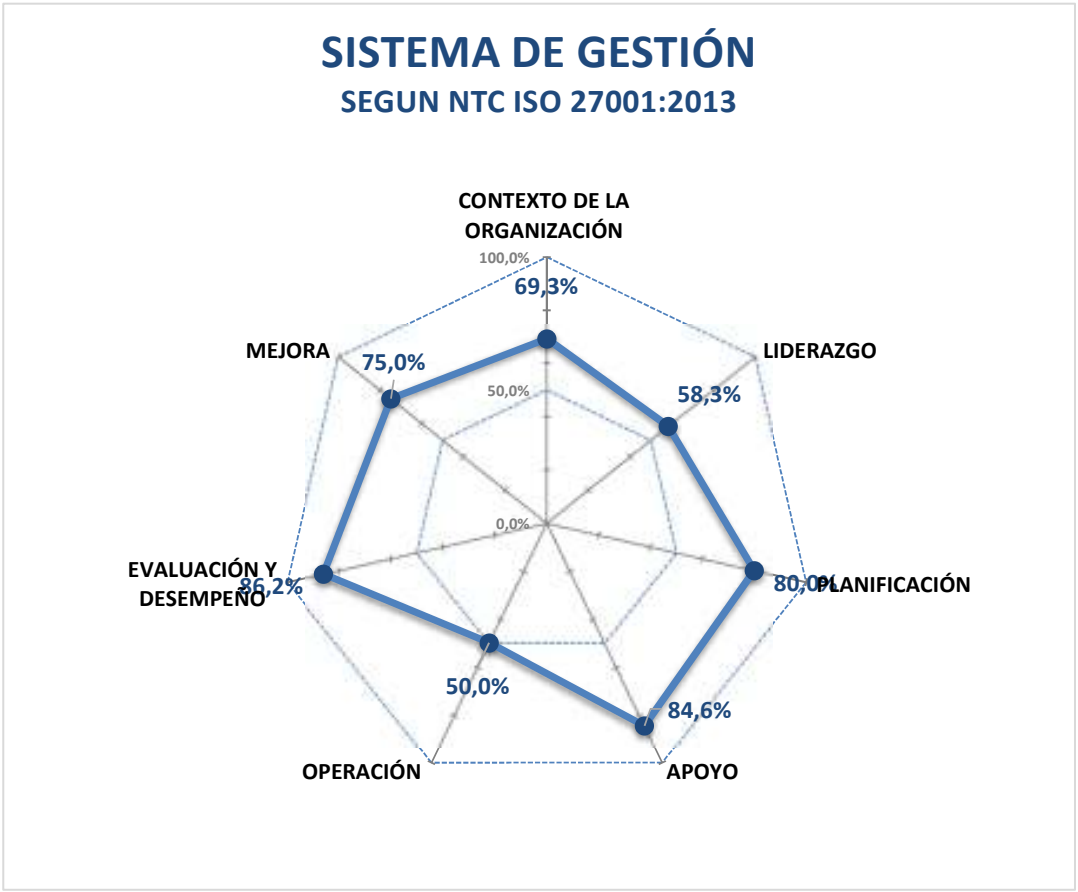
REQUISITOS	Avance Estimado	ACCIONES POR REALIZAR
CONTEXTO DE LA ORGANIZACIÓN	69,3%	MEJORAR
LIDERAZGO	87,5%	MANTENER
PLANIFICACIÓN	78,6%	MEJORAR
APOYO	84,6%	MEJORAR
OPERACIÓN	85,0%	MANTENER
EVALUACIÓN Y DESEMPEÑO	90,1%	MANTENER
MEJORA	81,3%	MEJORAR
TOTAL DEL SGA	82,3%	MEJORAR



ANEXO 2: Estimación de avance según criterios verificados y metodología descrita en Anexo 1

SISTEMA GESTIÓN BAJO MARCO 27001

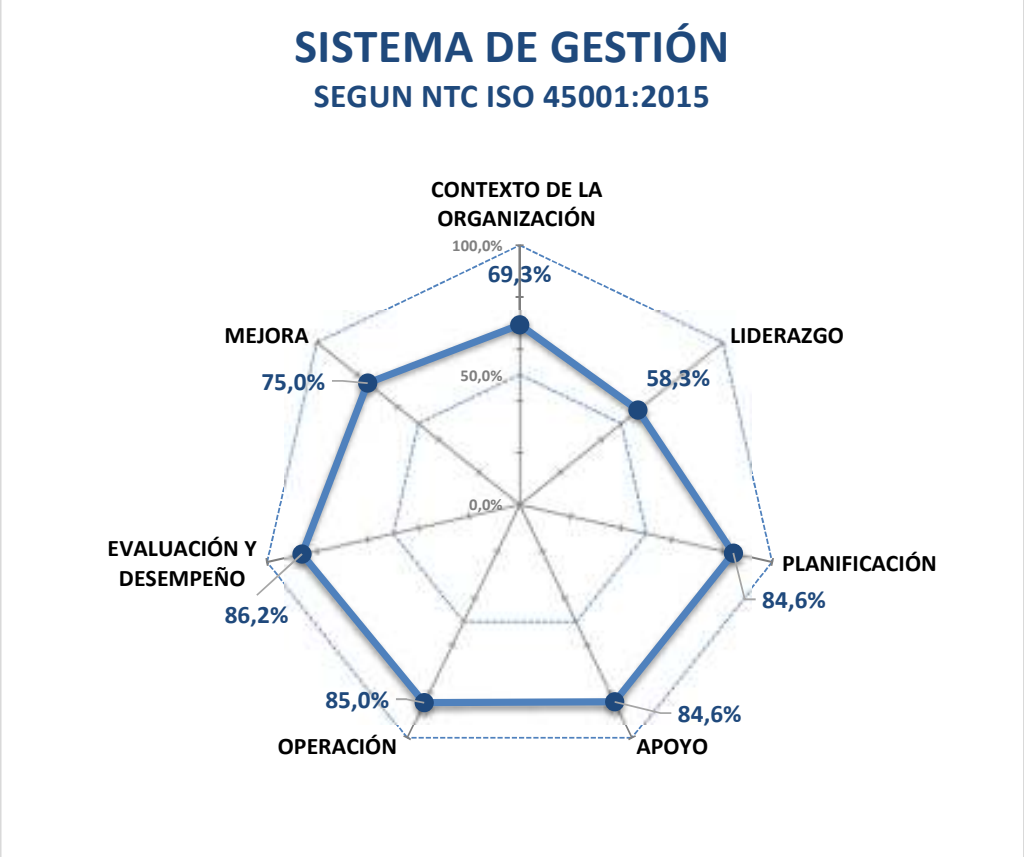
REQUISITOS	Avance Estimado	ACCIONES POR REALIZAR
CONTEXTO DE LA ORGANIZACIÓN	69,3%	MEJORAR
LIDERAZGO	58,3%	MEJORAR
PLANIFICACIÓN	80,0%	MEJORAR
APOYO	84,6%	MEJORAR
OPERACIÓN	50,0%	MEJORAR
EVALUACIÓN Y DESEMPEÑO	86,2%	MANTENER
MEJORA	75,0%	MEJORAR
TOTAL DEL SGSI	71,9%	MEJORAR



ANEXO 2: Estimación de avance según criterios verificados y metodología descrita en Anexo 1

SISTEMA GESTIÓN BAJO MARCO 45001

REQUISITOS	Avance Estimado	ACCIONES POR REALIZAR
CONTEXTO DE LA ORGANIZACIÓN	69,3%	MEJORAR
LIDERAZGO	58,3%	MEJORAR
PLANIFICACIÓN	84,6%	MEJORAR
APOYO	84,6%	MEJORAR
OPERACIÓN	85,0%	MANTENER
EVALUACIÓN Y DESEMPEÑO	86,2%	MANTENER
MEJORA	75,0%	MEJORAR
TOTAL DEL SGSST	77,6%	MEJORAR



ANEXO 3. CONCLUSIONES FRENTE AL NIVEL DE CUMPLIMIENTO DE LA DIRECTIVA 003 DE 2013

La Oficina de Control Interno dando cumplimiento al Plán Anual de Auditoria programó la auditoria al SIG de la Unidad de forma integral en concordancia con las Normas NTC ISO 9001:2015 Y NTC ISO 14001:2015. Por tal motivo y obrando bajo los principios celeridad, eficacia y economía integró como criterio de auditoria la Directiva 003 de 2013 específicamente en los numerales en cuanto a la perdida de documentos e incumplimiento de manuales de funciones y de procedimientos, para tal efecto se indago sobre las capacitaciones realizadas con esta temática la cual se establecieron las siguientes conclusiones:

- Frente a la perdida de Documentos la Directiva 003 de 2013 establece:

  Verificar la implementación y revisar el efectivo cumplimiento de las normas archivísticas y de conservación de documentos.: Se pudo determinar que cada proceso implementa de manera adecuada las TRD. No obstante, el proceso de Gestión Documental administra, custodia y ejerce la salvaguarda de la documentación que le es enviada por cada área o proceso.

  Incluir dentro de la estrategia de capacitación diseñada, esta temática. Según evidencia, se ha realizado sensibilización de instrumentos archivísticos en mayo y agosto de 2019. No obstante, se precisa que la sensibilización cuenta con el listado de asistencia, pero no hay información del contenido de la misma.

- Frente al cumplimiento del manual de Funciones y de procedimientos la Directiva 003 de 2013 establece:

  ** Verificar que en la estrategia de capacitación diseñada se haga énfasis en la aplicación rigurosa de los manuales de funciones y de procedimientos.* Se pudo determinar que no se han realizado capacitaciones de esta temática en la presente vigencia.

Por la anterior es importante que se pueda incluir en el Plan Institucional de Capacitaciones (PIC), con el fin de dar cumplimiento a la directiva 003 de 2015, capacitaciones con relación a la perdida de documentos, perdida de elementos y cumplimiento del manual de Funciones y de procedimientos de la Unidad.

Nota: Consolidación y análisis con base en papeles de trabajo (Listas de verificación) preparados, aplicados y validados por el equipo de Auditor.

---

9 de octubre de 2019

Realizó: Daniela Gordillo y Harold Puentes, Profesionales de OCI
Revisó: Andres Pabon S., Jefe Oficina de Control Interno

ANEXO 4: CONCLUSIONES FRENTE A LA GESTIÓN DE PQRSD

1. Se observa que la SAL atiende las Denuncias por actos de Corrupción desde el link http://www.uaesp.gov.co/content/transparencia-y-acceso-la-informacion-publica de la pagina web de la Unidad y el correo electrónico anticorrupción@uaesp.gov.co, que es administrado directamente por la SAL.

2. Se observa que desde la vigencia 2018 a la fecha se han presentado 4 denuncias por actos de corrupción de acuerdo con la verificación realizada a la SAL – Control Interno Disciplinario, que fueron autos inhibitorios por falta de fundamentos y por no hacer tránsito a cosa juzgada.

3. Se evidencia atención de PQRSD por medios presenciales en la Avenida caracas # 53-80, vía telefónica a línea 3580400 extensiones 1527, 1549, 1529, 1544 y 1567, formularios WEB, correos electrónicos uaesp@uaesp.gov.co y ventanilla.virtual@uaesp.gov.co, SDQS- Bogotá te escucha, Chat Virtual y la nueva APP Apporta.

4. Se observa que esta en proceso de modificación y aprobación el nuevo Manual de Atención al Ciudadano.

5. Se observa que el equipo de atención al ciudadano no esta utilizando el procedimiento GC-PCAC-FM-01 Peticiones, Quejas, reclamos y sugerencias, debido a que se esta aplicando el mismo formulario de forma virtual en la pagina web de la unidad, el formato GC-PCAC-FM-02 encuesta de satisfacción de la recepción de la prestación del servicio al ciudadano se sigue implementando por el equipo de atención al ciudadano.

6. El equipo de atención al ciudadano modificara el procedimiento y sus registros de acuerdo con los lineamientos que exige la circular 005 de 2019 de la subsecretaria de servicio a la ciudadanía de la secretaria general del distrito.

7. Se observa que existe un defensor al ciudadano a cargo de la SAF, designado mediante resolución 546 de 2018, de igual forma se observa el correo defensordelciudadano@uaesp.gov.co y la línea telefónica 3580400 extensión 1567 para atención al ciudadano con respecto a la defensoría del mismo.

8. Se observo que se recibieron 34 llamadas por la línea de la defensoría al ciudadano para el periodo de septiembre de 20'19, de las cuales 23 fueron contestadas, 1 fallida, 8 no contestadas y 2 en el momento de comunicarse se observaron ocupadas, no se presentó evidencias de las llamadas para los periodos de julio y agosto.

9. Se observo que de la muestra tomada (72 PQRSD) de un total 5.045 PQRSD de los periodos de junio, julio y agosto de 2019, se evidenció que para junio se dio respuesta a 17 PQRSD fuera de términos, para julio se dio respuesta 18 PQRSD fuera de términos y para agosto se dio respuesta a 9 PQRSD fuera de términos, para un total de 44 PQRSD con respuesta fuera de términos equivalentes al 61.11% del total de muestra. Así mismo se observa que se dio respuesta dentro de términos a 28 PQRSD del total de la muestra equivalentes al 38.88% del total.

Nota: Consolidación y análisis con base en papeles de trabajo (Listas de verificación) preparados, aplicados y validados por el equipo de Auditor.

9 de octubre de 2019

Realizó: Iván Sierra, Profesional OCI
Revisó: Andres Pabon S., Jefe Oficina de Control Interno

ANEXO 5: CONCLUSIONES FRENTE AL SIDEAP Y OTROS ASPECTOS

- Se solicito la TDR del proceso de Gestión de Talento Humano, la auxiliar auditada las indicó con destreza. Los tipos de documentos solicitados pertenecen a la Serie documental Expedientes laborales (Serie 37) la cual a su vez la conforma 110 tipos documentales y Actas (serie 02) y Programas (serie 72, asi:

	Serie	Subserie	Tipo D
Hojas de Vida	37	N/A	Hoja de vida
Bienes y rentas	37	N/A	Bienes y R
Evaluación M.O.	37	N/A	Examen de ingreso y r.
Permisos	37	N/A	Permisos
Actas Copasst	02	013	Actas Copasst
Actas del Comité SST	72	125	Actas comité SST

- Respecto con la verificación física de las actas del COPASST, Comité de SST y Comité de Convivencia. La auxiliar auditada y la Profesional del área informaron que estas las maneja y custodia el secretario de cada comité por lo tanto no se pudo evidenciar el soporte físico de las actas.

- Se seleccionaron 48 expedientes (14 correspondientes a profesionales especializados, 19 Profesionales Universitarios, 5 Técnicos, 3 secretarios, 5 Auxiliar Administrativo y 2 conductores; en los cuales se revisó uno a uno el último registro de bienes y rentas y hoja de vida, verificando los requisitos de suscrito, fechas y diligenciamiento. (Ver anexo 1 en 4 folios) Evidenciándose lo siguiente:

  - El 87,5% Cuarenta y dos (42) funcionarios Actualizaron y diligenciaron correctamente los formatos de Hojas de Vida y Bienes y Rentas. De estos 42 funcionarios 3 realizaron su actualización el 1 de agosto de 2019, un día después de la fecha establecida.

  - El 12,5% (6 funcionarios) no presentaron la actualización física de sus Hoja de vida ni Bienes y rentas. (Ver anexo 1)

  - Al realizar la verificación en la página del SIDEAP se verifico que 3 de los funcionarios que no habían allegado los formatos al área de talento humano, realizaron su actualización con posterioridad a la fecha establecida.

- Se observa que se firmó acta de compromiso de actualización permanente en la plataforma de SIDEAP, de novedades como cargos, vacantes, en el sistema y se encuentra al día. La actualización de contratistas la hace directamente legales.

- Se evidencia en los expedientes revisados que el jefe de la unidad de personal verificó el cumplimiento de la presentación de la declaración como de la actividad económica. (Todos los formatos de Hoja de Vida se encontraron firmados por la jefe de personal; en este caso Subdirectora Administrativa.)

De los cuarenta y ocho (48) expedientes revisados se evidencio que seis (6) funcionarios no allegaron los formatos al área de Talento Humano. La técnica auditada manifestó que se envió a todos los funcionarios que no allegaron los formatos, comunicación escrita solicitando informe por escrito si realizó la actualización de estos, para posteriormente revisar la posibilidad de enviar a Disciplinarios.

Nota: Consolidación y análisis con base en papeles de trabajo (Listas de verificación) preparados, aplicados y validados por el equipo de Auditor.

9 de octubre de 2019

Realizó: Martha Olaya, Técnico Operativo de OCI
Revisó: Andres Pabon S., Jefe Oficina de Control Interno

- Se evidencia en los expedientes revisados que el jefe de la unidad de personal verificó el cumplimiento de la presentación de la declaración como de la actividad económica. (Todos los formatos de Hoja de Vida se encontraron firmados por la jefe de personal; en este caso Subdirectora Administrativa.)

De los cuarenta y ocho (48) expedientes revisados se evidencio que seis (6) funcionarios no allegaron los formatos al área de Talento Humano. La técnica auditada manifestó que se envió a todos los funcionarios que no allegaron los formatos, comunicación escrita solicitando informe por escrito si realizó la actualización de estos, para posteriormente revisar la posibilidad de enviar a Disciplinarios.

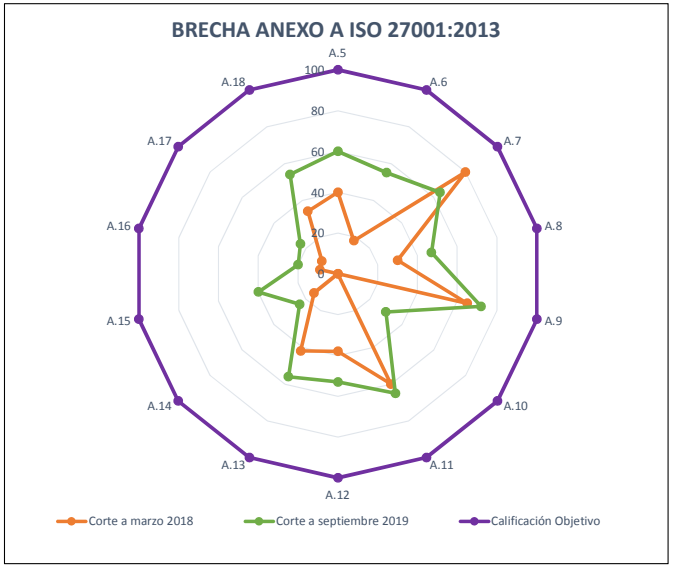
Nota: Consolidación y análisis con base en papeles de trabajo (Listas de verificación) preparados, aplicados y validados por el equipo de Auditor.

