**INSTITUTO PARA LA INVESTIGACIÓN EDUCATIVA Y EL DESARROLLO**

**PEDAGOGICO – IDEP**

**INFORME DE AUDITORIA AL PROCESO DE GESTIÓN TECNOLÓGICA**

**OFICINA DE CONTROL INTERNO**

**Bogotá, D.C. Noviembre de 2020.**

1. **OBJETIVO 4**
2. **ALCANCE 4**
3. **CRITERIOS DE AUDITORIA 4**
4. **METODOLOGIA 4** 
   1. **PRESENTACIÓN DE RESULTADOS 5**
5. **RESULTADOS DEL SEGUIMIENTO Y EVALUACIÓN 6** 
   1. **PLANEACIÓN Y ORGANIZACIÓN DE LA GESTIÓN TIC 7** 
      1. GESTIÓN ESTRATÉGICA DE TI 7
         1. Seguimiento a Recomendaciones 2019 18 5.1.1.2 Nuevas Recomendaciones 2020 22
      2. ESTRUCTURA ORGANIZACIONAL Y GOBIERNO DE TI 24 5.1.2.1 Seguimiento a Recomendaciones 2019 31 5.1.2.2 Nuevas Recomendaciones 2020 33
      3. PLAN DE ADMINISTRACIÓN DE RIESGOS Y CONTINGENCIAS 34 5.1.3.1 Administración y tratamiento de Riesgos 34
         1. Plan de Continuidad 37
         2. Procedimientos de Backup y Recuperación 41
         3. Seguimiento a Recomendaciones 2019 43 5.1.3.5 Nuevas Recomendaciones 2020 45
      4. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 45 5.1.4.1 Seguimiento a Recomendaciones 2019 53 5.1.4.2 Nuevas Recomendaciones 2020 53
   2. **ADMINISTRACIÓN DE ACCESOS Y SEGURIDAD LÓGICA 55** 
      1. SEGURIDAD DE LA RED 55 5.2.1.1 Pruebas de seguridad 66
      2. SEGURIDAD SERVICIOS DE CORREO 67 5.2.3 SEGURIDAD DE INTERNET Y PC ´S 69
      3. SEGURIDAD DE ARCHIVOS FUENTES Y DOCUMENTOS 72
      4. GESTIÓN DE ACCESOS 72
      5. SEGUIMIENTO A RECOMENDACIONES 2019 74
   3. **DESARROLLO Y ADQUISICIÓN DE SOFTWARE APLICATIVO 79** 
      1. SEGUIMIENTO A RECOMENDACIONES 2019 84
      2. NUEVAS RECOMENDACIONES 2020 85
   4. **ADMINISTRACIÓN DE RECURSOS DE TI 86** 
      1. INVENTARIOS DE ACTIVOS Y MANTENIMIENTO DE HARDWARE Y SOFTWARE 86
         1. Seguimiento a Recomendaciones 2019 88
         2. Nuevas Recomendaciones 2020 89
      2. HELP DESK 89
         1. Seguimiento a Recomendaciones 2019 91
         2. Nuevas Recomendaciones 2020 92
6. **CONCLUSIONES DE AUDITORÍA: 93**
7. **RECOMENDACIONES 93**

# 1 OBJETIVO

Prestación de servicios profesionales para apoyar las actividades a realizar en la auditoria al proceso de gestión tecnológica

# 2 ALCANCE

Controles generales de la gestión tecnología con respecto a los escenarios:

* Planeación Estratégica del proceso.
* Desarrollo y adquisición de software aplicativo
* Administración de datos y seguridad lógica • Administración de recursos de TI.

# 3 CRITERIOS DE AUDITORIA

* PRO-GT-12-05 Mantenimiento de Infraestructura Tecnológica
* PRO-GT-12-07 Registro de Activos de Información tipo Software, Hardware y Servicios
* PRO-GT-12-08 Formulación y Seguimiento al PETIC
* PRO-GT-12-10 Mesa de Servicios
* Referencia Manual de Gobierno Digital V7 2019

# 4 METODOLOGIA

La auditoría se ejecutó conforme a lo establecido por la entidad en sus Procedimientos de Auditorías Internas con el apoyo en algunos lineamientos y buenas prácticas del Manual para la Implementación de la Política de Gobierno Digital Versión 7 abril de 2019

Para efectos de la auditoría se revisan los controles generales de los escenarios planteados en el alcance, junto con la revisión de la configuración de controles en la plataforma tecnológica del IDEP.

La auditoría de controles generales no corresponde a una auditoría de cumplimiento del sistema de gestión de calidad, por lo tanto, se da reconocimiento a los instrumentos y procedimientos aplicados por la OAP para la gestión y operación de servicios tecnológicos sin condicionamiento de que dichos instrumentos o procedimientos sean documentos controlados del sistema de gestión.

Las actividades realizadas son las siguientes:

1. Entrevistas con los responsables de procesos, proyectos o gestión de activos TIC.
2. Levantamiento de información documental como evidencia de planeación, ejecución, seguimiento y acciones de mejora.
3. Inspección remota y captura de evidencias de la configuración de activos de la plataforma TIC.
4. Análisis documental y de evidencias.
5. Identificación de oportunidades de mejora, elaboración de informe y emisión de recomendaciones.

El área que suministro la información es el proceso de Tecnología de la Información y Comunicaciones

La auditoría fue ejecutada de acuerdo a la siguiente línea de tiempo



## 4.1 Presentación de Resultados

Considerando que el alcance de la auditoría contempla el seguimiento a las recomendaciones del informe de auditoría contrato 026 de 2019, la estructura del presente informe para cada dominio del alcance incluye los siguientes elementos:



**Observaciones**: Corresponden a los aspectos positivos (fortalezas) y negativos (debilidades) identificadas para el proceso de Gestión de Tecnología de Información y las Comunicaciones. Se utiliza la siguiente nomenclatura:  Observación Positiva.

Observación positiva con opción de mejora. Observación negativa que amerita una acción de mejora.



 **Recomendaciones:** Corresponde a las oportunidades de mejora que deben ser atendidas por el proceso de TI en respuesta a los hallazgos negativos o debilidades identificados en el ejercicio de la auditoría y que son la fuente para determinar y priorizar las acciones de mejoramiento. Vale aclarar que los hallazgos positivos no derivan en recomendaciones. Incluye dos elementos:

* **Seguimiento a las recomendaciones**: corresponde a los resultados el seguimiento a las acciones de mejoramiento implementadas por la OAP en respuesta a cada una de las recomendaciones emitidas en el informe de auditoría contrato 026 de 2019.

* **Nuevas recomendaciones**: corresponde a nuevas oportunidades de mejora identificadas en la presente auditoría y aquellas que no han sido atendidas y requieren de acciones de mejoramiento.

En los capítulos correspondientes a pruebas de seguridad técnicas se incluyen imágenes de evidencia.

# 5 RESULTADOS DEL SEGUIMIENTO Y EVALUACIÓN

A continuación, se presenta para cada dominio del alcance de auditoría, la conclusiones, observaciones y recomendaciones de mejora.

## 5.1 Planeación y Organización de la Gestión TIC

### 5.1.1 Gestión Estratégica de TI

 El PLAN ESTRATÉGICO DE DESARROLLO INSTITUCIONAL PEDI 2016-2020, ha

establecido la meta: *Sostener 100 % la implementación del Sistema integrado de Gestión SIG -MIPG (Meta 2016-2018)*, que conforme al documento “*Políticas del Sistema Integrado de*

*Gestión y subsistemas asociados” PO-MIC-03-01” incluye el “Subsistema de Gestión de Seguridad de la Información*”, por su parte el seguimiento al PEDI (*Seguimiento\_JULIO\_PEDI\_2020.xlsx*) reporta para la meta señalada que se han implementado los 7 Subsistemas que conforman el SIG, dando cumplimiento a la meta, sin embargo, a la fecha no se encuentra implementado el Sistema de Gestión de Seguridad de la información conforme a lo dispuesto en el Modelo de Seguridad y privacidad de la Información (en adelante MSPI) que es parte integral de las Políticas de Gobierno digital y Seguridad Digital del MIPG. Las observaciones al respecto se emiten en el numeral 5.1.4 de este informe.

 De igual manera, el seguimiento PEDI, reporta que de acuerdo al decreto 612 de 2018, en el primer trimestre se formularon y aprobaron en el Comité Institucional de Gestión y Desempeño los 12 planes institucionales, de los que hacen parte integral los planes: *10. Plan*

*Estratégico de Tecnologías de la Información y las Comunicaciones • PETI, 11. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y 12. Plan de Seguridad y Privacidad de la Información*, sin embargo el proceso de Gestión TIC no ha adelantado la identificación, ni incluido en los planes la correlación que se espera entre los Planes institucionales .Para facilitar esta articulación, el MINTIC emitió en julio de 2019 nuevas directrices en la *G.ES.06 Guía para la construcción del PETI versión 2*, que incorpora una metodología y se actualiza el contenido para la construcción del PETI con un enfoque de Arquitectura en la planeación de la Tecnología para la Transformación Digital. Es importante anotar que las 4 fases involucran a todas las áreas de la entidad como parte de la articulación del PETI. El siguiente es un ejemplo de correlación:

**Planes OTIC 7. Plan Estratégico de 8. Plan de Tratamiento de 9. Plan de Seguridad y**

**Tecnologías de la Riesgos de Seguridad y Privacidad de la Información.**

**Información y las Privacidad de la Información.**

**Otros Planes de la Entidad Comunicaciones – PETI.**

Riesgos de activos de

información tipo "personas" Dominio A6. Aspectos

Organizativos de seguridad de

**Plan Estratégico de Talento** Dominio de Uso y que son críticos para la

la información.