9 de octubre de 2019

Realizó: Martha Olaya, Técnico Operativo de OCI
Revisó: Andres Pabon S., Jefe Oficina de Control Interno

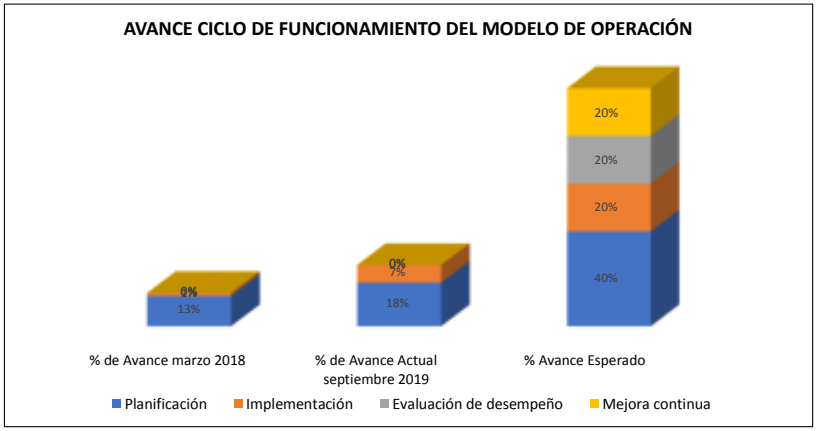
ANEXO 6: RESULTADOS DE VERIFICACIÓN DE CONTROLES SEGÚN METODOLOGIA MSPI

No.	Evaluación de Efectividad de controles				
	DOMINIO	Corte a marzo 2018	Corte a septiembre 2019	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	40	60	100	EFECTIVO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	18	55	100	EFECTIVO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	80	64	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	30	47	100	EFECTIVO
A.9	CONTROL DE ACCESO	65	72	100	GESTIONADO
A.10	CRIPTOGRAFÍA	0	30	100	REPETIBLE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	60	65	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	38	53	100	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	42	56	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	15	24	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	0	40	100	REPETIBLE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	9	20	100	INICIAL
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	10	24	100	REPETIBLE
A.18	CUMPLIMIENTO	34	54	100	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		***32***	**47**	**100**	EFECTIVO



AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

Año	AVANCE PHVA			
	COMPONENTE	% de Avance marzo 2018	% de Avance Actual septiembre 2019	% Avance Esperado
2015	Planificación	13%	18%	40%
2016	Implementación	1%	7%	20%
2017	Evaluación de desempeño	0%	0%	20%
2018	Mejora continua	0%	0%	20%
TOTAL		**14%**	**26%**	**100%**



Papel de Trabajo

Verificado: Javier Sarmiento, Profesional Oficina de Control Interno

										SEGUIMIENTO SEPTIEMBRE 2019		AUTODIAGNOSTICO MARZO 2018	
ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN													
AD.1	**Responsable de SI**	**POLITICAS DE SEGURIDAD DE LA INFORMACIÓN**	**Orientación de la dirección para gestión de la seguridad de la información**	**A.5**	**Componente planificación y modelo de madurez nivel gestionado**					60		40	
AD.1.1	Responsable de SI	Documento de la política de seguridad y privacidad de la información	Se debe definir un conjunto de políticas para la seguridad de la información aprobada por la dirección, publicada y comunicada a los empleados y a la partes externas pertinentes	A.5.1.1	Componente planificación y modelo de madurez inicial	ID.GV-1	Solicite la política de seguridad de la información de la entidad y evalúe: a) Si se definen los objetivos, alcance de la política b) Si esta se encuentra alineada con la estrategia y objetivos de la entidad c) Si fue debidamente aprobada y socializada al interior de la entidad por la alta dirección Revise si la política: a)Define que es seguridad de la información b) La asignación de las responsabilidades generales y específicas para la gestión de la seguridad de la información, a roles definidos; c) Los procesos para manejar las desviaciones y las excepciones. Indague sobre los responsables designados formalmente por la dirección para desarrollar, actualizar y revisar las políticas. Verifique cada cuanto o bajo que circunstancias se revisan y actualizan, verifique la ultima fecha de emisión de la política frente a la fecha actual y que cambios a sufrido, por lo menos debe haber una revisión anual. **Para la calificación tenga en cuenta que:**			60	Cuenta con los elementos señalados esta pendiente por aprobación mediante Resolución	40	Politicas de Seguridad de la Información Se crea el Comité de Seguridad de la Información y Gobierno Digital (Resolución 696 de 2017)
AD.1.2	Responsable de SI	Revisión y evaluación	Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.	A.5.1.2	componente planificación					60	Se debe establecer una periodicidad para la revisión y posibles actualizaciones de las políticas relacionadas con seguridad de la informacion.	40	
RESPONSABILIDADES Y ORGANIZACIÓN SEGURIDAD INFORMACIÓN													
A2	**Responsable de SI**	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	**Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización** **Garantizar la seguridad del teletrabajo y el uso de los dispositivos móviles**	**A.6**						55		18	
AD.2.1	**Responsable de SI**	**Organización Interna**	**Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización**	**A.6.1**	**Componente planificación y modelo de madurez gestionado**					60		36	
AD.2.1.1	Responsable de SI	Roles y responsabilidades para la seguridad de la información	Se deben definir y asignar todas las responsabilidades de la seguridad de la información	A.6.1.1	Componente planificación	ID.AM-6 ID.GV-2 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5 DE.DP-1 RS.CO-1	Para revisarlo frente a la NIST verifique si 1) los roles y responsabilidades frente a la ciberseguridad han sido establecidos 2) los roles y responsabilidades de seguridad de la información han sido coordinados y alineados con los roles internos y las terceras partes externas 3) Los a) proveedores, b) clientes, c) socios, d) funcionarios, e) usuarios privilegiados, f) directores y gerentes (mandos senior), g) personal de seguridad física, h) personal de seguridad de la información entienden sus roles y responsabilidades, i) Están claros los roles y responsabilidades para la detección de incidentes Solicite el acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o e que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección. Revise la estructura del SGSI: 1) Tiene el SGSI suficiente apoyo de la alta dirección?, esto se ve reflejado en comités donde se discutan temas como la política de SI, los riesgos o incidentes. 2) Están claramente definidos los roles y responsabilidades y asignados a personal con las competencias requeridas?, 3) Están identificadas los responsables y responsabilidades para la protección de los activos? (Una práctica común es nombrar un propietario para cada activo, quien entonces se convierte en el responsable de su protección) 4)Están definidas las responsabilidades para la gestión del riesgo de SI y la aceptación de los riesgos residuales? 5) Están definidos y documentados los niveles de autorización? 6) Se cuenta con un presupuesto formalmente asignado a las actividades del SGSI (por ejemplo campañas de sensibilización en seguridad de la información)			60	Mediante Acta de comité de seguridad de la información de 26/08/2019 se aprueba el rol de responsable de seguridad de la información de la entidad. Es importante definir las responsabilidades específicas de terceras partes y su relación con los activos de información EJ. Empresa de seguridad privada	20	De acuerdo a la Resolución 696 de 2017 se creo el comité de Seguridad y Gobierno Digital, el cual define las funciones y responsabilidades de cada integrante del comité. La Entidad ya cuenta con un profesional el cual es el responsable de seguridad de la información
AD.2.1.2	Responsable de SI	Separación de deberes / tareas	Los deberes y áreas de responsabilidad en conflicto se debe separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	A.6.1.2		PR.AC-4 PR.DS-5 RS.CO-3	Indague como evitan que una persona pueda acceder, modificar o usar activos sin autorización ni detección. La mejor práctica dicta que el inicio de un evento deber estar separado de su autorización. Al diseñar los controles se debería considerar la posibilidad de confabulación. Tenga en cuenta que para las organizaciones pequeñas la separación de deberes puede ser difícil de lograr, en estos casos se deben considerar controles compensatorios como revisión periódica de, los rastros de auditoría y la supervisión de cargos superiores.			60	Se evidencia la matriz de roles y responsabilidades sin embargo debe ser actualizada para dar alcance a la totalidad de sistemas de información que administra la UAESP.	60	
AD.2.1.3	Responsable de SI	Contacto con las autoridades.	Las organizaciones deben tener procedimientos establecidos que especifiquen cuándo y a través de que autoridades se debe contactar a las autoridades (por ejemplo, las encargadas de hacer cumplir la ley, los organismos de reglamentación y las autoridades de supervisión), y cómo se debe reportar de una manera oportuna los incidentes de seguridad de la información identificados (por ejemplo, si se sospecha una violación de la ley).	A.6.1.3		RS.CO-2	Solicite los procedimientos establecidos que especifiquen cuándo y a través de que autoridades se debería contactar a las autoridades, verifique si de acuerdo a estos procedimientos se han reportado eventos o incidentes de SI de forma consistente.			40	El manual de politicas de seguridad de la información contempla el rol al cual se deben reportar los incidentes de seguridad. Exisite un documento en costrucción "Gestión de incidentes de seguridad" Sin embargo este tiene un alcance enfocado en TI por lo cual se sugiere ampliarse.	0	No se tiene un procedimiento firmado por la alta direccion
AD.2.1.4	Responsable de SI	Contacto con grupos de interés especiales	Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad. Por ejemplo a través de una membresía	A.6.1.4		ID.RA-2	Pregunte sobre las membrecias en grupos o foros de interés especial en seguridad de la información en los que se encuentran inscritos las personas responsables de la SI.			100	Se evidencia que el responsable de seguridad de la información participa en foros y espacios relacionados con seguridad de la información, la participacion mas reciente fue	100	Colcert - Grupo de Respuestas a Emergencias Cibernetics de colombia

										SEGUIMIENTO SEPTIEMBRE 2019		AUTODIAGNOSTICO MARZO 2018	
ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
AD.2.1.5	Responsable de SI	Seguridad de la información en la gestión de proyectos	La seguridad de la información se debe integrar al(los) método(s) de gestión de proyectos de la organización, para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte de un proyecto. Esto se aplica generalmente a cualquier proyecto, independientemente de su naturaleza, por ejemplo, un proyecto para un proceso del negocio principal, TI, gestión de instalaciones y otros procesos de soporte.	A.6.1.5		PR.IP-2	Pregunte como la Entidad integra la seguridad de la información en el ciclo de vida de los proyectos para asegurar que para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proyecto. Tenga en cuenta que esto no solamente aplica para proyectos de TI, por ejemplo puede aplicar en proyectos de traslado de activos de información, gestión de instalaciones, personal en outsourcing que soporta procesos de la organización. Las mejores prácticas sugieren: a) Que los objetivos de la seguridad de la información se incluyan en los objetivos del proyecto; b) Que la valoración de los riesgos de seguridad de la información se lleve a cabo en una etapa temprana del proyecto, para identificar los controles necesarios; c) Que la seguridad de la información sea parte de todas las fases de la metodología del proyecto aplicada.			40	En el conjunto de documentos para inclusión en el MTO se observa un instructivo para gestión de proyectos el cual en el paso "Plan de gestion de Calidad" que trata la identificación de riesgos de seguridad y el monitoreo durane la ejecucion del proyecto.	0	Se tiene en cuenta pero aun no se han definido los riesgos del SGSI
AD.2.2	Responsable de SI	**Dispositivos Móviles y Teletrabajo**	**Garantizar la seguridad del teletrabajo y uso de dispositivos móviles**	**A.6.2**	**Modelo de Madurez Gestionado**					50		0	
AD.2.2.1	Responsable de SI	Política para dispositivos móviles	Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	A.6.2.1			Pregunte si la entidad asigna dispositivos móviles a sus funcionarios o permite que los dispositivos de estos ingresen a la entidad. Revise si existe una política y controles para su uso, que protejan la información almacenada o procesada en estos dispositivos y el acceso a servicios te TI desde los mismos. De acuerdo a las mejores prácticas esta política debe considerar, teniendo en cuenta el uso que se le dé al dispositivo, lo siguiente: a) el registro de los dispositivos móviles; b) los requisitos de la protección física; c) las restricciones para la instalación de software; d) los requisitos para las versiones de software de dispositivos móviles y para aplicar parches; e) la restricción de la conexión a servicios de información; f) los controles de acceso; g) técnicas criptográficas; h) protección contra software malicioso; i) des habilitación remota, borrado o cierre; j) copias de respaldo; k) uso de servicios y aplicaciones web. Cuando la política de dispositivos móviles permite el uso de			40	La UAESP asigna dispositivos móviles a determinados funcionarios dependiendo de sus funciones, se evidencian avances de un procedimiento para la gestión de dispositivos moviles. Sin embargo, aun no se encuenra en versión final para su control y aplicación.	0	
AD.2.2.2	Responsable de TICs	Teletrabajo	Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	A.6.2.2		PR.AC-3	Definición de teletrabajo: El teletrabajo hace referencia a todas las formas de trabajo por fuera de la oficina, incluidos los entornos de trabajo no tradicionales, a los que se denomina "trabajo a distancia", "lugar de trabajo flexible", "trabajo remoto" y ambientes de "trabajo virtual". Indague con la entidad si el personal o terceros pueden realizar actividades de teletrabajo, si la respuesta es positiva solicite la política que indica las condiciones y restricciones para el uso del teletrabajo. Las mejores prácticas consideran los siguientes controles: a) la seguridad física existente en el sitio del teletrabajo b) los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a la que se tendrá acceso y que pasará a través del enlace de comunicación y			60	Se observa el funcionamiento de herramienta desde la cual es posible hacer seguimiento a las sesiones remotas que desarrollan los funcionarios que tienen autorizada esta modalidad de trabajo.	0	Se realizaron pruebas piloto de teletrabajo, falta puesta en marcha, se adquirio el sistema Escritorios Virtuales para su operación.
SEGURIDAD DE LOS RECURSOS HUMANOS													
AD.3	**Responsable de SI/Gestión Humana/Líderes de los procesos**	**SEGURIDAD DE LOS RECURSOS HUMANOS**		**A.7**						64		80	
AD.3.1	**Responsable de SI**	**Antes de asumir el empleo**	**Asegurar que el personal y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que son considerados.**	**A.7.1**	**Modelo de Madurez Definido**					80		80	
AD.3.1.1	Gestión Humana	Selección e investigación de antecedentes	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	A.7.1.1		PR.DS-5 PR.IP-11	Revise el proceso de selección de los funcionarios y contratistas, verifique que se lleva a cabo una revisión de: a) Referencias satisfactorias b) Verificación de la de la hoja de vida del solicitante incluyendo certificaciones académicas y laborales; c) Confirmación de las calificaciones académicas y profesionales declaradas; d) Una verificación más detallada, como la de la información crediticia o de antecedentes penales. Cuando un individuo es contratado para un rol de seguridad de la información específico, las organizaciones deberían asegurar que el candidato tenga la competencia necesaria para desempeñar el rol de seguridad; e) sea confiable para desempeñar el rol, especialmente si es crítico para la organización. f) Cuando un trabajo, ya sea una asignación o una promoción, implique que la persona tenga acceso a las instalaciones de procesamiento de información, y en particular, si ahí se maneja información confidencial, por ejemplo, información financiera o información muy confidencial, la organización debería también considerar verificaciones adicionales más detalladas (por ejemplo estudio de seguridad, poligrafo, visita domiciliaria)			100	Hace parte del proceso de asuntos legales para garantizar que se cumplen con los requisitos para desarrollar las actividades objeto de la ontratación.	100	En el proceso Gestión de Asuntos Legales se encuentra la hoja de control, donde se verifica la documentación de los aspirantes. En el manual de funciones se describen las funciones para los funcionarios.

										SEGUIMIENTO SEPTIEMBRE 2019		AUTODIAGNOSTICO MARZO 2018	
ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
AD.3.1.2	Gestión Humana	Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas, deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	A.7.1.2		PR.DS-5				60	Actualmente se evidencia en proceso de aprobación para inclusion en el MTO un documento correspondiente a acuerdo de confidencialidad.	60	En contratistas: se especifica confidencialidad y el cumplimiento con administración de cuentas de sistema de información como condiciones referentes a seguridad de la información. Para provisionales y personal de carrera únicamente se tiene en cuenta la administración de cuentas de sistemas de información como requerimientos de seguridad de la información e
AD.3.2	**Responsable de SI/Líderes de los procesos**	**Durante la ejecución del empleo**	**Asegurar que los funcionarios y contratistas tomen consciencia de sus responsabilidades sobre la seguridad de la información y las cumplan.**	**A.7.1.2**	**Modelo de Madurez Definido**					53		60	
AD.3.2.1	Responsable de SI	Responsabilidades de la dirección	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	A.7.2.1		ID.GV-2	De acuerdo a la NIST los contratistas deben estar coordinados y alineados con los roles y responsabilidades de seguridad de la información. Indague y solicite evidencia del como la dirección se asegura de que los empleados y contratistas: a) Estén debidamente informados sobre sus roles y responsabilidades de seguridad de la información, antes de que se les otorgue el acceso a información o sistemas de información confidenciales. b) Se les suministren las directrices que establecen las expectativas de seguridad de la información de sus roles dentro de la Entidad. c) Logren un nivel de toma de conciencia sobre seguridad de la información pertinente a sus roles y responsabilidades dentro de			60	Se recomienda hacer enfasis en las responsabilidades de los Funcionarios y Contratistas en terminos de seguridad de la informacion, en los procesos de inducción y reinduccion.	60	Dentro de los contratos se encuentra una cláusula que determina la responsabilidad de la seguridad de la información. Así mismo en la entrega de los equipos se informa de los deberes que tienen durante su uso. Los servidores a través del canal de PQRS pueden enviar un queja para
AD.3.2.2	Responsable de SI/Líderes de los procesos	Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados de la Entidad, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	A.7.2.2	Componente planeación Modelo de Madurez Inicial	PR.AT-1 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5	Entreviste a los lideres de los procesos y pregúnteles que saben sobre la seguridad de la información, cuales son sus responsabilidades y como aplican la seguridad de la información en su diario trabajo. Pregunte como se asegura que los funcionarios, Directores, Gerentes y contratistas tomen conciencia en seguridad de la información, alineado con las responsabilidades, políticas y procedimientos existentes en la Entidad. Solicite el documento con el plan de comunicación, sensibilización y capacitación, con los respectivos soportes, revisado y aprobado por la alta Dirección. Verifique que se han tenido en cuenta buenas prácticas como: a) Desarrollar campañas, elaborar folletos y boletines. b) Los planes de toma de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, están aprobados y documentados, por la alta Dirección c) Verifique que nuevos empleados y contratistas son objeto de			60	Se evidencia la ejecución de procesos de sensibilización en la Entidad a Funcionarios y Contratistas acerca de sus responsabilidades en cuanto a seguridad de la información . Sin embargo, no es clara la forma de determinar si los funcionarios y contratistas realmente toman conciencia e interiorizan la información acerca de sus responsabilidades en cuanto al SGSI	20	Se han enviado correos institucionales con informacion sobre seguridad.
AD.3.2.3	Responsable de SI	Proceso disciplinario	Se debe contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	A.7.2.3			Pregunte cual es el proceso disciplinario que se sigue cuando se verifica que ha ocurrido una violación a la seguridad de la información, quien y como se determina la sanción al infractor?	Documento construido de incidentes de seguridad.		40	Hay una proyeccion de gestión de incidentes de seguridad pero no está terminado. Se recomienda que la versión final se articule con el procedimiento disciplinario vigente en la UAESP.	100	Existe un procedimiento disciplinario general, el cual contiene los pasos a seguir cuando se comete una falta.
AD.3.3	**Responsable de SI**	**Terminación y cambio de empleo**	**Proteger los intereses de la Entidad como parte del proceso de cambio o terminación de empleo.**	**A.7.3**	**Modelo de Madurez Definido**					60		100	
AD.5.1.3	Responsable de SI	Terminación o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.	A.7.3.1		PR.DS-5 PR.IP-11	Revisar los acuerdos de confidencialidad, verificando que deben acordar que después de terminada la relación laboral o contrato seguirán vigentes por un periodo de tiempo.	Acuerdo de confidencialidad		60	En acta adjunta se aprobó la implementacion de la nueva version del acuerdo de confidencialidad, Sin embargo, aun no esta integrado al MTO de la UAESP, alli se especifica el tiempo por el cual estara vigente l acuerdo de confidencialidad despues de terminada la relación contractual.	100	Minutas de los contratos publicados en el SECOP II
GESTIÓN DE ACTIVOS													
AD.4	**Responsable de SI**	**GESTIÓN DE ACTIVOS**		**A.8**						47		30	
AD.4.1	**Responsable de SI**	**Responsabilidad de los activos**	**Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.**	**A.8.1**	**Modelo de Madurez Gestionado**					60		65	
AD.4.1.1	Responsable de SI	Inventario de activos	Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	A.8.1.1	Componente Planificación Modelo de madurez inicial	ID AM-1 ID AM-2 ID.AM-5	Solicite el inventario de activos de información, revisado y aprobado por la alta Dirección y revise: 1) Ultima vez que se actualizó 2) Que señale bajo algún criterio la importancia del activo 3) Que señale el propietario del activo Indague quien(es) el(los) encargado(s) de actualizar y revisar el inventario de activos y cada cuanto se realiza esta revisión. De acuerdo a NIST se deben considerar como activos el personal, dispositivos, sistemas e instalaciones físicas que permiten a la entidad cumplir con su misión y objetivos, dada su importancia y riesgos estratégicos. Tenga en cuenta para la calificación:			60	Se evidencia que el documento se encuentra en ajuste ya que el vigente no da alcance a la clasificación de activos desde la parte técnica de TI y no permitia la valoración del riesgo asociado al activo.	40	

										SEGUIMIENTO SEPTIEMBRE 2019		AUTODIAGNOSTICO MARZO 2018	
ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
AD.4.1.2	Responsable de SI	Propiedad de los activos	Los activos mantenidos en el inventario deben tener un propietario.	A.8.1.2		ID AM-1 ID AM-2	Solicite el procedimiento para asegurar la asignación oportuna de la propiedad de los activos. Tenga en cuenta que la propiedad se debería asignar cuando los activos se crean o cuando son entregados a la Entidad. De acuerdo a las mejores prácticas el propietario de los activos (individuo o entidad, que es responsable por el activo) tiene las siguientes responsabilidades: a) asegurarse de que los activos están inventariados; b) asegurarse de que los activos están clasificados y protegidos apropiadamente; c) definir y revisar periódicamente las restricciones y clasificaciones de acceso a activos importantes, teniendo en cuenta las políticas de control de acceso aplicables; d) asegurarse del manejo apropiado del activo cuando es eliminado o destruido.	Procedimiento de activos de información.		60	Se evidencia una versión actualizadas del procedimiento de activos de información que esta pendiente por se aprobada para su inclusión en el MTO. Sin embargo, no es posible determinar que la totalidad de activos estan relacionado y cuenta con asignacion de propietariio hasta tanto no se concluya la actividad de ajuste del inventario de activos de informacion	100	
AD.4.1.3	Responsable de SI	Uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	A.8.1.3			Pregunte por la política, procedimiento, directriz o lineamiento que defina el uso aceptable de los activos, verifique que es conocida por los empleados y usuarios de partes externas que usan activos de la Entidad o tienen acceso a ellos.	Procedimiento de activos de información.		20	Se evidencia la construcción de un borrador de Politica de uUso Aceptable de activos informáticos de la UAESP. Se recomienda completar el documento para proceder a la aceptación y publicación correspondiente.	20	Para garantizar el uso adecuado de los activos de información se tienen controles como Directorio Activo, Kaspersky, entre otros.
AD.4.1.4	Responsable de SI	Devolución de activos	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	A.8.1.4		PR.IP-11	Revisar las políticas , normas , procedimientos y directrices relativas a los controles de seguridad de la información durante la terminación de la relación laboral por ejemplo, la devolución de los activos de información (equipos, llaves, documentos , datos, sistemas) , las llaves físicas y de cifrado, la eliminación de los derechos de acceso, etc. En caso de que un funcionario o tercero sea el dueño del activo indague como se asegura la transferencia de la información a la Entidad y el borrado seguro de la información de la Entidad. 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. Durante el período de notificación de la terminación, la Entidad debería controlar el copiado no autorizado de la información pertinente (por ejemplo, la propiedad intelectual) por parte de los empleados o contratistas que han finalizado el empleo.	Procedimiento de paz y salvo V1 Gestion humana		100	Existen controles de TI asociados a la devolucion de activos asignados. Se evidencia el funcionamiento de un flujo de procesos mediante la herramienta Runmyprocess para la generación de Paz y salvos.	100	Se tiene el formato Paz y salvo por retiro lo cual permite tener control de que el usuario entregue todo su inventario a las areas que corresponda. Se bloquea el usuario para que no tenga acceso a ningún activo de información.
AD.4.2	**Responsable de SI**	**Clasificación de información**	**Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la Entidad.**	**A.8.2**						**60**		**13**	
AD.4.2.1	Responsable de SI	Clasificación de la información	La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	A.8.2.1	Modelo de Madurez Inicial		Solicite el procedimiento mediante el cual se clasifican los activos de información y evalué: 1) Que las convenciones y criterios de clasificación sean claros y estén documentados 2) Que se defina cada cuanto debe revisarse la clasificación de un activo 3) La clasificación debería valorarse analizando la confidencialidad, integridad y disponibilidad. Solicite muestras de inventarios de activos de información clasificados y evalué que se aplican las políticas y procedimientos de clasificación definidos. Evalué si los procesos seleccionados aplican de manera consistente estas políticas y procedimientos.	Procedimiento de activos de información		60	El ajuste del inventario de activos de información incluye la clasificación de analisis por cada uno de los pilares de la información. Sin embargo, aun esta pendiente por incluir la totalidad de activos.	0	
AD.4.2.2	Responsable de SI	Etiquetado de la información		A.8.2.2		PR.DS-5 PR.PT-2	Solicite el procedimiento para el etiquetado de la información y evalúe: 1) Aplica a activos en formatos físicos y electrónicos (etiquetas físicas, metadatos) 2) Que refleje el esquema de clasificación establecido 3) Que las etiquetas se puedan reconocer fácilmente 4) Que los empleados y contratistas conocen el procedimiento de etiquetado Revise en una muestra de activos el correcto etiquetado			n/a	No se adelanta dado que es responsabilidad de Gestión documental decreto 1080 de 2015 Acuerdo 006 de 2014 modificando la ley general de archivo. Pendiente de verificación	40	
AD.4.2.3	Responsable de SI	Manejo de activos		A.8.2.3		PR.DS-1 PR.DS-2 PR.DS-3 PR.DS-5 PR.IP-6 PR.PT-2	Solicite los procedimientos para el manejo, procesamiento, almacenamiento y comunicación de información de conformidad con su clasificación. De acuerdo a las mejores prácticas evidencie si se han considerado los siguientes asuntos: a) Restricciones de acceso que soportan los requisitos de protección para cada nivel de clasificación; b) Registro formal de los receptores autorizados de los activos; c) Protección de copias de información temporal o permanente a un nivel coherente con la protección de la información original;			60	En revisión se evidencia documentos que en conjunto pueden dar al cance a este control, procedimiento de backup en equipos de computo, procedimiento de cifrado, y procedimiento de dispositivos moviles. Se observa que (1) esta vigente, (1) pendiente por aprobación y (1) en construcción, por lo cual se recomienda adelantar las acciones pertinentes	0	
AD.4.3	**Responsable de TICs**	**Manejo de medios**	**Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de la información almacenada en los medios.**	**A.8.3**						**20**		**13**	
AD.4.3.1	Responsable de TICs	Gestión de medios removibles		A.8.3.1		PR.DS-3 PR.IP-6 PR.PT-2	Solicite las directrices, guias, lineamientos y procedimientos para la gestión de medios removibles, que consideren: a) Si ya no se requiere, el contenido de cualquier medio reusable que se vaya a retirar de la organización se debe remover de forma que no sea recuperable; b) cuando resulte necesario y práctico, se debe solicitar autorización para retirar los medios de la organización, y se debe llevar un registro de dichos retiros con el fin de mantener un rastro de auditoría;			20	Se recomienda completar los documentos "procedimiento de borrado seguro", establecer y/o ajustar procedimiento para retiro de medios de la organización, en conjunto con el procedimiento para cifrado.	0	

										SEGUIMIENTO SEPTIEMBRE 2019		AUTODIAGNOSTICO MARZO 2018	
ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
AD.4.3.2	Responsable de TICs	Disposición de los medios		A.8.3.2		PR.DS-3 PR.IP-6	Solicite los procedimientos existentes para garantizar que los medios a deschar o donar, no contienen información confidencial que pueda ser consultada y copiada por personas no autorizadas. Verifique si se ha realizado esta actividad y si existen registros de la misma.	procedimiento de boorado seguro		20	Se evidencia procedimiento de borrado seguro en proceso de construcción	20	Cuando se hace entrega y devolución de equipos se realiza limpieza total del disco duro.
AD.4.3.3	Responsable de TICs	Transferencia de medios físicos		A.8.3.3		PR.DS-3 PR.PT-2	Solicite las directrices definidas para la protección de medios que contienen información durante el transporte. Verifique de acuerdo a las mejores prácticas que se contemple: a) El uso de un transporte o servicios de mensajería confiables. b) Procedimientos para verificar la identificación de los servicios de mensajería. c) Indague y evidencie como es el embalaje el cual debe proteger el contenido contra cualquier daño físico que pudiera presentarse durante el tránsito, y de acuerdo con las especificaciones de los fabricantes, por ejemplo, protección contra cualquier factor ambiental que pueda reducir la eficacia de la restauración del medio, tal como exposición al calor, humedad o campos electromagnéticos; d) Solicite los registros que dejen evidencia del transporte donde se identifique el contenido de los medios, la protección aplicada, al igual que los tiempos de transferencia a los responsables durante el transporte, y el recibo en su destino.	analisis de riesgo de equipos que no se encuentran en la sede principal de la entidad		20	Se evidencia que el analisis de riesgo de equipos que no se encuentran en la sede principal de la entidad, no se ha concluido. No se evidencia implementación de un procedimiento para control de información compartida por medios fisicos.	20	No se ha implementado un proceso o control para asegurar la información que se comparte o transfiere mediante medios físicos. Para documentos se tiene implementado el sistema de información de gestión documental Orfeo el cual permite llevar trazabilidad y control de los documentos. Se dispone de vehiculos contratados por la UAESP para el translado de inmuebles o equipos de computo lo cual se realiza con un sistema de embalaje
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO													
AD.5	**Responsable de la Continuidad**	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**		**A.17**						**23,5**		**10**	
AD.5.1	**Responsable de la Continuidad**	**Continuidad de la seguridad de la información**	**La continuidad de la seguridad de la información debe incluir en los sistemas de gestión de la continuidad del negocio de la Entidad.**	**A.17.1**						**7**		**0**	
AD.5.1.1	Responsable de la Continuidad	Planificación de la continuidad de la seguridad de la información		A.17.1.1	Modelo de Madurez Gestionado	ID.BE-5 PR.IP-9	Indagar si la Entidad cuenta con un BCP (Bussines Continuity Plan) o DRP (Disaster Recovery Plan). Determine si aplica para procesos criticos solamente o se han incluido otros procesos o por lo menos se ha reconocido la necesidad de ampliarlo a otros procesos (para determinar el nivel de madurez) Evalúe si se ha incluido en estos planes y procedimientos los requisitos de seguridad de la informacion. Tenga en cuenta que en ausencia de una planificación formal de continuidad de negocio y recuperación de desastres, la dirección de seguridad de la información debería suponer que los requisitos de seguridad de la información siguen siendo los mismos en situaciones adversas, en comparación con las condiciones	para continuidad de negocio y BIA		20	Estan planteados documentos para continuidad de negocio y BIA. Aun no estan incluidos en el MTO. Se han evidenciado situaciones de emergencia de las cuales no se ha definido un conducto para sumanejo contigente (servicios de impresión, licenciamiento de correos corporativos, licencimiento herramienta antivirus , firewall)	0	no existe
AD.5.1.2	Responsable de la Continuidad	Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa,	A.17.1.2	Modelo de Madurez Definido	ID.BE-5 PR.IP-4 PR.IP-9 PR.IP-9	Verifique si la Entidad cuenta con a) Una estructura organizacional adecuada para prepararse, mitigar y responder a un evento contingente, usando personal con la autoridad, experiencia y competencia necesarias. b) Personal formalmente asignado de respuesta a incidentes con la responsabilidad, autoridad y competencia necesarias para manejar un incidente y mantener la seguridad de la información. c) Planes aprobados, procedimientos de respuesta y recuperación documentados, en los que se especifique en detalle como la organización gestionará un evento contingente y mantendrá su seguridad de la información en un límite predeterminado, con base en los objetivos de continuidad de seguridad de la			0	No se evidencia el establecimiento, ni aprobación de plan de contingencia SGSI.	0	no existe
AD.5.1.3	Responsable de la Continuidad	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.		A.17.1.3	Modelo de Madurez Optimizado	PR.IP-4 PR.IP-10	Indague y solicite evidencias de la realización de pruebas de la funcionalidad de los procesos, procedimientos y controles de continuidad de la seguridad de la información, para asegurar que son coherentes con los objetivos de continuidad de la seguridad de la información; Tenga en cuenta que la verificación de los controles de continuidad de la seguridad de la información es diferente de las pruebas y verificación generales de seguridad de la información. Si			0	No se han realizado pues el plan no se ha implementado. En conjuno con planeacion para la gestion del documento BIA.	0	no existe
AD.5.2	**Responsable de la Continuidad**	**Redundancias**	**Asegurar la disponibilidad de las instalaciones de procesamiento de la información.**	**A.17.2**						**40**		**20**	
AD.5.2.1	Responsable de la Continuidad	Disponibilidad de instalaciones de procesamiento de información		A.17.2.1		ID.BE-5	Verifique si la Entidad cuenta con arquitecturas redundantes, ya sea un centro de cómputo principal y otro alterno o componentes redundantes en el único centro de cómputo. Indague como se han definido las necesidades de los procesos para seleccionar que elementos deben ser redundantes. Solicite si aplica las pruebas aplicadas para asegurar que un componente redundante funciona de la forma prevista durante una emergencia o falla.			40	Se evidencia que algunos sistemas gestionados por la OTIC cuentan con elementos redundantes sin embargo, actualmente, no se encuentra dispuestos, organizados o documentados de forma tal que pueda considerarse como parte de una arquitectura.	20	
CUMPLIMIENTO													
AD.6	**Responsable de SI/Responsable de TICs/Control Interno**	**CUMPLIMIENTO**		**A.18**						**54**		**34**	
AD.6.1	**Responsable de SI**	**Cumplimiento de requisitos legales y contractuales**	**Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.**	**A.18.1**		**ID.GV-3**	**De acuerdo a la NIST: Los requerimientos legales y regulatorios respecto de la ciberseguridad, incluyendo la privacidad y las libertades y obligaciones civiles, son entendidos y gestionados.**			**75**		**55**	
AD.6.1.1	Responsable de SI	Identificación de la legislación aplicable y de los requisitos contractuales.		A.18.1.1	**Modelo de Madurez Gestionado Cuantitativamente**		Solicite la relación de requisitos legales, reglamentarios, estatutarios, que le aplican a la Entidad (Normograma). Indague si existe un responsable de identificarlos y se definen los responsables para su cumplimiento.			100	Se evidencia que exste una identificacion de normas aplicables y la definicion de responsables para su cumplimiento.	100	

Papel de Trabajo

Verificado: Javier Sarmiento, Profesional Oficina de Control Interno

										SEGUIMIENTO SEPTIEMBRE 2019		AUTODIAGNOSTICO MARZO 2018	
ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
AD.6.1.2	Responsable de TICs	Derechos de propiedad intelectual.		A.18.1.2			1) Solicite los procedimientos para el cumplimiento de los requisitos y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados. 2) Verifique si la Entidad cuenta con una política publicada sobre el cumplimiento de derechos de propiedad intelectual que defina el uso legal del software y de productos informáticos. Esta política debe estar orientada no solo al software, si no también a documentos gráficos, libros, etc. 3) Indague como se controla que no se instale software ilegal. 4) Indague si se tiene un inventario de software instalado y se compara con el número de licencias adquiridas para asegurar que no se incumplen los derechos de propiedad intelectual. Tenga en			60	Se evidencia que el manual de políticas de seguridad informatica(versión no oficial) incluye un aparatado referente a propiedad intelectual y propiedad itelectual de software. Sn embargo, se sugiere complementar con los escenarios posibles.	20	
AD.6.1.3	Responsable de SI	Protección de registros.	Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales	A.18.1.3		PR.IP-4	Revise si la Entidad cuenta con tablas de retención documental que especifiquen los registros y el periodo por el cual se deberían retener, además del almacenamiento, manejo y destrucción. Posibles tipos de registros pueden ser registros contables, registros de bases de datos, logs de transacciones, logs de auditoria y procedimientos operacionales, los medios de almacenamiento permitidos pueden ser papel, microfichas, medios magnéticos, medios ópticos etc.			80	Se evidencia el establecimento de TRD que deben ser actualizadas (listado maestro de documentos desactualizados)	60	El Sistema de Gestión Documental Orfeo brinda la posibilidad de almacenar y salvaguardar los registros. Tambien cuenta con la tablas de retención documental actualizadas.
AD.6.1.4	Responsable de SI	Protección de los datos y privacidad de la información relacionada con los datos personales.	Se deben asegurar la protección y privacidad de la información personal tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales.	A.18.1.4		DE.DP-2	Indague sobre las disposiciones que ha definido la Entidad para cumplir con la legislación de privacidad de los datos personales, ley estatutaria 1581 de 2012 y decreto 1377 que reglamenta la ley de 2013. 1) Revise si existe una politica para cumplir con la ley 2) Si están definidos los responsables 3) Si se tienen identificados los repositorios de datos personales 4) Si se ha solicitado consentimiento al titular para tratar los datos personales y se guarda registro de este hecho. 5) Si se adoptan las medidas técnicas necesarias para proteger las bases de datos donde reposan estos datos.			60	9.1Se evidencia mediante correo del 25 de Julio de 2019, reporte de incidente de seguridad reportado por un contratista de la UAESP referente a la exposición de datos sus personales en la plataforma SECOP. GTI consulta a la SAL para que emita el concepto acerca de la procedencia de supresión u ocultación de la información. La SAL argumenta que en el documento de la propuesta de prestación de servicio se firma la autorización para el tratamiento y publicación de la información relacionada con el contrato. Se sugiere revisar en detalle el caso a la luz de la ley 1581 de 2012 – tratamiento de datos clasificados como sensibles y la ley 1712 de 2014 ley de transparencia la cual especifica la siguiente información de obligatoria publicación para funcionarios y contratistas: a. Nombres y apellidos completos. b. País, Departamento y Ciudad de nacimiento. c. Formación académica. d. Experiencia laboral y profesional. e. Empleo, cargo o actividad que desempeña (En caso de contratistas el rol que desempeña con base en el objeto contractual). f. Dependencia en la que presta sus servicios en la entidad o institución.	40	No se ha definido un mecanismo para realizar este tipo de protección, se tienen cubiertos parcialmente algunos activos tales como los expedientes de trabajo del personal custodiado por talento Humano.
AD.6.1.5	n/a	Reglamentación de controles criptográficos.		A.18.1.5			n/a			n/a		0	
AD.6.2	**Control interno**	**Revisiones de seguridad de la información**		**A.18.2**	**Modelo de Madurez Gestionado Cuantitativamente**					**33**		**13**	
AD.6.2.1	Control interno	Revisión independiente de la seguridad de la información		A.18.2.1			Investigue la forma como se realizan revisiones independientes (por personas diferentes o no vinculadas a un proceso o área que se revisa), de la conveniencia, la adecuación y la eficacia continuas de la gestionar la seguridad de la información. Para esto solicite: 1) El plan de auditorías del año 2015 2) El resultado de las auditorías del año 2015 3) Las oportunidades de mejora o cambios en la seguridad de la información identificados.			40	La OCI realiza auditorias deacuerdo al plan anual de auditorias.	0	
AD.6.2.2	Control interno	Cumplimiento con las políticas y normas de seguridad.	Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.	A.18.2.2		PR.IP-12	1) Verifique si los gerentes aseguran que todos los procedimientos de seguridad dentro de su área de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento de las políticas y estándares de seguridad. 2) Verifique la revisión periódica del cumplimiento del centro de cómputo con las políticas y normas de seguridad establecidas. 3) Verifique si los sistemas de información son revisados regularmente para asegurar el cumplimiento de las normas de seguridad de la información			20	No se evidencian soportes que permitan establecer que los jefes - subdirectores y dirección ejecutan los procedimientos de seguridad establecidos.	20	Existen los procedimientos enfocados a la seguridad de la información, pero no se lleva el control si los jefes de cada area realizan el seguimiento respecto a este tema.
AD.6.2.3	Responsable de SI	Revisión de cumplimiento técnico.	Los sistemas de información deben chequearse regularmente para el cumplimiento con los estándares de implementación de la seguridad.	A.18.2.3		ID.RA-1	Verifique si se realizan evaluaciones de seguridad técnicas por o bajo la supervisión de personal autorizado, apoyado en herramientas automáticas o con revisiones manuales realizadas por especialistas. Solicite evidencia de las últimas pruebas realizadas, sus resultados y seguimiento para asegurar que las brechas de seguridad fueron solucionadas.			40	Se evidencia la ejecución de actividades relacionas con pruebas automatizadas no documentadas.	20	Se adelantan analisis de vulnerabilidades dentro de la unidad.
RELACIONES CON LOS PROVEEDORES													
AD.7	**Responsable de compras y adquisiciones**	**RELACIONES CON LOS PROVEEDORES**		**A.15**						**40**		**0**	

										SEGUIMIENTO SEPTIEMBRE 2019		AUTODIAGNOSTICO MARZO 2018	
ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
AD.7.1	Responsable de compras y adquisiciones	Seguridad de la información en las relaciones con los proveedores	Asegurar la protección de los activos de la entidad que sean accesibles para los proveedores	A.15.1	Modelo de Madurez Definido		1) Solicite la política de seguridad de la información para las relaciones con los proveedores, que indique los requisitos de SI para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización, esta política debe reflejarse en los acuerdos con los proveedores que deben estar documentados. 2) Verifique en la muestra de proveedores con acceso a los activos de información (no necesariamente son proveedores de tecnología de la información, por ejemplo pueden ser proveedores que tengan por ejemplo un proceso de nomina en outsourcing), se hayan suscrito acuerdos (ANS) formales donde se establezcan y acuerden todos los requisitos de seguridad de la información pertinentes con cada proveedor. 3) Verifique para los proveedores si se tiene en cuenta los riesgos de SI asociados a la cadena de suministro, por ejemplo para los proveedores en la nube es muy común que se apoyen en otros proveedores para proporcionar las instalaciones y se deben manejar los riesgos asociados a este tercero con el cual la entidad no tiene una relación comercial directa. Solicite que le indiquen como identifican para cada proveedor su cadena de suministro y obtenga evidencia de este hecho.			40	Se evidencia que la política de seguridad de la información (no oficial) contiene un objetivo específico en relación con el cumplimiento de manejo de datos personales para proveedores	0	
AD.7.2	Responsable de compras y adquisiciones	Gestión de la prestación de servicios de proveedores	Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores	A.15.2	Modelo de Madurez Definido		1) Indague y solicite evidencia en una muestra de proveedores seleccionada, como la entidad hace seguimiento, revisa y audita con regularidad de acuerdo a 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. 2)			40	Se evidencia que la política de seguridad de la información (no oficial) contiene lineamientos para ANS de proveedores en terminos del SGSI. Sin embargo al no encontrase en su versión oficial no se esta aplicando.	0	No se cuenta con una política de seguridad donde se haga acuerdos para relaciones con los proveedores

										SEGUIMIENTO SEPTIEMBRE 2019		AUTODIAGNOSTICO MARZO 2018	
ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
CONTROL DE ACCESO													
T.1	**Responsable de SI/Responsable de TICs**	**CONTROL DE ACCESO**		**A.9**	**Componente planificación y modelo de madurez nivel gestionado**					72		**65**	
T.1.1	Responsable de SI	**REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO**	**Se debe limitar el acceso a información y a instalaciones de procesamiento de información.**	**A.9.1**	Modelo de madurez definido					80		**60**	
T.1.1.1	Responsable de SI	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	A.9.1.1		PR.DS-5	Revisar que la política contenga lo siguiente: a) los requisitos de seguridad para las aplicaciones del negocio; b) las políticas para la divulgación y autorización de la información, y los niveles de seguridad de la información y de clasificación de la información; c) la coherencia entre los derechos de acceso y las políticas de clasificación de información de los sistemas y redes; d) la legislación pertinente y cualquier obligación contractual concerniente a la limitación del acceso a datos o servicios; e) la gestión de los derechos de acceso en un entorno distribuido y en red, que reconoce todos los tipos de conexiones disponibles; f) la separación de los roles de control de acceso, (solicitud de acceso, autorización de acceso, administración del acceso); g) los requisitos para la autorización formal de las solicitudes de acceso; h) los requisitos para la revisión periódica de los derechos de acceso; i) el retiro de los derechos de acceso; j) el ingreso de los registros de todos los eventos significativos concernientes al uso y gestión de identificación de los usuarios, e información de autenticación secreta, en el archivo permanente; k) los roles de acceso privilegiado;			80	Se evidencia que la política proxima a aprobación cuenta con los elementos requeridos por la prueba.	40	Se cuenta con un documento de Politicas de Seguridad de la Información, falta aprobación por parte del Comité de Seguridad de la Información y Gobierno Digital (Resolución 696 de 2017)
T.1.1.2	Responsable de TICs	Acceso a redes y a servicios en red	Se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	A.9.1.2		PR.AC-4 PR.DS-5 PR.PT-3	Revisar la política relacionada con el uso de redes y de servicios de red y verificar que incluya: a) las redes y servicios de red a los que se permite el acceso; b) los procedimientos de autorización para determinar a quién se permite el acceso a qué redes y servicios de red; c) los controles y procedimientos de gestión para proteger el acceso a las conexiones de red y a los servicios de red; d) los medios usados para acceder a las redes y servicios de red (uso de VPN o redes inalámbricas); e) los requisitos de autenticación de usuarios para acceder a diversos servicios de red; f) el seguimiento del uso de servicios de red.			80	Se recomienda complementar dar alcance a la gestión especifica de las redes inalambricas y establecer si se deben actualizar su caracterización y proposito.	80	Se cuenta con un documento de Politicas de Seguridad de la Información, falta aprobación por parte del Comité de Seguridad de la Información y Gobierno Digital (Resolución 696 de 2017) Las politicas para el ingreso a los servicios y aplicativos de la unidad se realizan de acuerdo al area donde se encuentre o al requerimiento que solicite el jefe de area, se hace por medio de la herramienta trabajo colaborativo para autorizacion de accesos.
T.1.2	Responsable de SI	**GESTIÓN DE ACCESO DE USUARIOS**	**Se debe asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.**	**A.9.2**	Modelo de madurez gestionado cuantitativamente					73		**90**	
T.1.2.1	Responsable de SI	Registro y cancelación del registro de usuarios	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	A.9.2.1		PR.AC-1	Revisar el proceso para la gestión y la identificación de los usuarios que incluya: a) Identificaciones únicas para los usuarios, que les permita estar vinculados a sus acciones y mantener la responsabilidad por ellas; el uso de identificaciones compartidas solo se debe permitir cuando sea necesario por razones operativas o del negocio, y se aprueban y documentan; b) deshabilitar o retirar inmediatamente las identificaciones de los usuarios que han dejado la organización; c) identificar y eliminar o deshabilitar periódicamente las identificaciones de usuario redundantes; d) asegurar que las identificaciones de usuario redundantes no se asignen a otros usuarios.			100	Se evidencia el flujo de generación de paz y salvo mediante la herramienta Runmyproccess como control efectivo para soportar que se dan las debidas autorizaciones para ajustes a las identificaciones de usuarios.	100	Por medio del aplicativo trabajo colaborativo se desabilitan los usuarios al quedar paz y salvo con la entidad. Se realiza de forma periodica y automatica por el directorio activo ya que el detecta los usuarios redundantes, estos se eliminan manualmente.