**Humano.** Apropiación operación o tienen

Dominio A7 Seguridad ligada a

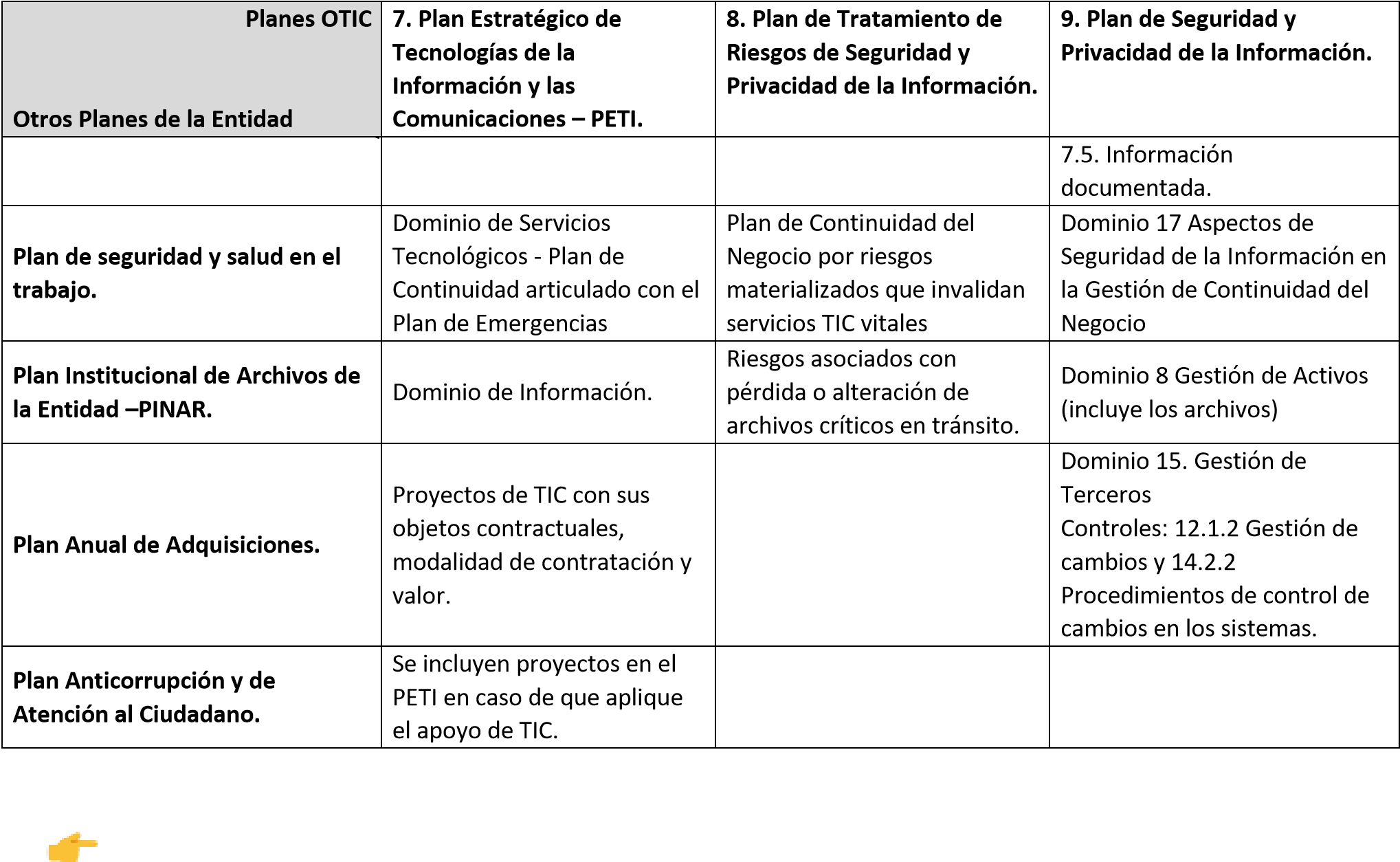
conocimiento especifico no los recursos Humanos trasferido.

Trasferencia de conocimiento Clausula 7. SOPORTE.

Dominio de Uso y como tratamiento del riesgo 7.1. Recursos

**Plan de Capacitación.** Apropiación de dependencia de 7.2. Competencia.

Gestión del Conocimiento conocimiento entre actores 7.3. Toma de conciencia, 7.4. TIC internos y terceros. Comunicación.