											SEGUIMIENTO SEPTIEMBRE 2019		AUTODIAGNOSTICO MARZO 2018	
ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA		NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
T.1.2.2	Responsable de SI	Suministro de acceso de usuarios	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	A.9.2.2		PR.AC-1	Revisar el proceso para asignar o revocar los derechos de acceso otorgados a las identificaciones de usuario que incluya: a) obtener la autorización del propietario del sistema de información o del servicio para el uso del sistema de información o servicio; b) verificar que el nivel de acceso otorgado es apropiado a las políticas de acceso y es coherente con otros requisitos, tales como separación de deberes; c) asegurar que los derechos de acceso no estén activados antes de que los procedimientos de autorización estén completos; d) mantener un registro central de los derechos de acceso suministrados a una identificación de usuario para acceder a sistemas de información y servicios; e) adaptar los derechos de acceso de usuarios que han cambiado de roles o de empleo, y retirar o bloquear inmediatamente los derechos de acceso de los usuarios que han dejado la organización; f) revisar periódicamente los derechos de acceso con los propietarios de los sistemas de información o servicios.	Matriz de roles y responsabilidades		80	No se evidencia revisión periodica para la supresión o cambio de privilegios a los usuarios que han cambiado de Rol.	100	Por medio del directorio activo el usuario la primera vez que ingresa al perfil este automaticamente le solicitara cambio de contraseña. En cuanto al correo institucional se les envia la notificacion a un correo personal con la clave temporal para acceso a este correo institucional lo cual puede ser cambiado si lo desean.
T.1.2.3	Responsable de SI	Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	A.9.2.3		PR.AC-4 PR.DS-5	Revisar la asignación de derechos de acceso privilegiado a través de un proceso de autorización formal de acuerdo con la política de control de acceso pertinente. el proceso debe incluir los siguientes pasos: a) Identificar los derechos de acceso privilegiado asociados con cada sistema o proceso, (sistema operativo, sistema de gestión de bases de datos, y cada aplicación) y los usuarios a los que es necesario asignar; b) definir o establecer los derechos de acceso privilegiado a usuarios con base en la necesidad de uso y caso por caso, alineada con la política de control de acceso; c) mantener un proceso de autorización y un registro de todos los privilegios asignados. Sólo se debe suministrar derechos de acceso cuando el proceso de autorización esté completo; d) definir los requisitos para la expiración de los derechos de acceso privilegiado; e) establecer los derechos de acceso privilegiado a través de una identificación de usuario diferente de la usada para las actividades regulares del negocio. Las actividades regulares del negocio no se ejecutan desde una identificación privilegiada; f) tener las competencias de los usuarios con derechos de acceso privilegiado y su revisión periódica para verificar si están en línea con sus deberes; g) establecer y mantener procedimientos genéricos para evitar el uso no autorizado de identificaciones de usuario de administración genérica, de acuerdo con las capacidades de configuración del sistema; h) establecer la confidencialidad de la información de autenticación secreta, para las identificaciones de usuario de administración genérica, cuando se comparta (cambiar las contraseñas con frecuencia, y cuando un usuario privilegiado ha dejado el trabajo o cambia de trabajo, comunicarlas entre los usuarios privilegiados con los mecanismos apropiados).			80	Se evidencia que la matriz de roles yu perfiles es suceptible de actualizacion.	100	Para los contratistas en el directorio activo se coloca la fecha de caducidad de usuario según la terminacion del contrato y para los funcionarios la terminacion es indefinida. Teniendo en cuenta esta politica ellos podran acceder a la red y a los aplicativos a los cuales fueron autorizados por el jefe de area.
T.1.2.4	Responsable de SI	Gestión de información de autenticación secreta de usuarios	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	A.9.2.4		PR.AC-1	Revisar el proceso, que incluya: a) establecer la firma de una declaración para mantener confidencial la información de autenticación secreta personal, y mantener la información de autenticación secreta del grupo (cuando es compartida) únicamente dentro de los miembros del grupo; esta declaración firmada se puede incluir en los términos y condiciones del empleo para todos los que los usuarios ; b) estipular que todos los usuarios deben mantener su propia información de autenticación secreta, y se les suministra una autentificación secreta temporal segura, que se obligue a cambiar al usarla por primera vez; c) establecer procedimientos para verificar la identidad de un usuario antes de proporcionarle la nueva información de autenticación secreta de reemplazo o temporal; d) definir que la información de autenticación secreta temporal se suministra a los usuarios de una manera segura; y se evitar utilizar partes externas o de mensajes de correo electrónico no protegidos (texto claro); e) establecer que la información de autenticación secreta temporal es única para un individuo y no es fácil de adivinar; f) definir que los usuarios deben acusar recibo de la información de autenticación secreta; g) establecer que la información de autenticación secreta por defecto, del fabricante, se modifica después de la instalación de los sistemas o software.			60	Se evidencia debilidades para la asignación y/o reestablecimiento de accesos a sistemas como el correo electrónico donde la información es conocida por personal diferente al usuario final. Se recomienda habilitar los mecanismos requeridos para gestión autonoma de contraseñas	80	Por medio del directorio activo el usuario la primera vez que ingresa al perfil este automaticamente le solicitara cambio de contraseña. En cuanto al correo institucional se les envia la notificacion a un correo personal con la clave temporal para acceso a este correo lo cual puede ser cambiado si lo desean. El sistema solicita cada mes cambio de contraseña con los parametros definidos, esto con el fin de proteger la información.

										SEGUIMIENTO SEPTIEMBRE 2019		AUTODIAGNOSTICO MARZO 2018	
ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
T.1.2.5	Responsable de SI	Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	A.9.2.5			Revisar los derechos de acceso que incluya: a) examinar los derechos de acceso de los usuarios periódicamente y después de cualquier cambio, promoción, cambio a un cargo a un nivel inferior, o terminación del empleo; b) establecer que los derechos de acceso de usuario se revisan y reasignan cuando pasan de un rol a otro dentro de la misma organización; c) definir las autorizaciones para los derechos de acceso privilegiado y revisar periódicamente; d) verificar las asignaciones de privilegios periódicamente, para asegurar que no se hayan obtenido privilegios no autorizados; e) revisar y registrar los cambios a las cuentas privilegiadas periódicamente.	Procedimiento gestion de cuentas y registro		60	Se evidencian debilidades en la revisión de accesos para supresión o escalamiento de privilegios.	60	Para los contratistas en el directorio activo se coloca la fecha de caducidad de usuario según la terminacion del contrato y para los funcionarios la terminacion es indefinida. Teniendo en cuenta esta politica ellos podran acceder a la red y a los aplicativos a los cuales fueron autorizados por el jefe de area. Cuando existe licencia de de un superior se activa el que se encuentre encargado con el rol del que no se encuentre y se desactiva este.
T.1.2.6	Responsable de SI	Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	A.9.2.6			Revisar los derechos de acceso a la información y a los activos asociados con instalaciones de procesamiento de información, antes de que el empleo termine o cambie, dependiendo de la evaluación de factores de riesgo que incluya: a) terminación o cambio lo inicia el empleado, el usuario de la parte externa o la dirección, y la razón de la terminación; b) revisar las responsabilidades actuales del empleado, el usuario de la parte externa o cualquier otro usuario; c) verificar el valor de los activos accesibles en la actualidad.	Cronograma de migracion		60	En varios aplicativos el acceso o revocación de permiso es manual, se evidencian pruebas de Autenticación SSO orfeo, office azure connect, el tiempo para el ajuste se estimo por el auditado en dos semanas	100	El jefe del area es quien informa que aplicativos o carpetas compartidas debe acceder el empleado lo cual lo debe solicitar por medio de la herramienta trabajo colaborativo para que sea autorizado su acceso.
T.1.3	**Responsable de SI**	**RESPONSABILIDADES DE LOS USUARIOS**	**Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.**	**A.9.3**	Modelo de madurez definido					**60**		**40**	
T.1.3.1	Responsable de SI	Uso de información de autenticación secreta	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	A.9.3.1		PR.AC-1	Revisar si el proceso de notificacion a usuarios incluye: a) Mantener la confidencialidad de la información de autenticación secreta, asegurándose de que no sea divulgada a ninguna otra parte, incluidas las personas con autoridad; b) evitar llevar un registro (en papel, en un archivo de software o en un dispositivo portátil) de autenticación secreta, a menos que se pueda almacenar en forma segura y que el método de almacenamiento haya sido aprobado (una bóveda para contraseñas); c) cambiar la información de autenticación secreta siempre que haya cualquier indicio de que se pueda comprometer la información; d) definir que cuando se usa contraseñas como información de autenticación secreta, se debe seleccionar contraseñas seguras con una longitud mínima suficiente que: 1) sean fáciles de recordar; 2) no estén basadas en algo que otra persona pueda adivinar fácilmente u obtener usando información relacionada con la persona, (nombres, números de teléfono y fechas de nacimiento, etc.); 3) no sean vulnerables a ataques de diccionario (es decir, no contienen palabras incluidas en los diccionarios); 4) estén libres de caracteres completamente numéricos o alfabéticos idénticos consecutivos; 5) si son temporales, cambiarlos la primera vez que se ingrese; e) no compartir información de autenticación secreta del usuario individual; f) establecer una protección apropiada de contraseñas cuando se usan éstas como información de autenticación secreta en procedimientos de ingreso automatizados, y estén almacenadas; g) no usar la misma información de autenticación secreta para propósitos de negocio y otros diferentes de estos.	Correo notificando manejo seguro de contraseñas		60	El metodo para el reestablecimiento de contraseñas actualmente no asegura la confidencialidad de la misma, en el caso de correo electronico se evidencia desarticulado con el sistema de autenticacion de la entidad LDAP, se tiene un riesgo importante de confidencialidad.	40	Para la definición de la clave se deben seguir unas condiciones minimas la cuales se controlan por medio del software de LDAP
T.1.4	Responsable de SI	**CONTROL DE ACCESO A SISTEMAS Y APLICACIONES**	**Se debe evitar el acceso no autorizado a sistemas y aplicaciones.**	**A.9.4**	Modelo de madurez gestionado cuantitativamente					**76**		**68**	
T.1.4.1	Responsable de SI	Restricción de acceso a la información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.	A.9.4.1		PR.AC-4 PR.DS-5	Revisar las restricciones de acceso a través de la aplicación individual del negocio y de acuerdo con la política de control de acceso definida; que incluya: a) suministrar menús para controlar el acceso a las funciones de sistemas de aplicaciones; b) controlar a qué datos puede tener acceso un usuario particular; c) controlar los derechos de acceso de los usuarios, (a leer, escribir, borrar y ejecutar); d) controlar los derechos de acceso de otras aplicaciones; e) limitar la información contenida en los elementos de salida; f) proveer controles de acceso físico o lógico para el aislamiento de aplicaciones, datos de aplicaciones o sistemas críticos.	LDAP		100		100	

										SEGUIMIENTO SEPTIEMBRE 2019		AUTODIAGNOSTICO MARZO 2018	
ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
T.1.4.2	Responsable de SI	Procedimiento de ingreso seguro	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	A.9.4.2		PR.AC-1	Revisar el procedimiento de ingreso que incluya: a) no visualizar los identificadores del sistema o de la aplicación sino hasta que el proceso de ingreso se haya completado exitosamente; b) visualizar una advertencia general acerca de que sólo los usuarios autorizados pueden acceder al computador; c) evitar los mensajes de ayuda durante el procedimiento de ingreso, que ayudarían a un usuario no autorizado; d) validar la información de ingreso solamente al completar todos los datos de entrada. ante una condición de error, el sistema no debe indicar qué parte de los datos es correcta o incorrecta; e) proteger contra intentos de ingreso mediante fuerza bruta; f) llevar un registro con los intentos exitosos y fallidos; g) declarar un evento de seguridad si se detecta un intento potencial o una violación exitosa de los controles de ingreso; h) visualizar la siguiente información al terminar un ingreso seguro: 1) registrar la fecha y la hora del ingreso previo exitoso; 2) registrar los detalles de cualquier intento de ingreso no exitoso desde el último ingreso exitoso; i) no visualizar una contraseña que se esté ingresando; j) no transmitir contraseñas en un texto claro en una red; k) terminar sesiones inactivas después de un período de inactividad definido, especialmente en lugares de alto riesgo tales como áreas públicas o externas por fuera de la gestión de seguridad de la organización o en dispositivos móviles; l) restringir los tiempos de conexión para brindar seguridad adicional para aplicaciones de alto riesgo y para reducir la ventana de oportunidad para acceso no autorizado.			80		40	
T.1.4.3	Responsable de TICs	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	A.9.4.3		PR.AC-1	Revisar el sistema de gestión de contraseñas que incluya: a) cumplir el uso de identificaciones y contraseñas de usuarios individuales para mantener la rendición de cuentas; b) permitir que los usuarios seleccionen y cambien sus propias contraseñas e incluyan un procedimiento de confirmación para permitir los errores de entrada; c) Exigir por que se escojan contraseñas de calidad; d) Forzar a los usuarios cambiar sus contraseñas cuando ingresan por primera vez; e) Exigir por que se cambien las contraseñas en forma regular, según sea necesario: f) llevar un registro de las contraseñas usadas previamente, e impedir su reusó; g) no visualizar contraseñas en la pantalla cuando se está ingresando; h) almacenar los archivos de las contraseñas separadamente de los datos del sistema de aplicaciones; i) almacenar y transmitir las contraseñas en forma protegida.			80	El metodo actualmente implementado no permite el reestablecimiento autonomo de contraseñas.	80	
T.1.4.4	Responsable de TICs	Uso de programas utilitarios privilegiados	Se debe restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.	A.9.4.4		PR.AC-4 PR.DS-5	Revisar las directrices para el uso de programas utilitarios con la capacidad de anular los controles de sistemas y de aplicaciones, que incluyan. a) utilizar procedimientos de identificación, autenticación y autorización para los programas utilitarios; b) separar los programas utilitarios del software de aplicaciones; c) limitar el uso de programas utilitarios al número mínimo práctico de usuarios confiables y autorizados; d) autorizar el uso adhoc de programas utilitarios; e) limitar la disponibilidad de los programas utilitarios; f) registrar el uso de los programas utilitarios; g) definir y documentar los niveles de autorización para los programas utilitarios; h) retirar o deshabilitar todos los programas utilitarios innecesarios; i) No poner a disposición los programas utilitarios a los usuarios que tengan acceso a aplicaciones en sistemas en donde se requiera la separación de deberes.			80	Algunos aplicativos pueden ser ejecutados sin necesidad de ser instalados	100	Esto se realiza mediante la herramienta de administracion de software llamada ocs ya que verifica las hojas de vida de todos los equipos, programas autorizados y hardware instalado en el equipo.Aunque se controla la instalación de programas no deseados mediante el directorio activo y la ejecución de algunas herramientas.
T.1.4.5	Responsable de TICs	Control de acceso a códigos fuente de programas	Se debe restringir el acceso a los códigos fuente de los programas.	A.9.4.5		PR.DS-5	Revisar el procedimiento para la gestión de códigos fuente de los programas, que incluya: a) definir en donde sea posible, las librerías de fuentes de programas no se deben mantener en los sistemas operativos; b) gestionar los códigos fuente de los programas y las librerías de las fuentes de los programas se debería hacer de acuerdo con procedimientos establecidos; c) establecer que el personal de soporte deben tener acceso restringido a las librerías de las fuentes de los programas; d) definir que la actualización de las librerías de fuentes de programas y elementos asociados, y la entrega de fuentes de programas a los programadores sólo se deben hacer una vez que se haya recibido autorización apropiada; e) establecer que los listados de programas se deben mantener en un entorno seguro; f) conservar un registro de auditoría de todos los accesos a la librerías de fuentes de programas; g) mantener y copiar las bibliotecas de fuentes de programas a través de procedimientos estrictos de control de cambios.	procedimiento de gestion de cambios		40	No esta completa en el manual de politicas de seguridad de la informacion, Procedimiento de gestion de cambios	20	Solo pueden ingresar personal autorizado - Administrador de los sistemas de Información, al momento de retiro de la entidad deben entregar losinformes y sus respectivas claves al supervisor del contrato.
CRIPTOGRAFÍA													

										SEGUIMIENTO SEPTIEMBRE 2019		AUTODIAGNOSTICO MARZO 2018	
ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
T.2	**Responsable de SI**	**CRIPTOGRAFÍA**	**Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización Garantizar la seguridad del teletrabajo y el uso de los dispositivos móviles**	**A.10**						30		**0**	
T.2.1	**Responsable de SI**	**CONTROLES CRIPTOGRÁFICOS**	**Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.**	**A.10.1**	Modelo de madurez gestionado cuantitativamente					30		0	
T.2.1.1	Responsable de SI	Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	A.10.1.1			Revisar la política sobre el uso de la criptográfica, que incluya: a) establecer el enfoque de la dirección con relación al uso de controles criptográficos en toda la organización, incluyendo los principios generales bajo los cuales se deben proteger la información del negocio; b) realizar una valoración de riesgos, que identifique el nivel de protección requerida, teniendo en cuenta el tipo, fortaleza y calidad del algoritmo de encriptación requerido. c) utilizar la encriptación para la protección de información transportada por dispositivos de encriptación móviles o removibles, o a través de líneas de comunicación; d) gestionar las llaves y los métodos para la protección de llaves criptográficas y la recuperación de información encriptada, en el caso de llaves perdidas, llaves cuya seguridad está comprometida, o que están dañadas; e) establecer roles y responsabilidades, quién es responsable por: 1) la implementación de la política. 2) la gestión de llaves, incluida la generación de llaves; f) establecer las normas que se van a adoptar para la implementación efectiva en toda la organización (procesos del negocio); g) definir el impacto de usar información encriptada en los controles que dependen de la inspección del contenido.			40	Se evidencia pendiente por implementar	0	No se esta poniendo en practica procedimiento de uso de controles criptográficos para la protección de la información .
T.2.1.2	Responsable de SI	Gestión de llaves	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.	A.10.1.2			Revisar el sistema de gestión de llaves que debe estar basado en un grupo establecido de normas, procedimientos y métodos seguros para: a) generar llaves para diferentes sistemas criptográficos y diferentes aplicaciones; b) generar y obtener certificados de llaves públicas; c) distribuir llaves a las entidades previstas, incluyendo la forma de recibir y activar las llaves; d) almacenar las llaves, incluyendo la forma en que los usuarios autorizados obtienen acceso a ellas; e) cambiar o actualizar las llaves, incluyendo las reglas sobre cuándo se deben cambiar y cómo hacerlo; f) dar tratamiento a las llaves cuya seguridad está comprometida; g) revocar las llaves, incluyendo la forma de retirarlas o desactivarlas, cuando la seguridad de las llaves ha estado comprometida, o cuando un usuario deja la organización; h) recuperar las llaves que estén perdidas o dañadas; i) hacer copias de respaldo de las llaves o archivarlas; j) destruir las llaves; k) registrar y auditar las actividades relacionadas con gestión de llaves.			20	Se evidencian debilidades en la gestión de llaves y metodos seguros. Se evidencia que actualmente las llaves de acceso a la administracion de diversos sistemas es almacenada en archivos Keepass versión free que no permite la segregación de accesos.	0	
SEGURIDAD FÍSICA Y DEL ENTORNO													
T.3	**Responsable de la seguridad física/Responsable de SI/Líderes de los procesos**	**SEGURIDAD FÍSICA Y DEL ENTORNO**		**A.11**						65		60	
T.3.1	**Responsable de la seguridad física**	**ÁREAS SEGURAS**	**Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.**	**A.11.1**	Modelo de madurez definido					63		**53**	