A nivel de Planeación institucional, hay correlación aceptable entre los documentos *Seguimiento plan acción MIPG II Trimestre 2020.xlsx* y *II Trimestre seguimiento POA 2020\_0.xls*, que incluyen las actividades de alto nivel que hacen parte de la gestión tecnológica de la entidad, incluyendo la atención de las políticas de gobierno Digital y Seguridad Digital, Sin embargo, no es claro el alcance contemplado en cada una de ellas con respecto a los lineamientos de gobierno Digital.

|  |  |  |
| --- | --- | --- |
| **PLAN DE ACCION MIPG** | **PRESUNTA CORRELACION POA** | **OBSERVACION AUDITORIA** |
| Formular y ejecutar el plan de mantenimiento preventivo y evolutivo (de mejoramiento) sobre la infraestructura de TI de acuerdo con los lineamientos de  Gobierno Digital (pregunta 84) | Formulación y ejecución del plan de mantenimiento y  monitoreo | De acuerdo a los lineamientos de  Gobierno Digital, debe dar cobertura a los equipos, sistemas de información y a los servicios TIC (numerales 88, 107 y 109 Furag) y desarrollar los instrumentos en el marco de los dominios A12, A15 y A14 del MSPI, sin embargo, según lo reportado ha sido orientado a:  Plan de Mantenimiento y Monitoreo y el contrato de mantenimiento preventivo 105 del 2019.  No se relacionan los procedimientos elaborados a la fecha en el marco del MSPI.    Las observaciones puntuales se emiten en el numeral 5.5.1 |
| Revisar el Plan Estratégico de | Formular, ejecutar y | En este numeral se emiten las |

|  |  |  |
| --- | --- | --- |
| **PLAN DE ACCION MIPG** | **PRESUNTA CORRELACION POA** | **OBSERVACION AUDITORIA** |
| Tecnologías de la Información y las comunicaciones PETI del IDEP para la vigencia 2020, específicamente el numeral 5.6 Gobierno de TI y 7.5 Proyectos a ejecutar en la vigencia 2020, así como los elementos requeridos por la política de Gobierno Digital según FURAG: Portafolio o mapa de ruta de los proyectos, proyección del presupuesto, entendimiento estratégico, análisis de la situación actual, plan de comunicaciones del PETI, tablero de indicadores para el seguimiento y control y la definición de la situación  objetivo y modelo de gestión de  TI. | hacer seguimiento del PETIC 2020 | debilidades encontradas en el documento “*PL-GT-12-01 PETIC V 19.pdf*” resultado del contrato 021 de 2020.    Los reportes corresponden al avance en los procesos de contratación. |
| Presentar al Comité Institucional de Gestión y Desempeño la versión actualizada de PETI 2020 y los cronogramas de actividades para el logro de los proyectos a ejecutar en la vigencia 2020. | Se entregaron a la auditoría los siguientes planes que incluyan actividades, fechas y seguimiento:  Plan Seguridad y Privacidad de la Info  2020 Seguimiento II.xlsx,  Plan Tratamiento de riesgos info 2020  Seguimiento II.xlsx,  Plan de Trabajo Conectividad Final-IDEP |
|  |  |
| Ejecutar en las fechas programadas los cronogramas de los proyectos a ejecutar en la vigencia en el marco del PETI 2020 y presentar trimestralmente el avance correspondiente al Comité Institucional de Gestión y Desempeño. |  | (26-06-2020).pdf    Ninguno de ellos corresponde a un cronograma de las actividades puntuales para atender los 5 proyectos planteados en el PETI.  En el seguimiento se reportan Actas de avance, pero no cronogramas. |
| Revisar el Plan de Seguridad y Privacidad de la Información formulado para la vigencia 2020 y asignar los responsables y fechas necesarias para el logro de dicho plan. | Formular, ejecutar y hacer seguimiento del Plan de Seguridad y privacidad de la información.    Realizar acciones de sensibilización, socialización y control  para promover la seguridad de la  información | El plan entregado a la auditoría Plan Seguridad y Privacidad de la Info 2020 Seguimiento II.xlsx, no da cobertura a lo requerido para la implementación del MSPI.    Las observaciones puntuales se emiten en el numeral 5.1.4 |
| Ejecutar las actividades programadas en el Plan de Seguridad y Privacidad de la Información, en las fechas definidas para la vigencia 2020 y presentar trimestralmente el avance correspondiente al Comité Institucional de Gestión y Desempeño. |
| Revisar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información formulado para la vigencia  2020 y asignar los responsables y fechas necesarios para el logro de dicho plan. | Formular, ejecutar y hacer seguimiento del Plan de tratamiento de riesgos de seguridad y privacidad de la  información 2020 | El plan entregado a la auditoría Plan Tratamiento de riesgos info 2020  Seguimiento II.xlsx, no da cobertura a lo requerido para la implementación del MSPI.  Las observaciones puntuales se emiten en el numeral 5.1.3 |
| Ejecutar las actividades programadas en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, en las fechas definidas para la vigencia 2020 y presentar trimestralmente el avance correspondiente al Comité  Institucional de Gestión y Desempeño. |
| Ejecutar el seguimiento a los indicadores | Realizar análisis del | Las observaciones sobre los indicadores |

|  |  |  |
| --- | --- | --- |
| **PLAN DE ACCION MIPG** | **PRESUNTA CORRELACION POA** | **OBSERVACION AUDITORIA** |
| de gestión por procesos | cumplimiento de los indicadores de gestión por proceso del trimestre anterior y presentar resultados en comité directivo. | TIC se emiten mas adelante en este numeral, pero en términos generales no dan cobertura a los lineamientos de evaluación y seguimiento de Gobierno  Digital. |
| Ejecutar el seguimiento a Mapas de riesgo institucionales y de corrupción | Realizar análisis del comportamiento del mapa de riesgos de la entidad, determinando el % de materialización de los riesgos, del trimestre anterior y presentar resultados en comité directivo. | Los riesgos identificados no dan cobertura a lo establecido en Gobierno Digital y más explícitamente en el MSPI, no están articulados con los activos de información ni con los controles de la norma ISO  27001:2013    Se emiten las observaciones puntuales en el numeral 5.1.3 |
| Formular y ejecutar el cronograma necesario para adoptar el protocolo IPV6 antes del 31 de diciembre de 2020, para dar cumplimiento a la Resolución 2710 de 2017 de MinTic | No hay correlación en el  POA | Con respecto a este proyecto, se incluye correctamente el plan de implementación en el anexo técnico del contrato 53 de  2020  La actividad general esta incluida en el Plan de seguridad y Privacidad de la Información. |
| No hay correlación en el Plan de Acción MIPG. | Gestionar  oportunamente las  solicitudes de creación, modificación o anulación de la documentación del SIG. | La actividad de articulación del SGSI con el SIG, no está incluida en el Plan de seguridad y Privacidad de la información, ni en el Plan de Acción MIPG para la atención de las políticas de gobierno Digital y Seguridad Digital, pese a que el MSPI requiere en su implementación la articulación entre elementos ISO 9001 impactados por ISO 27001. |
| No hay correlación en el Plan de Acción MIPG. | Actualizar el plan de contingencia tecnológica | La actividad no esta incluida en el Plan de acción, ni en los planes de Seguridad y privacidad de la información y el Plan de tratamiento de riesgos.    Sin embargo, se recibió el PL-GT-12-02 Plan Contingencia Tecno V11\_0.pdf actualizado a mayo de 2020, sobre el cual se emiten observaciones en el numeral  5.1.3. |
| No hay correlación en el Plan de Acción MIPG. | Formular y ejecutar el plan de trabajo de acuerdo a los  lineamientos establecidos en las políticas de "Seguridad digital", "Gobierno digital" y "Transparencia acceso a la información y lucha contra la corrupción" de MIPG para la implementación de estas políticas. | Se presume inmerso en los demás planes entregados y en especial en las obligaciones del contrato 021 de 2020. |

* Se observa que algunos de los proyectos del PETIC responden a dos de los objetivos específicos de la entidad declarados en el PEDI, sin embargo, no se incluye la trazabilidad explicita en el PETIC.

|  |  |
| --- | --- |
| **NIVEL ESTRATEGICO ENTIDAD PEDI** | **NIVEL ESTRATEGICO PETIC** |
| Desarrollar 1 estrategia de comunicación, socialización y divulgación de la cualificación, investigación e innovación docente: Comunidades de saber y de práctica pedagógica. | Afiliar al Instituto para la Investigación Educativa y el Desarrollo Pedagógico - IDEP a la Red Nacional Académica de Tecnología Avanzada – RENATA y  contar con los servicios de conectividad a la comunidad científica y de tecnología avanzada y la conectividad avanzada (internet 1:1 sin reúso + atributos de redes académicas). |
| Ejecutar el plan de acción del proyecto de inversión 1039 fortalecimiento a la Gestión Institucional y el Plan de adecuación y  sostenibilidad del SIG con referente MIPG, para la implementación del Modelo Integrado de Planeación y Gestión y sus 7 dimensiones. | Prestación de servicios profesionales para la administración y gestión de la infraestructura tecnológica del IDEP y para la implementación de las políticas Gobierno Digital y Seguridad Digital en el marco del Modelo Integrado de Planeación y Gestión. |

* Con respecto a la gestión de adquisiciones, se observa correcto tramite contractual entre los proyectos del PETI y el Plan de Adquisiciones 2020 (*SEGUIMIENTO JUNIO 2020 V15 PAA INVER SIÓN Y V16 PAA FUNCIONAMIENTO P.xlsx*). De igual manera, las adquisiciones se planearon de manera anticipada con base en los resultados de la auditoría 2019 y el análisis técnico de los requisitos de aprovisionamiento de la plataforma TIC. El Plan de adquisiciones es el resultado de las necesidades priorizadas de acuerdo al presupuesto disponible. Las iniciativas no priorizadas han sido registradas en el PETI para vigencias futuras.