										SEGUIMIENTO SEPTIEMBRE 2019		AUTODIAGNOSTICO MARZO 2018	
ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
T.3.1.1	Responsable de la seguridad física	Perímetro de seguridad física	Se debe definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.	A.11.1.1		PR.AC-2	Revisar las directrices relacionadas con los perímetros de seguridad física: a) definir los perímetros de seguridad, y el emplazamiento y fortaleza de cada uno de los perímetros deben depender de los requisitos de seguridad de los activos dentro del perímetro y de los resultados de una valoración de riesgos; b) establecer los perímetros de una edificación o sitio que contenga instalaciones de procesamiento de la información debe ser físicamente seguros; el techo exterior, las paredes y el material de los pisos del sitio deben ser de construcción sólida, y todas las paredes externas deben estar protegidas adecuadamente contra acceso no autorizado con mecanismos de control (barras, alarmas, cerraduras); las puertas y ventanas deben estar cerradas con llave cuando no hay supervisión, y se debe considerar protección externa para ventanas, particularmente al nivel del suelo; c) definir un área de recepción con vigilancia u otro medio para controlar el acceso físico al sitio o edificación; el acceso a los sitios y edificaciones debe estar restringido únicamente para personal autorizado; d) establecer cuando sea aplicable y construir barreras físicas para impedir el acceso físico no autorizado y la contaminación ambiental; e) establecer que todas las puertas contra incendio en un perímetro de seguridad deben tener alarmas, estar monitoreadas y probadas junto con las paredes, para establecer el nivel requerido de resistencia de acuerdo con normas regionales, nacionales e internacionales adecuadas; deben funcionar de manera segura de acuerdo al código local de incendios; f) instalar sistemas adecuados para detección de intrusos de acuerdo con normas nacionales, regionales o internacionales y se deben probar regularmente para abarcar todas las puertas externas y ventanas accesibles; las áreas no ocupadas deben tener alarmas en todo momento; también deben abarcar otras áreas, tales como las salas de computo o las salas de	soporte correo bodegas identificacion de areas		40	Se evidencia soporte para agendamiento de visita a bodegas con el acompañimiento de GTIC en agosto. Sin embargo, esta visita no se dio por lo cual no se ha hecho identificacion de perimetros de seguridad alli. En la sede administrativa de la UAESP el perimetro definido y que cuenta con controles de seguridad verificables es el DATA Center. Se recomienda con el acompañamiento de SAF la definifición y verificación de los controles de acceso fisicos existentes (compañia de vigilancia)	60	El perimetro de seguridad física, así como el control de acceso, se encuentra a cargo del área administrativa y a su vez tercerizado a la empresa de vigilancia privada. Las áreas seguras estan protegidas mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado. Tambien se tiene un control por parte de la vigilancia con respecto al acceso a personal externo que ingresa a la unidad por medio de un libro de registro. El datacenter de la unidad contiene informacion muy sensible y otros cuartos donde se encuentra el cableado estructurado estan custodiados por acceso a biometrico y esta debidamente protegido con alarmas de seguridad y sin problemas de humedad
T.3.1.2	Responsable de SI	Controles físicos de entrada	Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	A.11.1.2		PR.AC-2 PR.MA-1	Revisar los controles de acceso físico y las siguientes directrices: a) tener un registro de la fecha y hora de entrada y salida de los visitantes, y todos los visitantes deben ser supervisados a menos que su acceso haya sido aprobado previamente; solo se les debe otorgar acceso para propósitos específicos autorizados y se deben emitir instrucciones sobre los requisitos de seguridad del área y de los propósitos de emergencia. La identidad de los visitantes se deben autenticar por los medios apropiados; b) establecer que el acceso a las áreas en las que se procesa o almacena información confidencial se debería restringir a los individuos autorizados solamente mediante la implementación de controles de acceso apropiados, (mediante la implementación de un mecanismo de autenticación de dos factores, tales como una tarjeta de acceso y un PIN secreto); c) mantener y hacer seguimiento de un libro de registro (physical log book) físico o un rastro de auditoría electrónica de todos los accesos; d) definir que todos los empleados, contratistas y partes externas deben portar algún tipo de identificación visible, y se deben notificar de inmediato al personal de seguridad si se encuentran visitantes no acompañados, y sin la identificación visible; e) establecer que el personal de servicio de soporte de la parte externa se le debería otorgar acceso restringido a áreas seguras o a instalaciones de procesamiento de información confidencial solo cuando se requiera; este acceso se deben autorizar y se le debe hacer seguimiento; f) definir los derechos de acceso a áreas seguras se deben revisar y actualizar regularmente, y revocar cuando sea necesario.			60	No se lleva bitacora fisica o rastro digital de los visitantes que realizan soporte.	100	Los controles de acceso físico se encuentran bajo la supervisión del área administrativa y a su vez tercerizado a la empresa de vigilancia privada. Se lleva un control del ingreso y salida de los visitantes por medio de bitacora y se les entrega una escarpela para su identificación, que en el momento de salida debe ser entregada al personal de vigilancia. Los funcionarios registran la entrada y salida por medio del biometrico. Todas las personas que trbajan en la entidad deben portar el carnet institucional. La entrada a ciertas partes de la entidad estan sujetas a verificación o controles de acceso a las zonas.
T.3.1.3	Líderes de los procesos	Seguridad de oficinas, recintos e instalaciones	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	A.11.1.3			Revisar las siguientes directrices relacionadas con la seguridad a oficinas, recintos e instalaciones: a) establecer que las instalaciones clave deben estar ubicadas de manera que se impida el acceso del público; b) definir donde sea aplicable, las edificaciones deben ser discretas y dar un indicio mínimo de su propósito, sin señales obvias externas o internas, que identifiquen la presencia de actividades de procesamiento de información; c) establecer que las instalaciones deben estar configuradas para evitar que las actividades o información confidenciales sean visibles y audibles desde el exterior. El blindaje electromagnético también se debe ser el apropiado; d) definir 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.			80	Se recomienda establecer junto con el tercero encargado de la seguridad física la definicion de perimetros de seguridad.	100	Las areas se encuentran separadas al acceso al publico ya que se encuentran en diferentes pisos de la sede y deben de ingresar con autorizacion de algun funcionario a menos que necesiten radicar. las instalaciones estan configuradas para evitar que las actividades o información confidenciales sean visibles y audibles desde el exterior.
T.3.1.4	Responsable de SI	Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	A.11.1.4		ID.BE-5 PR.AC-2 PR.IP-5	De acuerdo a la NIST deben identificarse los elementos de resiliencia para soportar la entrega de los servicios críticos de la entidad.			40		20	El área administrativa toma control sobre la prevención e identificación de amenazas ambientales, se evidencian algunas deficiencias en la sede caracas aunque se encuentran demarcadas salidas de emergencia, extintores.

										SEGUIMIENTO SEPTIEMBRE 2019		AUTODIAGNOSTICO MARZO 2018	
ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
T.3.1.5	Responsable de SI	Trabajo en áreas seguras	Se debe diseñar y aplicar procedimientos para trabajo en áreas seguras.	A.11.1.5	Componente planeación		Revisar trabajo en área segura y las siguientes directrices: a) establecer que el personal solo debe conocer de la existencia de un área segura o de actividades dentro de un área segura, con base en lo que necesita conocer; b) definir que el trabajo no supervisado en áreas seguras se debe evitar tanto por razones de seguridad como para evitar oportunidades para actividades malintencionadas; c) establecer que las áreas seguras vacías deben estar cerradas con llave y se revisan periódicamente; d) no se permite el ingreso y uso de equipo fotográfico, de video, audio u otro equipo de grabación, tales como cámaras en dispositivos móviles, a menos que se cuente con autorización para ello.			80		20	Falta sensibilización
T.3.1.6	Responsable de la seguridad física	Áreas de despacho y carga	Se debe controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	A.11.1.6		PR.AC-2	Revisar las siguientes directrices: a) establecer que el acceso al área de despacho y de carga desde el exterior de la edificación se debería restringir al personal identificado y autorizado; b) definir que el área de despacho y carga se debe diseñar de manera que los suministros se puedan cargar y descargar sin que el personal de despacho tenga acceso a otras partes de la edificación; c) establecer que las puertas externas de un área de despacho y carga se aseguran cuando las puertas internas están abiertas; d) definir que el material que ingresa se inspecciona y examina para determinar la presencia de explosivos, químicos u otros materiales peligrosos, antes de que se retiren del área de despacho y carga; e) establecer que el material que ingresa se registra de acuerdo con los procedimientos de gestión de activos al entrar al sitio; f) definir que los despachos entrantes y salientes se están separados físicamente, en donde sea posible; g) establecer que el material entrante se inspecciona para determinar evidencia de manipulación durante el viaje. Si se descubre esta manipulación, se debería reportar de inmediato al personal de seguridad.			80		20	El perímetro de seguridad física, así como el control de acceso, se encuentra a cargo del área administrativa y a su vez tercerizado a la empresa de vigilancia privada ya que revisan todo lo que ingresa a las sedes y verifican su procedencia y autorizacion.
T.3.2	**Responsable de SI**	**EQUIPOS**	**Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.**	**A.11.2**	Modelo de madurez definido					67		**67**	
T.3.2.1	Responsable de SI	Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.	A.11.2.1		PR.IP-5	Revisar las siguientes directrices para proteger los equipos: a) establecer que los equipos están ubicados de manera que se minimice el acceso innecesario a las áreas de trabajo; b) definir que las instalaciones de procesamiento de la información que manejan datos sensibles están ubicadas cuidadosamente para reducir el riesgo de que personas no autorizadas puedan ver la información durante su uso; c) establecer que las instalaciones de almacenamiento se aseguran para evitar el acceso no autorizado; d) definir que los elementos que requieren protección especial se salvaguardan para reducir el nivel general de protección requerida; e) establecer los controles para minimizar el riesgo de amenazas físicas y ambientales, (robo, incendio, explosivos, humo, agua (o falla en el suministro de agua, polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo); f) establecer directrices acerca de comer, consumir líquidos y fumar en cercanías de las instalaciones de procesamiento de información; g) hacer seguimiento de las condiciones ambientales tales como temperatura y humedad, para determinar las condiciones que puedan afectar adversamente las instalaciones de procesamiento de información; h) proteger contra descargas eléctricas atmosféricas se debe aplicar a todas las edificaciones y se deben colocar filtros a todas las líneas de comunicaciones y de potencia entrantes, para la protección contra dichas descargas; i) considerar el uso de métodos de protección especial, tales como membranas para teclados, para equipos en ambientes industriales; j) proteger los equipos para procesamiento de información confidencial para			80		100	Los equipos de escritorio permanecen en sus respectivos puestos sin que sean trasladados en cuanto a portatiles todos tienes su respectiva guaya para que no sean manipulados por extraños, se dispone de personal de vigilancia y camaras lo cual estan verificando las diferentes areas de la entidad. Tambien cuenta con instalaciones aisladas para salvaguardar la informacion sensible y se reduce el riesgo de que personas externas no vean su uso. Se realiza un seguimiento de las condiciones ambientales tales como temperatura y humedad, para determinar las condiciones que puedan afectar adversamente las instalaciones de procesamiento de información.
T.3.2.2	Responsable de TICs	Servicios de suministro	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	A.11.2.2		ID.BE-4 PR.IP-5	Revisar los servicios de suministro (electricidad, telecomunicaciones, suministro de agua, gas, alcantarillado, ventilación y aire acondicionado) para que cumplan: a) cumplir con las especificaciones de los fabricantes de equipos y con los requisitos legales locales; b) evaluar regularmente en cuanto a su capacidad para estar al ritmo del crecimiento e interacciones del negocio con otros servicios de soporte; c) inspeccionar y probar regularmente para asegurar su funcionamiento apropiado; d) si es necesario, contar con alarmas para detectar mal funcionamiento; e) si es necesario, tener múltiples alimentaciones con diverso enrutado físico.			80	Se evidenciaron fallas en el suministro electrico, se evidencian fallas en sistemas de video vigilancia. Se sugiere revisar proyecto para implementacion de cableado estructurado en las oficinas de casitas dado que se reportan constantemente fallas en el fluido electrico y red.	80	

										SEGUIMIENTO SEPTIEMBRE 2019		AUTODIAGNOSTICO MARZO 2018	
ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
T.3.2.3	Responsable de TICs	Seguridad del cableado	El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información deben estar protegido contra interceptación, interferencia o daño.	A.11.2.3		ID.BE-4 PR.AC-2 PR.IP-5	Revisar las siguientes directrices para seguridad del cableado: a) establecer que las líneas de potencia y de telecomunicaciones que entran a instalaciones de procesamiento de información deben ser subterráneas en donde sea posible, o deben contar con una protección alternativa adecuada; b) establecer que los cables de potencia están separados de los cables de comunicaciones para evitar interferencia; c) definir para sistemas sensibles o críticos los controles adicionales que se deben considerar incluyen: 1) la instalación de conduit apantallado y recintos o cajas con llave en los puntos de inspección y de terminación; 2) el uso de blindaje electromagnético para proteger los cables; 3) el inicio de barridos técnicos e inspecciones físicas de dispositivos no autorizados que se conectan a los cables			100		100	
T.3.2.4	Responsable de TICs	Mantenimiento de equipos	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	A.11.2.4		PR.MA-1 PR.MA-2	Revisar las siguientes directrices para mantenimiento de equipos: a) mantener los equipos de acuerdo con los intervalos y especificaciones de servicio recomendados por el proveedor; b) establecer que solo el personal de mantenimiento autorizado debería llevar a cabo las reparaciones y el servicio a los equipos; c) llevar registros de todas las fallas reales o sospechadas, y de todo el mantenimiento preventivo y correctivo; d) implementar los controles apropiados cuando el equipo está programado para mantenimiento, teniendo en cuenta si éste lo lleva a cabo el personal en el sitio o personal externo a la organización; en donde sea necesario, la información confidencial se debe borrar del equipo, o el personal de mantenimiento debería retirarse (cleared) lo suficientemente de la información; e) cumplir todos los requisitos de mantenimiento impuestos por las políticas de seguros; f) establecer que antes de volver a poner el equipo en operación después de mantenimiento, se debería inspeccionar para asegurarse de que no ha sido alterado y que su funcionamiento es adecuado.			100		100	
T.3.2.5	Responsable de TICs	Retiro de activos	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	A.11.2.5		PR.MA-1	Revisar las siguientes directrices para el retiro de activos: a) identificar a los empleados y usuarios de partes externas que tienen autoridad para permitir el retiro de activos del sitio; b) establecer los límites de tiempo para el retiro de activos y verificar que se cumplen las devoluciones; c) definir cuando sea necesario y apropiado, registrar los activos se retiran del sitio y cuando se hace su devolución; d) documentar la identidad, el rol y la filiación de cualquiera que maneje o use activos, y devolver esta documentación con el equipo, la información y el software. Información adicional			40	Para autorizar las salidas no se cuenta un procedimiento desde GTIC,	100	Cada vez que se solicita una consulta a un documento de archivo se tiene que enviar un correo para autorizacion del jefe de Asuntos Legales y se tiene que firmar una bitacora donde se tiene historial de las consultas del documento. En cuanto a bienes fisicos se tiene relacion con la bitacora que maneja el personal de vigilancia por si los funcionarios desean llevarse su portatil.
T.3.2.6	Responsable de SI	Seguridad de equipos y activos fuera de las instalaciones	Se debe aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	A.11.2.6		ID.AM-4	De acuerdo a la NIST se deben catalogar los sistemas de información externos. Revisar las siguientes directrices para proteger los equipos fuera de las instalaciones: a) establecer que los equipos y medios retirados de las instalaciones no se deben dejar sin vigilancia en lugares públicos; b) seguir en todo momento las instrucciones del fabricante para proteger los equipos, (contra exposición a campos electromagnéticos fuertes); c) controlar los lugares fuera de las instalaciones, tales como trabajo en la casa, teletrabajo y sitios temporales se deben determinar mediante una valoración de riesgos y se deben aplicar los controles adecuados según sean apropiados, (gabinetes de archivo con llave, política de escritorio limpio, controles de acceso para computadores y comunicación segura con la oficina); d) establecer que cuando el equipo que se encuentra afuera de las instalaciones es transferido entre diferentes individuos y partes externas, llevar un registro que defina la cadena de custodia para el equipo, que incluya al menos los nombres y las organizaciones de los responsables del equipo.	Catalogo de servicios de inofrmacion		80	Se debe complementar con el analisis de riesgo de los equipos fuera de la UAESP	60	No hay un procedimiento como tal pero se tiene un seguimiento permanente con los equipos que estan fuera de las instalaciones, los equipos portatiles cuentan con garantia y con polizas
T.3.2.7	Responsable de TICs	Disposición segura o reutilización de equipos	Se debe verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reusó.	A.11.2.7		PR.DS-3 PR.IP-6	Revisar las siguientes directrices del proceso de borrado de discos y de encriptación del disco (para evitar la divulgación de la información confidencial cuando se dispone del equipo o se le da un destino diferente, siempre y cuando): a) establecer que el proceso de encriptación sea suficientemente fuerte y abarque todo el disco (incluido el espacio perdido, archivos temporales de intercambio, etc.); b) definir que las llaves de encriptación sean lo suficientemente largas para resistir ataques de fuerza bruta; c) establecer que las llaves de encriptación se mantengan confidenciales.			20	Se evidencia borrador de procedimiento para borrado seguro, sin embargo no se ha construido una versión definitiva por tanto no es posible evidenciar que se tienen un lineamiento que adopte la entidad para asegurar esta actividad.	20	En el momento a los equipos que se van a entregar por devolucion a la empresa proveedora o los que se van a dar de baja o los que se van a asignar a otra persona son estrictamente formateados para que no halla ingreso a informacion privada de otros usuarios

										SEGUIMIENTO SEPTIEMBRE 2019		AUTODIAGNOSTICO MARZO 2018	
ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
T.3.2.8	Responsable de SI	Equipos de usuario desatendidos	Los usuarios deben asegurarse de que a los equipos desatendidos se les dé protección apropiada.	A.11.2.8			Revisar que el procedimiento equipos de usuarios desatendidos incluya: a) establecer que se cierren las sesiones activas cuando hayan terminado, a menos que se puedan asegurar mediante un mecanismo de bloqueo apropiado (un protector de pantalla protegido con contraseña); b) establecer que es obligatorio salir de las aplicaciones o servicios de red cuando ya no los necesiten; c) asegurar que los computadores o dispositivos móviles contra uso no autorizado mediante el bloqueo de teclas o un control equivalente (acceso con contraseña, cuando no están en uso).	Política de seguridad de la informacion		80	Se sugiere revisar la configuración de la politica de bloqueo de sesión, pues se evidenció que los tiempos definidos se exceden.	20	Falta un procedimiento especifico pero se esta realizando sensibilizacion mediante correo electronico acerca de tips para seguridad de la informacion y bloqueo de sesion. Se tiene una politica de usuarios desatendidos por un tiempo de 2 minutos esto con el fin de proteger la informacion si algun usuario deja su sesion abierta. De la misma forma se tiene cambio de contraseña de ingreso de perfil cada mes.
T.3.2.9	Responsable de SI	Política de escritorio limpio y pantalla limpia	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	A.11.2.9		PR.PT-2	Revisar las siguientes directrices para escritorio limpio: a) establecer que la información sensible o crítica del negocio, (sobre papel o en un medio de almacenamiento electrónico), se guarda bajo llave (idealmente, en una caja fuerte o en un gabinete u otro mueble de seguridad) cuando no se requiera, especialmente cuando la oficina esté desocupada. b) definir un procedimiento para la gestión de equipos desatendidos; los computadores y terminales deben estar fuera del sistema y estar protegidos con un sistema de bloqueo de la pantalla y el teclado, controlado por una contraseña, token o mecanismo similar de autenticación de usuario, y deben estar protegidos por bloqueo de teclas u otros controles, cuando no están en uso; c) evitar el uso no autorizado de fotocopiadoras y otra tecnología de reproducción (escáneres, cámaras digitales); d) establecer que los medios que contienen información sensible o clasificada se deben retirar de las impresoras inmediatamente.			20	Actualmente no se evidencia seguimiento de politica de escritorio limpio.	20	Se envian correos institucionales acerca de tips para seguridad de la informacion, se tiene politica de bloqueo de sesion y cada funcionario tiene en su puesto un escritorio con cajones y su respectiva llave con el fin de guardar su documentacion.
SEGURIDAD DE LAS OPERACIONES													
T.4	**Responsable de TICs/Responsable de SI**	**SEGURIDAD DE LAS OPERACIONES**		**A.12**						53		38	
T.4.1	**Responsable de TICs**	**PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES**	**Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.**	**A.12.1**	Modelo de madurez definido					45		**10**	
T.4.1.1	**Responsable de TICs**	Procedimientos de operación documentados	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.	A.12.1.1			Revisar los procedimientos de operación con instrucciones operacionales, que incluyen: a) instalar y configurar sistemas; b) establecer el procesamiento y manejo de información, tanto automático como manual; c) establecer la gestión de las copias de respaldo; d) definir los requisitos de programación, incluidas las interdependencias con otros sistemas, los tiempos de finalización del primer y último trabajos; e) establecer las instrucciones para manejo de errores u otras condiciones excepcionales que podrían surgir durante la ejecución del trabajo, incluidas las restricciones sobre el uso de sistemas utilitarios; f) definir contactos de apoyo y de una instancia superior, incluidos los contactos de soporte externo, en el caso de dificultades operacionales o técnicas inesperadas; g) establecer las instrucciones sobre manejo de medios y elementos de salida, tales como el uso de papelería especial o la gestión de elementos de salida confidenciales, incluidos procedimientos para la disposición segura de elementos de salida de trabajos fallidos; h) definir los procedimientos de reinicio y recuperación del sistema para uso en el caso de falla del sistema; i) definir la gestión de la información de rastros de auditoria y de información del log del sistema; j) establecer los procedimientos de seguimiento.	proceso de soporte y mantenimiento. Sin la linea de ITIL		60	Estado de plataforma help people, la herramienta esta parametrizada en ambiente de produccion. Se plantea plan pilotocon la OAP	20	Se tienen documentados los procedimientos para Back up, administración de servidores, gestión de software y Hardware y Administración de Tics.