|  |  |
| --- | --- |
| **NIVEL ESTRATEGICO PETIC** | **GESTION DE ADQUISICIONES** |
| Afiliar al Instituto para la Investigación Educativa y el Desarrollo Pedagógico - IDEP a la Red Nacional Académica de Tecnología Avanzada – RENATA y contar con los servicios de conectividad a la comunidad científica y de tecnología avanzada y la conectividad  avanzada (internet 1:1 sin reúso + atributos de redes académicas). | Contrato 048 de 2020  CORPORACION RED NACIONAL ACADEMICA  DE TECNOLOGIA  Proyectado PETI: $27.186.000 en Funcionamiento  Real: $42.214.459 en INVERSIÓN 1079 |
| Migración del sistema de información HUMANO | Contrato 26 de 2020  SOPORTE LOGICO LTDA  Coinciden los montos. |
| Proveer y mantener actualizados y en buen estado los  recursos de Tecnología de  Información y Comunicación necesarios para el funcionamiento del IDEP | Contrato 31 de 2020 y 50 de 2020  GOOBI SAS. Coinciden los montos  Contrato 60 2020 ITO SOFTWARE SAS Los demás ítems del PETI se encuentran registrados en el Plan de adquisiciones |

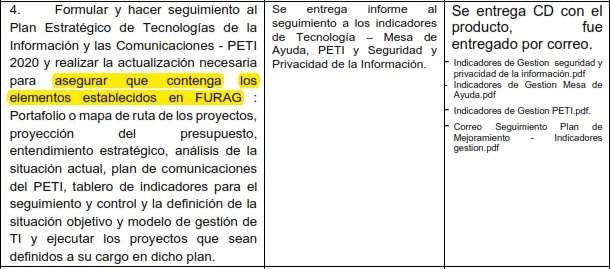
|  |  |
| --- | --- |
| **NIVEL ESTRATEGICO PETIC** | **GESTION DE ADQUISICIONES** |
| Prestación de servicios profesionales para la administración y gestión de la infraestructura tecnológica del IDEP y para la implementación de las políticas Gobierno Digital y Seguridad Digital en el marco del Modelo Integrado de  Planeación y Gestión. | Contrato 21 de 2020  ARMANDO ALFONSO LEYTON GONZALEZ  Funcionamiento, el monto coincide |
| Prestación de servicios para la adquisición, instalación,  configuración y puesta en  funcionamiento de una solución de copias de respaldo | La decisión esta en proceso de análisis |
| Realizar el análisis, diseño, adopción, implementación y transferencia de conocimiento del protocolo ipv6 en coexistencia con el protocolo ipv4, para el Instituto para la  Investigación Educativa y el Desarrollo Pedagógico – IDEP. | Contrato 53 de 2020  UNIÓN TEMPORAL UT IPV6 BG 2020  Presupuestado $64.600.000  Real: $170.408.000 |

Con el propósito de atender las acciones de las políticas de Gobierno Digital y Seguridad Digital incluidas en el Plan de Adecuación y Sostenibilidad del SIG con referente MIPG para el 2020 (*Seguimiento plan acción MIPG II Trimestre 2020.xlsx),* el 21 de febrero de, 2020, se celebró el contrato 021, cuyo alcance cita: “3*.1. Alcance: Responder por la formulación, ejecución, seguimiento y control del Plan Estratégico de Tecnologías de la información y las Comunicaciones - PETl de la vigencia 2020 así como los planes orientados a implementar las políticas de Gobierno Digital y Seguridad Digital y el plan relacionado con la implementación de la Ley de protección de datos personales*.”, donde uno de los productos es el PETI actualizado, que según informes de actividades del contratista del 12 de junio y 21 de julio de 2020 fue entregado con el documento “*PL-GT-12- 01 PETIC V 19.pdf*”, pese a que presenta las deficiencias que se relacionan a continuación.

Con respecto a los Planes de Seguridad y Privacidad de la información y el Plan de Tratamiento de Riesgos TIC, que son parte del alcance del contrato 021 de 2020, estos tampoco abarcan la envergadura de las directrices de Gobierno digital y seguridad Digital. Se emiten las observaciones en los numerales 5.1.3 y 5.1.4.

 De acuerdo al informe de actividades del 12 de junio y 21 de julio del 2020, la actividad 4 se reporta como cumplida, pese a que el PETIC no se encuentra actualizado a los lineamientos de construcción de PETI del Manual de Gobierno Digital V7, el MAE.G.GEN.01 Documento Maestro del Modelo de Arquitectura Empresarial V1 y en especial la G.ES.06 Guía para la construcción del PETI versión 2. En entrevista adelantada con el contratista, al cuestionar sobre las falencias relacionadas en los siguientes ítems, el contratista manifiesta que el alcance de su contrato contemplaba solo la actualización del PETIC 2020 con respecto a lo que incluía el PETIC 2019, desconociendo no solo las nuevas directrices publicadas por MINTIC, sino también los hallazgos evidenciados en el informe de auditoría del año 2019, para las cuales no se encontraron acciones de mejoramiento en los documentos: “*Consolidado Plan mejoramiento 2019-4.xlsx” y Plan de Mejoramiento Seguimiento II trimestre OCI.xlsx”.*

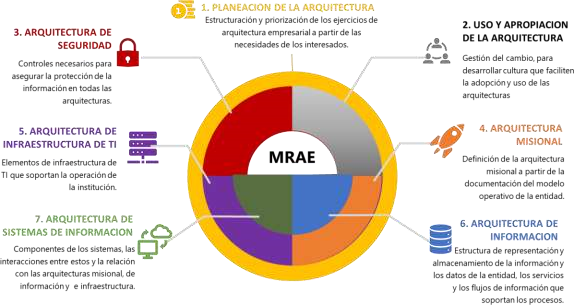
La siguiente imagen corresponde al informe del 12 de junio de 2020. En el informe del 21 de julio de 2020 se reporta una actualización, que corresponde al documento evaluado en la presente auditoría.