										SEGUIMIENTO SEPTIEMBRE 2019		AUTODIAGNOSTICO MARZO 2018	
ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
T.4.1.2	Responsable de TICs	Gestión de cambios	Se debe controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	A.12.1.2		PR.IP-1 PR.IP-3	Revisar los procedimientos de control de cambios, que incluyen: a) Identificar y registrar los cambios significativos; b) Planificar y puesta a prueba de los cambios; c) Valorar los impactos potenciales, incluidos los impactos de estos cambios en la seguridad de la información; d) Tener un procedimiento de aprobación formal para los cambios propuestos; e) Verificar que se han cumplido los requisitos de seguridad de la información; f) Comunicar todos los detalles de los cambios a todas las personas pertinentes; g) Tener un procedimiento de apoyo, incluidos procedimientos y responsabilidades para abortar cambios no exitosos y recuperarse de ellos, y eventos no previstos; h) Contar con un suministro de un proceso de cambio de emergencia que posibilite la implementación rápida y controlada de los cambios necesarios para resolver un incidente.			20	Se evidencia borrador de procedimiento de gestion de cambios. Se sugiere completar para que surta los tramitees correspondientes y proceder a su implementación	0	
T.4.1.3	Responsable de TICs	Gestión de capacidad	Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.	A.12.1.3		ID.BE-4	Revisar los procedimientos para la gestión de la demanda de capacidad, que incluyen: a) Eliminar datos obsoletos (espacio en disco); b) realizar cierre definitivo de aplicaciones, sistemas, bases de datos o ambientes; c) optimizar cronogramas y procesos de lotes; d) optimizar las consultas de bases de datos o lógicas de las aplicaciones; e) realizar una negación o restricción de ancho de banda a servicios ávidos de recursos, si estos no son críticos para el negocio (por ejemplo, video en tiempo real).			80	Se evidencia el establecimiento de reglas de revision 70% capacidad de disco, mediante alertas se definio una accion de mejora para control de tiempos se servico y gestion de proyectos. Se estima desarrollarlo en tres meses. Captura de pantalla de herramienta PRTG Network	0	
T.4.1.4	Responsable de TICs	Separación de los ambientes de desarrollo, pruebas y operación	Se debe separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	A.12.1.4		PR.DS-7	Revisar los procedimientos para la separación de ambientes, que incluyen: a) definir y documentar las reglas para la transferencia de software del estatus de desarrollo al de operaciones. b) establecer que el software de desarrollo y de operaciones debe funcionar en diferentes sistemas o procesadores de computador y en diferentes dominios o directorios; c) definir que los cambios en los sistemas operativos y aplicaciones se deben probar en un entorno de pruebas antes de aplicarlos a los sistemas operacionales; d) definir que solo en circunstancias excepcionales, las pruebas no se deben llevar a cabo en los sistemas operacionales; e) establecer que los compiladores, editores y otras herramientas de desarrollo o utilitarios del sistema no debe ser accesibles desde sistemas operacionales cuando no se requiere; f) establecer que los usuarios deben usar diferentes perfiles de usuario para sistemas operacionales y de pruebas, y los menús deben desplegar mensajes de identificación apropiados para reducir el riesgo de error; g) definir que los datos sensibles no se debe copiar en el ambiente del sistema de pruebas, a menos que se suministren controles equivalentes para el sistema de pruebas			20	Actualmente no se evidencia lineamientos que den cuenta de la separación de ambientes para el desarrollo de sistemas.	20	
T.4.2	**Responsable de SI**	**PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS**	**Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.**	**A.12.2**						**40**		**20**	

										SEGUIMIENTO SEPTIEMBRE 2019		AUTODIAGNOSTICO MARZO 2018	
ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
T.4.2.1	**Responsable de SI**	Controles contra códigos maliciosos	Se debe implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	A.12.2.1	Modelo de madurez gestionado	PR.DS-6 DE.CM-4 RS.MI-2	Revisar las siguientes directrices: a) establecer una política formal que prohíba el uso de software no autorizado; b) implementar controles para evitar o detectar el uso de software no autorizado (listas blancas de aplicaciones); b) implementar controles para evitar o detectar el uso de sitios web malicioso o que se sospecha que lo son (listas negras); d) establecer una política formal para proteger contra riesgos asociados con la obtención de archivos y de software ya sea mediante redes externas o cualquier otro medio, indicando qué medidas externas se deben tomar; e) reducir las vulnerabilidades de las que pueda aprovecharse el software malicioso, (medio de la gestión de la vulnerabilidad técnica); f) llevar a cabo revisiones regulares del software y del contenido de datos de los sistemas que apoyan los procesos críticos del negocio; se debería investigar formalmente la presencia de archivos no aprobados o de enmiendas no autorizadas; g) instalar y actualizar software de detección y reparación del software malicioso en los computadores y medios como una medida de control, en forma rutinaria; el análisis realizado debería incluir: 1) el análisis de cualquier archivo recibido por la red o por cualquier forma de medio de almacenamiento, para detectar el software malicioso, antes de uso; 2) el análisis de los adjuntos y descargas de los correos electrónicos, para determinación del software malicioso antes de uso; este análisis se debería llevar a cabo en diferentes lugares, (los servidores de los correos electrónicos, en los computadores de escritorio) y cuando se ingresa a la red de la organización; el análisis de páginas web, para determinar el software			40	Actualmente se evidencia debilidades en los controles de protección contra códigos maliciosos debido a que no se cuenta con herramienta antimalware por problemas en la contratación.	20	Se cuenta con firewall (corta fuegos) para la proteccion de la red de la entidad en cuanto a ataques cibernéticos, tambien se tienen instaladas en todas las maquinas antivirus Karpeski para la proteccion
T.4.3	**Responsable de TICs**	**COPIAS DE RESPALDO**	**Proteger contra la pérdida de datos.**	**A.12.3**	Modelo de madurez gestionado					**80**		**80**	
T.4.3.1	Responsable de TICs	Respaldo de la información	Se debe hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.	A.12.3.1		PR.DS-4 PR.IP-4	Revisar las siguientes directrices: a) producir registros exactos y completos de las copias de respaldo, y procedimientos de restauración documentados; b) establecer la cobertura (copias de respaldo completas o diferenciales) y la frecuencia con que se hagan las copias de respaldo debe reflejar los requisitos del negocio de la organización, los requisitos de la seguridad de la información involucrada, y la criticidad de la información para la operación continua de la organización; c) definir las copias de respaldo se debe almacenar en un lugar remoto, a una distancia suficiente que permita escapar de cualquier daño que pueda ocurrir en el sitio principal; d) establecer la información de respaldo y un nivel apropiado de protección física y del entorno, de coherencia con las normas aplicadas en el sitio principal; e) definir los medios de respaldo se debe poner a prueba regularmente para asegurar que se puede depender de ellos para uso de emergencia en caso necesario; esto se debería combinar con una prueba de los procedimientos de restauración, y se debe verificar contra el tiempo de restauración requerido. f) definir las situaciones en las que la confidencialidad tiene importancia, las copias de respaldo deben estar protegidas por medio de encriptación.			80	Se evidencia la ejecución de la herramienta para generacion de copias de seguridad sin embargo no se evidencia para todos los sistemas la ejecución de pruebas de restauracón.	80	
T.4.4	Responsable de SI	**REGISTRO Y SEGUIMIENTO**	**Registrar eventos y generar evidencia.**	**A.12.4**	Modelo de madurez gestionado cuantitativamente					**65**		**55**	
T.4.4.1	Responsable de SI	Registro de eventos	Se debe elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	A.12.4.1	Modelo de madurez gestionado cuantitativamente	PR.PT-1 DE.CM-3 RS.AN-1	Revisar los registros de eventos que incluyan: a) identificar los usuarios; b) establecer las actividades del sistema; c) definir las fechas, horas y detalles de los eventos clave, (entrada y salida); d) identificar el dispositivo o ubicación, si es posible, e identificador del sistema; e) tener registros de intentos de acceso al sistema exitosos y rechazados; e) definir registros de datos exitosos y rechazados y otros intentos de acceso a recursos; g) establecer los cambios a la configuración del sistema; h) definir el uso de privilegios; i) establecer el uso de utilitarios y aplicaciones del sistema; j) definir los archivos a los que se tuvo acceso, y el tipo de acceso; k) establecer las direcciones y protocolos de red; l) definir las alarmas accionadas por el sistema de control de acceso; m) activar y desactivar los sistemas de protección, tales como sistemas antivirus y sistemas de detección de intrusión; n) registrar las transacciones ejecutadas por los usuarios en las aplicaciones.			60	Se sugiere adoptar un metodo para generar trazabilidad de las acciones de los usuarios en los distintos sistemas	40	Los requerimientos de falla se encuentran dentro de la mesa de ayuda.

										SEGUIMIENTO SEPTIEMBRE 2019		AUTODIAGNOSTICO MARZO 2018	
ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
T.4.4.2	Responsable de SI	Protección de la información de registro	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	A.12.4.2		PR.PT-1	Revisar los procedimientos y controles dirigidos a proteger contra cambios no autorizados de la información del registro y contra problemas con la instalación de registro, que incluya: a) verificar todas las alteraciones a los tipos de mensaje que se registran; b) establecer los archivos log que son editados o eliminados; c) verificar cuando se excede la capacidad de almacenamiento del medio de archivo log, lo que da como resultado falla en el registro de eventos, o sobre escritura de eventos pasados registrados.			60	Se evidencian logs de aplicaciones sin embargo, no se revisan periodicamente.	20	Cada aplicacion genera su log de eventos automatico Se deja registro de quién accede a la información, los logs se encuentran en formato editable.
T.4.4.3	Responsable de SI	Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se debe registrar, y los registros se deben proteger y revisar con regularidad.	A.12.4.3		PR.PT-1 RS.AN-1	Revisar los registros de las actividades del administrador y del operador del sistema, los registros se deben proteger y revisar con regularidad.			40	se tiene activados los roles de auditoria sin embargo no se revisan pues no se tiene una herramienta que correlacione los eventos	60	Cada aplicacion genera su log de eventos automatico Se deja registro de quién accede a la información, los logs se encuentran en formato editable.
T.4.4.4	Responsable de SI	Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	A.12.4.4		PR.PT-1	Revisar se deberían sincronizar con una única fuente de referencia de tiempo Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.			100		100	Si se cuenta con sincronización de relojes entre servidores, bases de datos y dispositivos de red.
T.4.5	**Responsable de TICs**	**CONTROL DE SOFTWARE OPERACIONAL**	**Asegurar la integridad de los sistemas operacionales.**	**A.12.5**	Modelo de madurez definido					**60**		**20**	
T.4.5.1	Responsable de TICs	Instalación de software en sistemas operativos	Se debe implementar procedimientos para controlar la instalación de software en sistemas operativos.	A.12.5.1		PR.DS-6 PR.IP-1 PR.IP-3 DE.CM-5	Revisar las siguientes directrices para control de software operacional: a) actualizar el software operacional, aplicaciones y bibliotecas de programas solo la debe llevar a cabo administradores entrenados, con autorización apropiada de la dirección; b) definir que los sistemas operacionales sólo debe contener códigos ejecutables aprobados, no el código de desarrollo o compiladores; c) establecer que las aplicaciones y el software del sistema operativo solo se debe implementar después de pruebas extensas y exitosas; los ensayos deben abarcar la usabilidad, la seguridad, los efectos sobre otros sistemas y la facilidad de uso, y se debe llevar a cabo en sistemas separados; se debe asegurar que todas las bibliotecas de fuentes de programas correspondientes hayan sido actualizadas; d) usar un sistema de control de la configuración para mantener el control de todo el software implementado, al igual que la documentación del sistema; e) establecer una estrategia de retroceso (rollback) antes de implementar los cambios; f) mantener un log de auditoría de todas las actualizaciones de las bibliotecas de programas operacionales; g) definir las versiones anteriores del software de aplicación se deben conservar como una medida de contingencia; h) establecer que las versiones de software anteriores se deben llevar al archivo permanente, junto con toda la información y parámetros, procedimientos, detalles de configuración y software de soporte anteriores, en tanto los datos permanezcan en el archivo permanente.			60	se evidencia procedimiento para regular la instalación de Sw pero no se evidencia el alcance para realización de pruebas y definición de rollback en casos de contigencia.	20	Se tienen permisos de administrador para poder instalar software estos permisos solo los tiene el personal de TIC, tambien se cuenta con un software OSC Inventory lo cual detecta software diferente al basico de la entidad.
T.4.6	**Responsable de SI**	**GESTIÓN DE LA VULNERABILIDAD TÉCNICA**	**Prevenir el aprovechamiento de las vulnerabilidades técnicas.**	**A.12.6**	Modelo de madurez gestionado					**60**		**60**	
T.4.6.1	Responsable de SI	Gestión de las vulnerabilidades técnicas	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	A.12.6.1		ID.RA-1 ID.RA-5 PR.IP-12 DE.CM-8 RS.MI-3	Revisar las siguientes directrices para vulnerabilidades técnicas: a) definir y establecer los roles y responsabilidades asociados con la gestión de la vulnerabilidad técnica, incluido el seguimiento de la vulnerabilidad, la valoración de riesgos de vulnerabilidad, la colocación de parches, el seguimiento de activos y cualquier responsabilidad de coordinación requerida; b) definir los recursos de información que se usarán para identificar las vulnerabilidades técnicas pertinentes y para mantener la toma de conciencia acerca de ellos se debe identificar para el software y otra tecnología; c) una línea de tiempo para reaccionar a las notificaciones de vulnerabilidades técnicas pertinentes potencialmente; d) establecer que una vez que se haya identificado una vulnerabilidad técnica potencial, la organización debería identificar los riesgos asociados y las acciones por tomar; esta acción puede involucrar la colocación de parches de sistemas vulnerables o la aplicación de otros controles; Si no es posible colocar controles se deben documentar en los riesgos de acuerdo a su probabilidad e impacto y colocarlo como riesgo aceptado. e) definir dependiendo de la urgencia con la que se necesite tratar una vulnerabilidad técnica, la acción tomada se debería llevar a cabo de acuerdo con los controles relacionados con la gestión de cambios, o siguiendo los procedimientos de respuesta a incidentes de seguridad de la información; f) establecer, si está disponible un parche de una fuente legítima, se debe valorar los riesgos asociados con la instalación del parche (los riesgos que acarrea la vulnerabilidad se debe comparar con el riesgo de instalar el parche); g) establecer que los parches se deben probar y evaluar antes de su instalación, para asegurarse de que son eficaces y no producen efectos secundarios que no se puedan tolerar; si no hay parches disponibles, se debe			20	No se evidencia un lineamiento formal para el tratamiento de vulnerabilidades técnicas	20	

										SEGUIMIENTO SEPTIEMBRE 2019		AUTODIAGNOSTICO MARZO 2018	
ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
T.4.6.2	Responsable de TICs	Restricciones sobre la instalación de software	Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.	A.12.6.2		PR.IP-1 PR.IP-3	Revisar las restricciones y las reglas para la instalación de software por parte de los usuarios.			100	Sse recomienda hacer revisión de aplicativos que se ejecutan sin requerir instalación	100	
T.4.7	**Responsable de TICs**	**CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN**	**Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.**	**A.12.7**	Modelo de madurez gestionado cuantitativamente					**20**		**20**	
T.4.7.1	Responsable de TICs	Controles sobre auditorías de sistemas de información	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se debe planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	A.12.7.1			Revisar las siguientes directrices para las auditorias de sistemas de información: a) establecer los requisitos de auditoría para acceso a sistemas y a datos se debe acordar con la dirección apropiada; b) definir el alcance de las pruebas técnicas de auditoría se debe acordar y controlar; c) establecer las pruebas de auditoría se debe limitar a acceso a software y datos únicamente para lectura; d) definir el acceso diferente al de solo lectura solamente se debe prever para copias aisladas de los archivos del sistema, que se deben borrar una vez que la auditoría haya finalizado, o se debe proporcionar información apropiada si hay obligación de mantener estos archivos bajo los requisitos de documentación de auditoría; e) definir los requisitos para procesos especiales y adicionales se debe identificar y acordar; f) establecer las pruebas de auditoría que puedan afectar la disponibilidad del sistema se deben realizar fuera de horas laborales; g) hacer seguimiento de todos los accesos y logged para producir un rastro de referencia.	Instructivo Analisis de vulnerabilidades LDAP rol de audiria		20	NO se han plateado Roles de auditoria	20	En la auditoria que se realizo este año no se evidencia la la verificación de los sistemas operativos
SEGURIDAD DE LAS COMUNICACIONES													
T.5	**Responsable de TICs/Responsable de SI**	**SEGURIDAD DE LAS COMUNICACIONES**		**A.13**						56		42	
T.5.1	**Responsable de TICs**	**GESTIÓN DE LA SEGURIDAD DE LAS REDES**	**Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.**	**A.13.1**	Modelo de madurez definido					**87**		**73**	
T.5.1.1	Responsable de TICs	Controles de redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	A.13.1.1		PR.AC-3 PR.AC-5 PR.DS-2 PR.PT-4	Revisar las siguientes directrices para la gestión de seguridad de redes: a) establecer las responsabilidades y procedimientos para la gestión de equipos de redes; b) definir la responsabilidad operacional por las redes se debería separar de las operaciones informáticas, en donde sea apropiado; c) establecer controles especiales para salvaguardar la confidencialidad e integridad de los datos que pasan sobre redes públicas o sobre redes inalámbricas, y para proteger los sistemas y aplicaciones conectados; d) De acuerdo a NIST, Gestionar el acceso remoto d) aplicar logging y seguimiento adecuados para posibilitar el registro y detección de acciones que pueden afectar, o son pertinentes a la seguridad de la información; e) definir las actividades de gestión a coordinar estrechamente tanto para optimizar el servicio de la organización, como para asegurar que los controles se apliquen en forma coherente a través de la infraestructura de procesamiento de información; f) establecer los sistemas en la red que se autenticar; g) restringir la conexión de los sistemas a la red.			80	Se evidencian controles asociados a la gestión de redes y egmentación. Se recomienda dar alcance a la gestión de redes inalambricas las cuales son administradas totalmente por la UAESP	60	Las redes inalámbricas se controlan mediante el firewall sonicwall, y para la red cableada con la segmentación por VLANs y el directorio activo.
T.5.1.2	Responsable de SI	Seguridad de los servicios de red	Se debe identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.	A.13.1.2			Revisar las siguientes directrices para la seguridad de los servicios de red: a) establecer la tecnología aplicada a la seguridad de servicios de red, tales como autenticación, encriptación y controles de conexión de red; b) definir los parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de conexión de seguridad y de red; c) establecer los procedimientos para el uso de servicios de red para restringir el acceso a los servicios o aplicaciones de red, cuando sea necesario.			80		60	Para garantizar los servicios seguros de red se cuenta con dispositivos de seguridad perimetral SonicWall Firewall,
T.5.1.3	Responsable de TICs	Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	A.13.1.3		PR.AC-5 PR.DS-5	De acuerdo a NIST se debe proteger la integridad de las redes incorporando segregación donde se requiera.			100	Se recomienda actualizar el esquema de red de la entidad para tener en cuenta la implementación de IPV6	100	La red se encuentra devidamente segmentada
T.5.2	**Responsable de TICs**	**TRANSFERENCIA DE INFORMACIÓN**	**Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.**	**A.13.2**	Modelo de madurez definido					**25**		**10**	

										SEGUIMIENTO SEPTIEMBRE 2019		AUTODIAGNOSTICO MARZO 2018	
ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
T.5.2.1	Responsable de TICs	Políticas y procedimientos de transferencia de información	Se debe contar con politicas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.	A.13.2.1		ID.AM-3 PR.AC-5 PR.AC-3 PR.DS-2 PR.DS-5 PR.PT-4	De acuerdo a la NIST: Se deben mapear los flujos de comunicaciones y datos para poder cumplir con este ítem. Revisar las siguientes directrices: a) definir los procedimientos diseñados para proteger la información transferida contra interceptación, copiado, modificación, enrutado y destrucción; b) definir los procedimientos para la detección de software malicioso y protección contra éste, que puede ser transmitido mediante el uso de comunicaciones electrónicas; c) definir los procedimientos para proteger información electrónica sensible comunicada que están como adjuntos;			40	el Procedimiento de cifrado contiene las directrices para criptográficas y certificados digitales, se tiene una herramienta alternativa para cifrado de correo electronico.	0	Se debe implementar este procedimiento en la Unidad
T.5.2.2	Responsable de TICs	Acuerdos sobre transferencia de información	Los acuerdos deben tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.	A.13.2.2			Revisar las siguientes directrices para transferencia segura de la información: a) establecer las responsabilidades de la dirección para controlar y notificar la transmisión, despacho y recibo; b) definir los procedimientos para asegurar trazabilidad y no repudio; c) definir los estándares técnicos mínimos para empaquetado y transmisión; d) tener certificados de depósito de títulos en garantía; e) establecer los estándares de identificación de mensajería; f) definir las responsabilidades y obligaciones en el caso de incidentes de seguridad de la información, tales como pérdidas de datos; g) establecer el uso de un sistema de etiquetado acordado para información			20	No se evidencian lineamientos para la transferencia segura de información en medio fisico.	20	
T.5.2.3	Responsable de TICs	Mensajería electrónica	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	A.13.2.3		PR.DS-2 PR.DS-5	Revisar las siguientes directrices para mensajería electrónica: a) definir la protección de mensajes contra acceso no autorizado, modificación o denegación del servicio proporcionales al esquema de clasificación adoptado por la organización; b) asegurar el direccionamiento y transporte correctos del mensaje; c) establecer la confiabilidad y disponibilidad del servicio; d) definir las consideraciones legales, (los requisitos para firmas electrónicas; e) establecer la obtención de aprobación antes de usar servicios públicos externos como mensajería instantánea, redes sociales o intercambio de información); f) definir niveles más fuertes de autenticación para control del acceso desde redes accesibles públicamente.			20		0	No se tiene una directriz en cuanto a mensajeria electronica
T.5.2.4	Responsable de SI	Acuerdos de confidencialidad o de no divulgación	Se debe identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	A.13.2.4		PR.DS-5	Revisar las siguientes directrices para acuerdos de confidencialidad: a) definir la información que se va a proteger (información confidencial); b) determinar la duración esperada de un acuerdo, incluidos los casos en los que podría ser necesario mantener la confidencialidad indefinidamente; c) establecer las acciones requeridas cuando termina el acuerdo; d) definir las responsabilidades y acciones de los firmantes para evitar la divulgación no autorizada de información; e) definir la propiedad de la información, los secretos comerciales y la propiedad intelectual, y cómo esto se relaciona con la protección de información confidencial; f) definir el uso permitido de información confidencial y los derechos del firmante para usar la información; g) establecer el derecho a actividades de auditoría y de seguimiento que involucran información confidencial; h) definir el proceso de notificación y reporte de divulgación no autorizada o fuga de información confidencial; i) definir los plazos para que la información sea devuelta o destruida al cesar el acuerdo; j) establecer las acciones que se espera tomar en caso de violación del acuerdo.			20		20	Para el ingreso de nuevo personal provisional o de carrera, Talento Humano cubre este requerimiento mediante la ley 734 de 2002, art 34. Para contratista se enuncia en la minuta del contrato,
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS													
T.6	**Responsable de SI/Responsable de TICs**	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**		**A.14**						24		15	
T.6.1	**Responsable de SI**	**REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN**	**Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.**	**A.14.1**	Modelo de madurez definido					**40**		**20**	

										SEGUIMIENTO SEPTIEMBRE 2019		AUTODIAGNOSTICO MARZO 2018	
ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
T.6.1.1	Responsable de SI	Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados con seguridad de la información se debe incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	A.14.1.1		PR.IP-2	Revisar las siguientes directrices para análisis y especificaciones de requisitos de seguridad de la información: a) establecer el nivel de confianza requerido con relación a la identificación declarada de los usuarios, para obtener los requisitos de autenticación de usuario. b) definir los procesos de suministro de acceso y de autorización para usuarios del negocio, al igual que para usuarios privilegiados o técnicos; c) informar a los usuarios y operadores sobre sus deberes y responsabilidades; d) definir las necesidades de protección de activos involucrados, en particular acerca de disponibilidad, confidencialidad, integridad; e) definir los requisitos obtenidos de los procesos del negocio, tales como los requisitos de ingreso y seguimiento, y de no repudio; 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).			40		20	En el manual de seguridad de la información se incluye política para tener en cuenta en la seguridad de la información en la adquisición de nuevos sistemas de información, sin embargo la política no se está aplicando actualmente y no se han definido requisitos generales para abordar la seguridad de la información en nuevos sistemas de información.
T.6.1.2	Responsable de SI	Seguridad de servicios de las aplicaciones en redes públicas	La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	A.14.1.2		PR.DS-2 PR.DS-5 PR.DS-6	Revisar las siguientes directrices para la seguridad de servicios de las aplicaciones en redes públicas: a) definir el nivel de confianza que cada parte requiere con relación a la identidad declarada por la otra parte, (por medio de autenticación); b) establecer los procesos de autorización asociados con quien puede aprobar el contenido o expedir o firmar documentos transaccionales clave; c) asegurar que los socios de comunicación estén completamente informados de sus autorizaciones para suministro o uso del servicio; d) determinar y cumplir los requisitos para confidencialidad, integridad, prueba de despacho y recibo de documentos clave y el no repudio de los contratos, (asociados con procesos de ofertas y contratos); e) definir el nivel de confianza requerido en la integridad de los documentos clave; f) establecer los requisitos de protección de cualquier información confidencial; g) definir la confidencialidad e integridad de cualquier transacción de pedidos, información de pagos, detalles de la dirección de entrega y confirmación de recibos; h) definir el grado de verificación apropiado de la información de pago suministrada por un cliente; i) seleccionar la forma de arreglo de pago más apropiado para protegerse contra fraude; j) definir el nivel de protección requerido para mantener la confidencialidad e integridad de la información del pedido; k) evitar la pérdida o duplicación de información de la transacción; l) definir la responsabilidad civil asociada con cualquier transacción fraudulenta;			40		20	Para proteger la información de UAESP que transita por redes públicas se realizan escaneos de vulnerabilidades y parcheo, además se tiene dispositivos de seguridad perimetral. No se cuenta con una directriz
T.6.1.3	Responsable de SI	Protección de transacciones de los servicios de las aplicaciones	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	A.14.1.3		PR.DS-2 PR.DS-5 PR.DS-6	Revisar las siguientes directrices protección de transacciones de los servicios de las aplicaciones: a) definir el uso de firmas electrónicas por cada una de las partes involucradas en la transacción; b) establecer todos los aspectos de la transacción, es decir, asegurar que: 1) definir la información de autenticación secreta de usuario, de todas las partes, se valide y verifique; 2) definir a transacción permanezca confidencial; 3) mantener la privacidad asociada con todas las partes involucradas; c) definir la trayectoria de las comunicaciones entre todas las partes involucradas esté encriptada; d) definir los protocolos usados para comunicarse entre todas las partes involucradas estén asegurados; e) asegurar que el almacenamiento de los detalles de la transacción esté afuera de cualquier entorno accesible públicamente, (en una plataforma de almacenamiento existente en la intranet de la organización, y no retenido ni expuesto en un medio de almacenamiento accesible directamente desde Internet); f) utilizar una autoridad confiable (para los propósitos de emitir y mantener firmas digitales o certificados digitales), la seguridad está integrada e incluida en todo el proceso de gestión de certificados/firmas de un extremo a otro.			40	Se evidencia procedimiento de cifrado de información que indica los pasos y protocolos definidos por GTIC	0	No se tiene ninguna directriz acerca de cifrado todo el trafico que se encuentra en las redes no esta cifrado
T.6.2	**Responsable de SI**	**SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE**	**Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.**	**A.14.2**	Modelo de madurez definido					33		**4**	

											SEGUIMIENTO SEPTIEMBRE 2019		AUTODIAGNOSTICO MARZO 2018	
ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA		NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
T.6.2.1	Responsable de SI	Política de desarrollo seguro	Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.	A.14.2.1		PR.IP-2	Revisar las siguientes directrices política de desarrollo seguro: a) definir la seguridad del ambiente de desarrollo; b) orientar la seguridad en el ciclo de vida de desarrollo del software: 1) definir la seguridad en la metodología de desarrollo de software; 2) establecer las directrices de codificación seguras para cada lenguaje de programación usado; c) definir los requisitos de seguridad en la fase diseño; d) definir los puntos de chequeo de seguridad dentro de los hitos del proyecto; e) establecer los depósitos seguros; f) definir la seguridad en el control de la versión; g) establecer el conocimiento requerido sobre seguridad de la aplicación; h) definir la capacidad de los desarrolladores para evitar, encontrar y resolver las vulnerabilidades.			40	desarrollo seguro	0	
T.6.2.2	Responsable de TICs	Procedimientos de control de cambios en sistemas	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se debe controlar mediante el uso de procedimientos formales de control de cambios.	A.14.2.2		PR.IP-1 PR.IP-3	Revisar las siguientes directrices procedimientos control de cambio en sistemas: a) llevar un registro de los niveles de autorización acordados; b) asegurar que los cambios se presenten a los usuarios autorizados; c) revisar los controles y procedimientos de integridad para asegurar que no se vean comprometidos por los cambios; d) identificar todo el software, información, entidades de bases de datos y hardware que requieren corrección; e) identificar y verificar el código crítico de seguridad para minimizar la posibilidad de debilidades de seguridad conocidas; f) obtener aprobación formal para propuestas detalladas antes de que el trabajo comience; g) revisar antes de la implementación, asegurar que los usuarios autorizados aceptan los cambios; h) asegurar que el conjunto de documentación del sistema está actualizado al completar cada cambio, y que la documentación antigua se lleva al archivo permanente, o se dispone de ella; i) mantener un control de versiones para todas las actualizaciones de software; j) mantener un rastro de auditoría de todas las solicitudes de cambio; k) asegurar que la documentación de operación y los procedimientos de los usuarios experimenten los cambios que les permitan seguir siendo apropiados; l) asegurar que la implementación de los cambios ocurre en el momento correcto y no afecta los procesos de negocio involucrados.	Nist 800-6 instrtructivo de gestion proyectos		20	Se evidencia borrador de documento para la gestion de cambios que requiere ser completado para aprobacion y posterior implementacion	0	
T.6.2.3	Responsable de TICs	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	A.14.2.3		PR.IP-1	Revisar las siguientes directrices revisión técnica de las aplicaciones después de cambios en la plataforma de operación: a) revisar los procedimientos de integridad y control de aplicaciones para asegurar que no estén comprometidos debido a los cambios en las plataformas de operaciones; b) asegurar que la notificación de los cambios en la plataforma operativa se hace a tiempo para permitir las pruebas y revisiones apropiadas antes de la implementación; c) asegurar que se hacen cambios apropiados en los planes de continuidad del negocio.			20	Se evidencia borrador de documento para la gestion de cambios que requiere ser completado para aprobacion y posterior implementacion	0	
T.6.2.4	Responsable de TICs	Restricciones en los cambios a los paquetes de software	Se deben desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	A.14.2.4		PR.IP-1	Revisar las siguientes directrices restricciones en los cambios a los paquetes de software: a) definir el riesgo de que los procesos de integridad y los controles incluidos se vean comprometidos; b) obtener el consentimiento del vendedor; c) obtener del vendedor los cambios requeridos, a medida que se actualiza el programa estándar; d) evaluar el impacto, si la organización llega a ser responsable del mantenimiento futuro del software como resultado de los cambios; e) definir la compatibilidad con otro software en uso.			20	Se evidencia borrador de documento para la gestion de cambios que requiere ser completado para aprobacion y posterior implementacion	0	
T.6.2.5	Responsable de TICs	Principios de construcción de sistemas seguros	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	A.14.2.5		PR.IP-2	Revisar la documentación y los principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.			40	Se evidencia documento instructivo para gestion de proyecto que tiene alcance para pruebas de calidad y seguridad.	0	

										SEGUIMIENTO SEPTIEMBRE 2019		AUTODIAGNOSTICO MARZO 2018	
ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
T.6.2.6	Responsable de TICs	Ambiente de desarrollo seguro	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	A.14.2.6			Revisar las siguientes directrices para ambiente de desarrollo seguro: a) carácter sensible de los datos que el sistema va a procesar, almacenar y transmitir; b) definir los requisitos externos e internos aplicables, (reglamentaciones o políticas); c) definir los controles de seguridad ya implementados por la organización, que brindan soportar al desarrollo del sistema; d) establecer la confiabilidad del personal que trabaja en el ambiente; e) definir el grado de contratación externa asociado con el desarrollo del sistema; f) definir la necesidad de separación entre diferentes ambientes de desarrollo; g) definir el control de acceso al ambiente de desarrollo; h) establecer el seguimiento de los cambios en el ambiente y en los códigos almacenados ahí; i) definir las copias de respaldo se almacenan en lugares seguros fuera del sitio; j) definir el control sobre el movimiento de datos desde y hacia el ambiente.			40	Se evidencia documento instructivo para gestion de proyecto que tiene alcance para pruebas de calidad y seguridad.	0	
T.6.2.7	Responsable de TICs	Desarrollo contratado externamente	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	A.14.2.7		DE.CM-6	Revisar las siguientes directrices desarrollo contratado externamente: a) definir los acuerdos de licenciamiento, propiedad de los códigos y derechos de propiedad intelectual relacionados con el contenido contratado externamente; b) establecer los requisitos contractuales para prácticas seguras de diseño, codificación y pruebas; c) definir el suministro del modelo de amenaza aprobado, al desarrollador externo; d) realizar los ensayos de aceptación para determinar la calidad y exactitud de los entregables; e) definir la evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad; f) definir la evidencia de que se han hecho pruebas suficientes para proteger contra contenido malicioso intencional y no intencional en el momento de la entrega; g) definir la evidencia de que se han hecho pruebas suficientes para proteger contra la presencia de vulnerabilidades conocidas; h) definir los certificados de depósito de títulos en garantía: (el código fuente			40	Se evidencia documento instructivo para gestion de proyecto que tiene alcance para pruebas de calidad y seguridad.	0	
T.6.2.8	Responsable de SI	Pruebas de seguridad de sistemas	Durante el desarrollo se debe llevar a cabo pruebas de funcionalidad de la seguridad.	A.14.2.8	Modelo de madurez gestionado cuantitativamente	DE.DP-3	Verifique en una muestra que para pasar a producción los desarrollos se realizan pruebas de seguridad. También verifique que los procesos de detección de incidentes son probados periódicamente.			40	Se evidencia la ejecucion de pruebas automatizadas de seguirdad. Sin embargo, no se aplican a la totalidad de sistemas.	20	
T.6.2.9	Responsable de TICs	Prueba de aceptación de sistemas	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se debe establecer programas de prueba para aceptación y criterios de aceptación relacionados.	A.14.2.9			Revisar las pruebas de aceptación de sistemas, para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.			40	Se evidencia documento instructivo para gestion de proyecto que tiene alcance para pruebas de calidad y seguridad.	20	
T.6.3	Responsable de SI	**DATOS DE PRUEBA**	**Asegurar la protección de los datos usados para pruebas.**	**A.14.3**	Modelo de madurez definido					**0**		**20**	
T.6.3.1	Responsable de SI	Protección de datos de prueba	Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente.	A.14.3.1			Revisar las siguientes directrices para protección de datos de prueba: a) establecer los procedimientos de control de acceso, que se aplican a los sistemas de aplicación operacionales, se debe aplicar también a los sistemas de aplicación de pruebas; b) tener una autorización separada cada vez que se copia información operacional a un ambiente de pruebas; c) definir que la información operacional se debe borrar del ambiente de pruebas inmediatamente después de finalizar las pruebas; d) establecer que el copiado y uso de la información operacional se debe logged para suministrar un rastro de auditoría.			0	No se evidencia directrices para proteccion de datos en sistemas de prueba asi como las autorizaciones para borrado.	20	
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN													
T.7.	**Responsable de SI/Responsable de TICs**	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**		**A.16**						20		9	
T.7.1	**Responsable de SI**	**GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN**	**Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.**	**A.16.1**						**20**		**9**	

										SEGUIMIENTO SEPTIEMBRE 2019		AUTODIAGNOSTICO MARZO 2018	
ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
T.7.1.1	Responsable de SI	Responsabilidades y procedimientos	Se debe establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	A.16.1.1		PR.IP-9 DE.AE-2 RS.CO-1	Revisar las siguientes directrices responsabilidades y procedimientos: a) establecer las responsabilidades de gestión, para asegurar que los siguientes procedimientos se desarrollan y comunican adecuadamente dentro de la organización: 1) los procedimientos para la planificación y preparación de respuesta a incidentes; 2) los procedimientos para seguimiento, detección, análisis y reporte de eventos e incidentes de seguridad de la información; 3) los procedimientos para logging las actividades de gestión de incidentes; 4) los procedimientos para el manejo de evidencia forense; 5) los procedimientos para la valoración y toma de decisiones sobre eventos de seguridad de la información y la valoración de debilidades de seguridad de la información; 6) los procedimientos para respuesta, incluyendo aquellos para llevar el asunto a una instancia superior, recuperación controlada de un incidente y comunicación a personas u organizaciones internas y externas; b) establecer los procedimientos para asegurar que: 1) el personal competente maneje las cuestiones relacionadas con incidentes de seguridad de la información dentro de la organización; 2) se implemente un punto de contacto para la detección y reporte de incidentes de seguridad; 3) se mantengan contactos apropiados con las autoridades, grupos de interés o foros externos que manejen las cuestiones relacionadas con incidentes de seguridad de la información; c) definir el reporte de procedimientos debería incluir: 1) la preparación de formatos de reporte de eventos de seguridad de la información para apoyar la acción de reporte y ayudar a la persona que reporta a recordar todas las acciones necesarias en caso de un evento de			20	Se evidencia borrador para el manejo de incidentes de segurida, requiere ser complementado, para solicitar su aprobación y posterior implementación.	0	No se cuenta con un procedimiento relacionado con responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
T.7.1.2	Responsable de SI	Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información se debe informar a través de los canales de gestión apropiados, tan pronto como sea posible.	A.16.1.2	Modelo de madurez definido	DE.DP-4	Revisar las siguientes directrices reporte de eventos de seguridad de la información: a) establecer un control de seguridad ineficaz; b) definir la violación de la integridad, confidencialidad o expectativas de disponibilidad de la información; c) definir los errores humanos; d) definir las no conformidades con politicas o directrices; e) definir las violaciones de acuerdos de seguridad física; f) establecer los cambios no controlados en el sistema; g) definir mal funcionamiento en el software o hardware; h) definir violaciones de acceso. **Tenga en cuenta para la calificación:** 1) Si se elaboran informes de TODOS los incidentes de seguridad y privacidad de la información, TODOS están documentados e incluidos en el plan de mejoramiento continuo. Se definen los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro, están en 40. 2) Si los controles y medidas identificados para disminuir los incidentes fueron implementados, están en 60.			0	No se evidencia reportes de incidentes de seguridad ni de su impacto.	0	No se cuenta con un informe especifico en cuanto a los incidentes de seguridad de la informacion
T.7.1.3	Responsable de SI	Reporte de debilidades de seguridad de la información	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	A.16.1.3	Modelo de madurez definido	RS.CO-2	Observe si los eventos son reportados de forma consistente en toda la entidad de acuerdo a los criterios establecidos.			20	Se observa que los reportes de incidentes no son significativos en terminos de cantidad. Sin embargo, no es posible afirmar que los pocos reportes se deban a que no se presentan incidentes de seguridad. Se sugiere sensibilizar a funcionarios y contratistas acerca del Rol de responsable de seguridad de la información	20	
T.7.1.4	Responsable de SI	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Los eventos de seguridad de la información se debe evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	A.16.1.4	Madurez Inicial	DE.AE-2 RS.AN-4	Revise si los eventos de SI detectados son analizados para determinar si constituyen un incidentes de seguridad de la información y entender los objetivos del ataque y sus métodos. Evidencia si los incidentes son categorizados y se cuenta con planes de respuesta para cada categoría.			60	Se evidencia reporte de incidente de seguridad , contratista afirma exposición de sus datos personales en la plataforma SECOP. No se evidencia una categorización de incidentes.	0	No se cuenta con una directriz firmada por la alta Direccion donde se haga referencia.