La consecuencia de esta ambigüedad en el entendimiento del alcance, ha repercutido en que la actualización del PETI 2020, corresponde más a un informe de actividades ejecutadas y no a una planeación bajo los lineamientos del MRAE.

 El procedimiento *PRO-GT-12-08 Formulación y Seguimiento al PETIC V5\_0.pdf*, no ha sido actualizado a los lineamientos de construcción de PETI del Manual de Gobierno Digital V7, el MAE.G.GEN.01 Documento Maestro del Modelo de Arquitectura Empresarial V1 y en especial la G.ES.06 Guía para la construcción del PETI versión 2, en los documentos de referencia externos solo relaciona a NTC-ISO/IEC 27001 la cual es la norma técnica de implementación del MSPI, pero no del PETI.

 El PETI, no ha sido actualizado al nuevo Marco de Referencia de arquitectura Empresarial que modifico los dominios a los siguientes ítems.



Vale aclarar que si bien, el PETI nombra 6 de los dominios no los desarrolla a cabalidad:

|  |
| --- |
| **Estrategia de TI:** falta mejorar la arquitectura misional de TI (misión, visión, indicadores y líneas estratégicas TIC). Con respecto a la articulación con el PEDI 20162020, se entiende que el PETI se encuentra alineado al Proyecto de inversión 1039: *Fortalecimiento a la Gestión Institucional* cuya meta *4) es Sostener 100% la implementación del Sistema Integrado de Gestión -SIG-MIPG*, entre los que se encuentra el Subsistema de Seguridad de la Información, lo cual es consistente con los compromisos del PETI en *5.2.5 Políticas de Tecnologías de la Información y las Comunicaciones del IDEP,* sin embargo la implementación del MSPI a pesar de su envergadura no se encuentra como un proyecto independiente entre los 5 proyectos formulados para la vigencia 2020 y los planes y políticas establecidos no dan cobertura al alcance del MSPI (*PL-GT-12-04 Plan Seguridad y Privacidad de la Info V5.pdf, PLGT-12-05 Plan Tratamiento de riesgos info V5.pdf y PO-GT-12-01 Política*  *seguridad privacidad info V3.pdf*), sobre los cuales se emiten observaciones de mejora en el presente informe (3.1.3 y 3.1.4). |
| En cuanto al **Gobierno de TI**, el instituto ha instaurado de manera correcta el Comité de Sistemas, Informática y de Seguridad de la Información -Resolución 159 de 2009, el cual se incorpora al Comité Institucional de Gestión y Desempeño conforme la Resolución No. 0214 de 2019, que opera como órgano decisorio en materia de inversión TIC. El PETIC incluye la matriz de roles en la cual se establecen las responsabilidades, pero es preciso determinar que cada persona asignada tenga los conocimientos tecnológicos requeridos para el Rol, tal es el caso del Oficial de  Seguridad y del responsable de seguridad en la entidad (ver  G4\_Roles\_responsabilidades.pdf). Cabe anotar que las responsabilidades asignadas a control interno corresponden parcialmente con los lineamientos MSPI, toda vez que |

|  |
| --- |
| al estar basado en una normal ISO es aplicable la responsabilidad de las clausulas 9. Evaluación y desempeño y 10. Mejora, con respecto a la ejecución de auditorías internas y el seguimiento a la atención de no conformidades y mejoramiento. Falta la inclusión de gestión de calidad como articulador de las normas ISO 9001 e IO 27001 en el SIG. |
| **Uso y apropiación de TI**: el dominio esta relacionado mas no desarrollado en articulación con el Plan de capacitación Institucional y la Clausula 7. SOPORTE del MSPI. De igual manera los indicadores planteados en el PETIC no incluyen medición del uso y apropiación de TI y no hay planes de Gestión y de Transferencia de conocimiento. |
| En el capítulo de **sistemas de información** se listan los actualmente existentes, pero no se desarrolla el dominio siguiendo los lineamientos (MRAE) en cuanto a la construcción de un modelo metodológico de estandarización, gestión de cambios y apropiación del control, mantenimiento y conocimiento. Este componente es relevante en la entidad ya que se observa una alta dependencia de conocimiento y control de los proveedores sobre los sistemas Humano y GOBBI. |
| El dominio de **Servicios Tecnológicos** muestra una descripción de las mejoras realizadas a la plataforma tecnológica desde el año 2017, las condiciones de conectividad y el modelo de administración, sin embargo, no está desarrollada conforme a los lineamientos (MRAE) la estructura de modelo de servicios tecnológicos con su correspondiente planeación de capacidad, documentación suficiente de operación e infraestructura y mesa de servicios TIC centralizada con ANS y articulación de terceros. Finalmente, el numeral 5.5.3 Información Vigencia de Servicios, Soportes, Garantías y otros, no incluye todos los servicios y/o productos contratados o todos los terceros que intervienen en los servicios tecnológicos. |
| **Gestión de Información**: este dominio no ha sido desarrollado, y es el que permite definir: el diseño de los servicios de información, la gestión del ciclo de vida del dato, al análisis de información y el desarrollo de capacidades para el uso estratégico de la misma mediante el desarrollo de los 4 componentes de información:  Planeación y Gobierno, Diseño, Análisis y Aprovechamiento y Calidad y Seguridad. |