										SEGUIMIENTO SEPTIEMBRE 2019		AUTODIAGNOSTICO MARZO 2018	
ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
T.7.1.5	Responsable de SI	Respuesta a incidentes de seguridad de la información	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	A.16.1.5	Modelo de madurez gestionado cuantitativamente	RS.RP-1 RS.AN-1 RS.MI-2 RC.RP-1 RC.RP-1	Revisar las siguientes directrices para respuesta a incidentes de seguridad de la información: a) Los incidentes son contenidos y la probabilidad de que vuelvan a ocurrir mitigada. b) Se debe contar con un plan de recuperación de incidentes durante o después del mismo. b) recolectar evidencia lo más pronto posible después de que ocurra el incidente; c) llevar a cabo análisis forense de seguridad de la información, según se requiera d) llevar el asunto a una instancia superior, según se requiera; e) asegurar que todas las actividades de respuesta involucradas se registren adecuadamente para análisis posterior; f) comunicar la existencia del incidente de seguridad de la información o de cualquier detalle pertinente a él, al personal interno o externo a las organizaciones que necesitan saberlo; g) tratar las debilidades de seguridad de información que se encontraron que causan o contribuyen al incidente; g) establecer que una vez que el incidente se haya tratado lo suficiente, cerrarlo formalmente y hacer un registro de esto. h) de acuerdo a la NIST se deben investigar las notificaciones de los sistemas de detección. **Tenga en cuenta para la calificación:** 1) Si los planes de respuesta a incidentes incluyen algunas áreas de la entidad y si se evalúa la efectividad los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro es 60 2) Se incluyan todas las áreas de la Entidad en los planes de respuesta de			20	Se evidencia borrador para el manejo de incidentes de segurida, requiere ser complementado, para solicitar su aprobación y posterior implementación.	20	No se cuenta con procedimientos documentados acerca de respuesta a incidentes de seguridad de la informacion.
T.7.1.6	Responsable de TICs	Aprendizaje obtenido de los incidentes de seguridad de la información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	A.16.1.6	Modelo de madurez gestionado cuantitativamente	DE.DP-5 RS.AN-2 RS.IM-1	De acuerdo a la NIST se debe entender cual fue el impacto del incidente. Las lecciones aprendidas deben ser usadas para actualizar los planes de respuesta a los incidentes de SI. **Tenga en cuenta para la calificación:** La Entidad aprende continuamente sobre los incidentes de seguridad presentados.			20	No se evidencia una recopilación que permita concluir que se adquiere conocimiento para reducir el impacto de incidentes de segurida futuros	20	Se tiene contacto con el colcert para cualquier incidente informatico reportarlo y tomar conciencia para incidentes futuros y como actuar ante nuevas amenazas y tomar correctivos.
T.7.1.7	Responsable de TICs	Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	A.16.1.7	Modelo de madurez gestionado Modelo de madurez definido	RS.AN-3	Revisar las siguientes directrices para recolección de evidencia: a) definir la cadena de custodia; b) establecer la seguridad de la evidencia; c) definir la seguridad del personal; d) definir los roles y responsabilidades del personal involucrado; e) establecer la competencia del personal; f) realizar la documentación; g) definir las sesiones informativas.			0	No se evidencian lineamientos para recoleccion de evidencias	0	No se cuenta con una directriz para recoleccion de evidencias

										SEGUIMIENTO SEPTIEMBRE 2019		AUTODIAGNOSTICO MARZO 2018	
COMPONENTE	ID	CARGO	ITEM	DESCRIPCIÓN	PRUEBA	NUMERAL ISO 27001	MSPI	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A	RECOMENDACIÓN	NIVEL DE CUMPLIMIENTO ANEXO A	RECOMENDACIÓN
PLANIFICACIÓN	P.1	Responsable SI	Alcande MSPI (Modelo de Seguridad y Privacidad de la Información)	Se debe determinar los límites y la aplicabilidad del SGSI para establecer su alcance.	Solicite el documento del alcance que debe estar aprobado, socializado al interior de la Entidad, por la alta dirección. Determine si en la definición del alcance se consideró: 1) Aspectos internos y externos referidos en el 4.1.: La Entidad debe determinar los aspectos externos e internos que son necesarios para cumplir su propósito y que afectan su capacidad para lograr los resultados previstos en el SGSI. Nota. La terminación de estos aspectos hace referencia a establecer el contexto interno y externo de la empresa, referencia a la norma ISO 31000:2009 en el apartado 5.3. 2) Los requisitos referidos en 4.2.: a. Se debe determinar las partes interesadas que son pertinentes al SGSI. b. Se debe determinar los requisitos de las partes interesadas. Nota. Los requisitos pueden incluir los requisitos legales y de reglamentación y las obligaciones contractuales. 3) Las interfaces y dependencias entre las actividades realizadas y las que realizan otras entidades del gobierno nacional o entidades exteriores	4.1 , 4.2, 4.3	componente planificación			40	Se evidencia como parte del SGSI sin embargo, la política, objetivos y alcance del SGI de la UAESP no contempla los requisitos mínimos de los sistemas que integra.	40	Se tiene planteado el documento pero no esta socializado ni firmado por alta direccion
	P.2		Políticas de seguridad y privacidad de la información	Se debe definir un conjunto de políticas para la seguridad de la información aprobada por la dirección, publicada y comunicada a los empleados y a la partes externas pertinentes	Solicite la política de seguridad de la información de la entidad y evalúe: a) Si se definen los objetivos, alcance de la política b) Si esta se encuentra alineada con la estrategia y objetivos de la entidad c) Si fue debidamente aprobada y socializada al interior de la entidad por la alta dirección Revise si la política: a)Define que es seguridad de la información b) La asignación de las responsabilidades generales y específicas para la gestión de la seguridad de la información, a roles definidos; c) Los procesos para manejar las desviaciones y las excepciones. Indague sobre los responsables designados formalmente por la dirección para desarrollar, actualizar y revisar las políticas. Verifique cada cuanto o bajo que circunstancias se revisan y actualizan, verifique la ultima fecha de emisión de la política frente a la fecha actual y que cambios a sufrido, por lo menos debe haber una revisión anual. Para la calificación tenga en cuenta que: 1) Si se empiezan a definir las políticas de seguridad y privacidad de la información basada en el Modelo de Seguridad y Privacidad de la Información, están en 20. 2) Si se revisan y se aprueban las políticas de seguridad y privacidad de la información, , están en 40. 3) Si se divulgan las políticas de seguridad y privacidad de la información, están en 60.	5.1, 5.2, 5.3, 6.2	componente planificación			60	Cuenta con los elementos señalados esta pendiente por aprobación mediante Resolución	40	Políticas de Seguridad de la Información Se crea el Comité de Seguridad de la Información y Gobierno Digital (Resolución 696 de 2017)
										60	Se debe establecer una periodicidad para la revisión y posibles actualizaciones de las políticas relacionadas con	40	0
	P.3	Calidad	Procedimientos de control documental del MSPI	La información documentada se debe controlar para asegurar que: a. Esté disponible y adecuado para su uso, cuando y donde se requiere b. Esté protegida adecuadamente.	Solicite Formatos de procesos y procedimienos debidamente definidos, establecidos y aprobados por el comité que integre los sistemas de gestión institucional, por ejemplo el sistema de calidad SGC. Verifique: 1) Cómo se controla su distribución, acceso, recuperación y uso 2) Cómo se almacena y se asegura su preservación 3) Cómo se controlan los cambios	7.5.1, 7.5.2, 7.5.3	componente planificación			40	Se disponen y son accesibles mediante el micrositio del MTO de la UAESP. Su control se establece mediante el procedimiento del proceso de direccionamiento estratégico. Sin embargo se evidenciaron debilidades en versionamiento y actualizacion del formato de listado maestro de documentos.	20	
	P.4	Responsable SI	Roles y responsabilidades para la seguridad de la información	Se deben definir y asignar todas las responsabilidades de la seguridad de la información	Solicite el acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (ó e que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección. Revise la estructura del SGSI: 1) Tiene el SGSI suficiente apoyo de la alta dirección?, esto se ve reflejado en comités donde se discutan temas como la política de SI, los riesgos o incidentes. 2) Están claramente definidos los roles y responsabilidades y asignados a personal con las competencias requeridas?, 3) Están identificadas los responsables y responsabilidades para la protección de los activos? (Una práctica común es nombrar un propietario para cada activo, quien entonces se convierte en el responsable de su protección) 4)Estan definidas las responsabilidades para la gestión del riesgo de SI y la aceptación de los riesgos residuales? 5) Estan definidos y documentados los niveles de autorización? 6) Se cuenta con un presupuesto formalmente asignado a las actividades del SGSI (por ejemplo campañas de sensibilización en seguridad de la información)	5.3, 6.2	componente planificación			60	Mediante Acta de comité de seguridad de la información de 26/08/2019 se aprueba el rol de responsable de seguridad de la información de la entidad. Es importante definir las responsabilidades especificas de terceras partes y su relación con los activos de información EJ. Empresa de seguridad privada	20	De acuerdo a la Resolución 696 de 2017 se creo el comité de Seguridad y Gobierno Digital, el cual define las funciones y responsabilidades de cada integrante del comité. La Entidad ya cuenta con un profesional el cual es el responsable de seguridad de la información
	P.5	Responsable SI	Inventario de activos	Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	Solicite el inventario de activos de información, revisado y aprobado por la alta Dirección y revise: 1) Ultima vez que se actualizó 2) Que señale bajo algún criterio la importancia del activo 3) Que señale el propietario del activo Indague quien(es) el(los) encargado(s) de actualizar y revisar el inventario de activos y cada cuanto se realiza esta revisión. De acuerdo a NIST se deben considerar como activos el personal, dispositivos, sistemas e instalaciones físicas que permiten a la entidad cumplir con su misión y objetivos, dada su importancia y riesgos estratégicos. Tenga en cuenta para la calificación: 1) Si Se identifican en forma general los activos de información de la Entidad, están en 40. 2) Si se cuenta con un inventario de activos de información física y lógica de toda la entidad, documentado y firmado por la alta dirección, están en 60. 3) Si se revisa y monitorean periódicamente los activos de información de la entidad, están en 80.	6.1.2	componente planificación			60	Se evidencia que el documento se encuentra en ajuste ya que el vigente no da alcance a la clasificación de activos desde la parte técnica de TI y no permitia la valoración del riesgo asociado al activo.	40	0

										SEGUIMIENTO SEPTIEMBRE 2019		AUTODIAGNOSTICO MARZO 2018	
COMPONENTE	ID	CARGO	ITEM	DESCRIPCIÓN	PRUEBA	NUMERAL ISO 27001	MSPI	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A	RECOMENDACIÓN	NIVEL DE CUMPLIMIENTO ANEXO A	RECOMENDACIÓN
	P.6	Responsable SI	Identificación y valoración de riesgos	Metodología de análisis y valoración de riesgos e informe de análisis de riesgos	1) Solicite a la entidad la metodología y criterios de riesgo de seguridad, aprobado por la alta Dirección que incluya: 1. Criterios de Aceptación de Riesgos o tolerancia al riesgo que han sido informados por la alta Dirección. 2. Criterios para realizar evaluaciones de riesgos. 2) Solicite los resultados de las evaluaciones de riesgos y establezca: a. Cuantas evaluaciones repetidas de riesgos se han realizado y que sus resultados consistentes, validos y comparables. b. Que se hayan identificado los riesgos asociados con la pérdida de la confidencialidad, de integridad y de disponibilidad de la información dentro del alcance. c. Que se hayan identificado los dueños de los riesgos. d. Que se hayan analizado los riesgos es decir: - Evaluado las consecuencias (impacto) potenciales si se materializan los riesgos identificados - Evaluado la probabilidad realista de que ocurran los riesgos identificados - Determinado los niveles de riesgo. e. Que se hayan evaluado los riesgos es decir: - Comparado los resultados del análisis de riesgos con los criterios definidos - Priorizado los riesgos analizados para el tratamiento de riesgos.	6.1.1, 6.1.2	componente planificación			40	Se evidencia que la nueva metodologia de gestión de riesgos la cual da alcance a la gestion de riesgos de seguridad de la información, se encuentra en tramite de aprobación por lo cual aun no es una versión oficial, para integrarse a IMTO	0	
	P.8	Responsable SI	Tratamiento de riesgos de seguridad de la información	Los riesgos deben ser tratados para mitigarlos y llevarlos a niveles tolerables por la Entidad	1) Solicite el plan de tratamiento de riesgos y la declaración de aplicabilidad verifique que: a. Se seleccionaron opciones apropiadas para tratar los riesgos, teniendo en cuenta los resultados de la evaluación de riesgos. b. Se determinaron todos los controles necesarios para implementar las opciones escogidas para el tratamiento de riesgos. c. Compare los controles determinados en el plan de tratamiento con los del Anexo A y verifique que no se han omitidos controles, si estos han sido omitidos se debe reflejar en la declaración de aplicabilidad. d. Revise la Declaración de Aplicabilidad que tenga los controles necesarios y la justificación de las exclusiones, ya sea que se implementen o no y la justificación para las exclusiones de los controles del Anexo A, y que haya sido revisado y aprobado por la alta Dirección. e. Revise que el plan de tratamiento de riesgos haya sido revisado y aprobado por la alta Dirección. f. Revise que exista una aceptación de los riesgos residuales por parte de los dueños de los riesgos.	6.1.3	Modelo de Seguridad y Privacidad de la Información, componente planificación			20	Se debe actualizar el conjunto de controles ante los riesgos identificados pues se evidencia que algunos de los controles estan alineados a sistemas que actualmente no administra la UAESP.	20	
	P.9	Responsable SI	Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados de la Entidad, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	Entreviste a los líderes de los procesos y pregúnteles que saben sobre la seguridad de la información, cuales son sus responsabilidades y como aplican la seguridad de la información en su diario trabajo. Pregunte como se asegura que los funcionarios, Directores, Gerentes y contratistas tomen conciencia en seguridad de la información, alineado con las responsabilidades, políticas y procedimientos existentes en la Entidad. Solicite el documento con el plan de comunicación, sensibilización y capacitación, con los respectivos soportes, revisado y aprobado por la alta Dirección. Verifique que se han tenido en cuenta buenas prácticas como: a) Desarrollar campañas, elaborar folletos y boletines. b) Los planes de toma de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, están aprobados y documentados, por la alta Dirección c) Verifique que nuevos empleados y contratistas son objeto de sensibilización en SI. d) Indague cada cuanto o con que criterios se actualizan los programas de toma de conciencia. e) Verifique que en las evidencias se puede establecer los asistentes al programa y el tema impartido. f) Incluir en los temas de toma de conciencia los procedimientos básicos de seguridad de la información (tales como el reporte de incidentes de seguridad de la información) y los controles de linea base (tales como la seguridad de las contraseñas, los controles del software malicioso, y los escritorios limpios). g) De acuerdo a NIST verifique que los funcionarios con roles privilegiados entienden sus responsabilidades y roles. Para la calificación tenga en cuenta que: Si Los funcionarios de la Entidad no tienen conciencia de la seguridad y privacidad de la información. Diseñar programas para los conciencia y comunicación de las políticas de seguridad y	7.3, 7.4	componente planificación			20	No se evidencia claridad frente a las responsabilidades sel SGSI de los lideres de los procesos	60	
	P.10	Responsable de TICs	Plan y Estrategia de transisición de IPv4 a IPv6	Las razones de que se requiera el cambio del protocolo de V4 a V6, se resumen a continuación: 1) Debido al aumento de la utilización de las redes de telecomunicaciones las direcciones de internet que permiten establecer conexiones para cada elementos conectado a la red, conocidas como direciones IP (Internet Protocol Versión 4), han entrado en una fase de agotamiento. 2) Mejora de la seguridad de la red en virtud de la arquitectura del nuevo protocolo y sus servicio. En esta etapa se requiere hacer un diagnóstico que ayude a definir el plan y la estrategia para la transición entre los dos protocolos.	Verifique: 1) El Inventario de TI (Hardware, software) levantado 2) El análisis de la infraestructura actual de red de comunicaciones, recomendaciones para adquisición de elementos de comunicaciones, cómputo y almacenamiento, compatibles con el protocolo IPv6 3) El Protocolo de pruebas de validación de aplicativos, comunicaciones y bases de datos, el plan de seguridad y coexistencia de los protocolos. Plan de manejo de excepciones e informe de preparación de los sistemas de comunicaciones, bases de datos y aplicaciones. 4) El Plan de trabajo para la transición de los servicios tecnológicos de la Entidad de IPv4 a IPv6 5) La validación de estado actual de los sistemas de información y comunicaciones y la interfaz entre ellos y revisión de los RFC correspondientes. 6) La identificación de esquemas de seguridad de la información y seguridad de los sistemas de comunicaciones 7) Plan de capacitación en IPv6 a los funcionarios de las Áreas de TI de las Entidades y plan de sensibilización al total de funcionarios de las Entidades.		componente planificación			60	Se evidencian rezagos en la implementación según PAI	40	Existe levantamiento de informacion con respecto a la transicion de ipv4 a ipv6 en la Entidad
PROMEDIO										46	18,4	32	12,8
	I.1	Responsable SI	Planificación y control operacional	Estrategia que se debe ejecutar con las actividades para lograr la implementación y puesta en marcha del MSPI de la entidad.	Solicite y evalue el documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	6.1.1	componente implementación			60	Se evidencia documento de plan operacional del MSPI sin embargo el documento no contiene fechas establecidad que permitan determinarcon claridad el grado de avance en la implementación	0	
	I.2	n/a	Implementación de controles	Grado de implementación de controles del Anexo A de la ISO 27001	N/A		componente implementación		N/A	47	N/A	32	N/A

										SEGUIMIENTO SEPTIEMBRE 2019		AUTODIAGNOSTICO MARZO 2018	
COMPONENTE	ID	CARGO	ITEM	DESCRIPCIÓN	PRUEBA	NUMERAL ISO 27001	MSPI	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A	RECOMENDACIÓN	NIVEL DE CUMPLIMIENTO ANEXO A	RECOMENDACIÓN
IMPLEMENTACIÓN	I.3	Responsable SI	Implementación del plan de tratamiento de riesgos	Porcentaje de avance en la ejecución de los planes de tratamiento	Verifique los compromisos de avance en el plan de tratamiento de riesgos y el grado de cumplimiento de los mismos y genere un dato con el porcentaje de avance.	8.3	componente implementación			20	No se evidencia soporte de establecimiento o ejecucion de la actividad	0	
	I.4	Responsable de TICs	Implementación del plan de estrategia de transición de IPv4 a IPv6	Porcentaje de avance en la ejecución de la de estrategia de transición de IPv4 a IPv6	Verifique: 1) De acuerdo al informe de plan detallado de implementación del nuevo protocolo la Habilitación direccionamiento IPv6 para cada uno de los componentes de hardware y software. 2) Solicite el documento con todas las configuraciones del del nuevo protocolo realizadas y revise: a. La Configuración de servicios de DNS, DHCP, Seguridad, VPN, servicios WEB, b. La Configuración del protocolo IPv6 en Aplicativos, Sistemas de Comunicaciones, Sistemas de Almacenamiento. 3) La activación de políticas de seguridad de IPv6 en los equipos de seguridad y comunicaciones que posea cada entidad de acuerdo con los RFC de seguridad en IPv6. 4) La forma como se realizó la coordinación con el (los) proveedor (es) de servicios de Internet para lograr la conectividad integral en IPv6 hacia el exterior. 5) El Informe de resultados de las pruebas realizadas a nivel de comunicaciones, de aplicaciones y sistemas de almacenamiento.		componente implementación			60	En revisión del documento "Informe de migración IPV4-IPV6" se evidencia que corresponde al plan de transición IPV4-IPV6, allí se consignó un conjunto de actividades/entregables para las FASES I,II y III que son Diagnostico, implementacion y pruebas respectivamente, se observa que no se definieron fechas especificas para completar estas actividades. Así las cosas, no es posible determinar cuales actividades se desarrollan de maneja secuencial o cuales de ellas se desarrollan de manera paralela. Se observa que el documento "Cronograma de pruebas de implementación" se encuentra incompleto en varias de sus columnas como por ejemplo: Inicio de pruebas, Servidor, responsable técnico, responsable soporte ente otras. En general los informes	0	
	I.5	Responsable SI	Indicadores de gestión del MSPI	Indicadores de gestión del MSPI definidos	Solicite los Indicadores de gestión del MSPI definidos, revisados y aprobados por la alta Dirección.	9.1	componente implementación			0	No se evidencia soporte de establecimiento o ejecucion de la actividad	0	
PROMEDIO										37,48	7,495714286	6,3	1,26
EVALUACIÓN DE DESEMPEÑO	E.1	Responsable SI	Plan de seguimiento, evaluación y análisis del MSPI	Plan para evaluar el desempeño y eficacia del MSPI a través de instrumentos que permita determinar la efectividad de la implantación del MSPI.	Solicite y evalue el documento con el plan de seguimiento, evaluación, análisis y resultadosdel MSPI, revisado y aprobado por la alta Dirección.	9.1	componente evaluación del desempeño			0	No se evidencia soporte de establecimiento o ejecucion de la actividad	0	
	E.2	Control Interno	Auditoría Interna	Plan de auditoría interna	Documento con el plan de auditorías internas y resultados, de acuerdo a lo establecido en el plan de auditorías, revisado y aprobado por la alta Dirección.	9.2	componente evaluación del desempeño			0	No se evidencia soporte de establecimiento o ejecucion de la actividad	0	
	E.3	Responsable SI	Evaluación del plan de tratamiento de riesgos	Evaluación y seguimiento a los compromisos establecidos para ejecutar el plan de tratamiento de riesgos.	Resultado del seguimiento, evaluación y análisis del plan de tratamiento de riesgos, revisado y aprobado por la alta Dirección.	9.1	componente evaluación del desempeño			0	No se evidencia soporte de establecimiento o ejecucion de la actividad	0	
PROMEDIO										0	0	0	0
MEJORA CONTINUA	M.1	Responsable SI	Plan de seguimiento, evaluación y análisis del MSPI	Resultados consolidados del componente evaluación de desempeño	Solicite y evalue el documento con el plan de seguimiento, evaluación y análisis para el MSPI, revisado y aprobado por la alta Dirección.	8.3, 9.1	componente mejora continua			0	No se evidencia soporte de establecimiento o ejecucion de la actividad	0	
	M.2	Control Interno	Auditoría Interna	Comunicación delos resultados y plan para subsanar los hallazgos y oportunidades de mejora.	Solicite el documento con el consolidado de las auditorías realizadas de acuerdo con el plan de auditorías, revisado y aprobado por la alta dirección y verifique como se asegura que los hallazgos, brechas, debilidades y oportunidaes de mejora se subsanen, para asegurar la mejora continua. **Tenga en cuenta para la calificación que:** 1) Elaboración de planes de mejora es 60 2) Se implementan las acciones correctivas y planes de mejora es 80	9.2	componente mejora continua			0	La OCI realiza auditorias deacuerdo al plan anual de auditorias.	0	0
PROMEDIO										0	0	0	0