 Con respecto seguimiento y evaluación de Gobierno Digital, el PETIC declara tres indicadores de gestión, que resultan insuficientes para medir cumplimiento y resultado, con un enfoque de mejoramiento continuo, que es una de las premisas del Manual de Gobierno Digital V7*: Todas las entidades públicas deben desarrollar una cultura de evaluación y seguimiento al desempeño, capacidad, efectividad, costos, pertenencia y demás criterios de calidad que se definan para medir la ejecución de los proyectos que hagan uso de TIC. Para ello deben definir indicadores de proceso, resultado e impacto, realizar medición, publicar resultados y a partir de estos, iniciar acciones correctivas o de mejora continua.* A continuación, se emiten las observaciones puntuales con base en el PETIC y en el archivo INDICADORES GT 2020 II.xls.

|  |  |
| --- | --- |
| **INDICADOR**  **DESCRIPCIÓN DEL INDICADOR** | **OBSERVACION AUDITORIA** |
| **Eficacia en la atención de solicitudes recibidas a través de mesa de ayuda**:    Conocer qué porcentaje de las solicitudes presentadas por los usuarios internos del IDEP a través de la mesa de ayuda son atendidas y cerradas en el mismo periodo de tiempo e identificar qué tipo de solicitud se recibe de manera más recurrente | El indicador presenta las siguientes debilidades:  No da cobertura al concepto de cumplimiento toda vez que son los SLA´s o ANS los que determinan las condiciones de cumplimiento de soporte del dominio de servicios tecnológicos, y estos no están configurados en la herramienta actual y el indicador no los incorpora en su medición. (ver indicadores G.ST.01 Guía del dominio de Servicios Tecnológicos). Esto significa que el indicador mide que los incidentes se hayan cerrado, pero no las condiciones de calidad en términos de tiempos y satisfacción del resultado.  No da cobertura a los servicios tecnológicos declarados en el PETI, toda vez que tanto los soportes de Humano como de GOOBI y en general de terceros responsables, son direccionados a los proveedores sin que sean previamente registrados en OSTicket. Esto significa que el indicador mide únicamente los incidentes de soporte interno y no el modelo de servicios tecnológicos.  Dado que la medición no incorpora elementos de efectividad y calidad, no es base suficiente para que el indicador aporte valor de mejora continua a servicio tecnológicos gestionados de manera interna y/o con terceros. |
| **Cumplimiento de las actividades del plan**  **estratégico de tecnologías de la información y las comunicaciones PETI en la vigencia**.    Medir el nivel de cumplimiento de las actividades definidas en el  Plan Estratégico de Tecnologías de la Información y las Comunicaciones para atender las necesidades tecnológicas del IDEP | De acuerdo con el habilitador de arquitectura de Gobierno Digital: La entidad debe definir y medir indicadores de monitoreo, desempeño y evaluación del PETI través a través de tableros de control, y formular acciones de mejora frente a desviaciones, sin embargo, el indicador establecido por la OAP no tiene como fuente tableros de control de los 5 proyectos con actividades discriminadas, fechas por estimación de esfuerzo, responsables individuales y criterios de calidad de entregables, para determinar cumplimiento, desempeño y calidad respectivamente. En el seguimiento a los Planes de Acción, POA y planes institucionales se registran actividades ejecutadas de manera general, pero no hay un documento que permita verificar planeación vs avance.  No responde a los lineamientos de Gobierno Digital con respecto a la cobertura en términos de los dominios del MRAE, para el diseño de indicadores asociados al PETI, que aporten valor a la entidad. La  siguiente imagen corresponde al tipo de indicadores para 3 de los 7 dominios del MRAE.  [(https://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue- 8017.html](https://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-8017.html) - Indicadores de gestión de TI, Lineamientos del Marco de Referencia de AE para la gestión de TI) |

|  |  |  |
| --- | --- | --- |
| **INDICADOR DESCRIPCIÓN**  **INDICADOR** | **DEL** | **OBSERVACION AUDITORIA** |
|  |  |  |
| **Cumplimiento** | **de las** |  |
| **actividades del plan de seguridad y privacidad de la información en la vigencia.**    Medir el nivel de cumplimiento de las actividades definidas en el plan de seguridad y privacidad de la  información para mantener su integridad, confidencialidad y disponibilidad. | | Si bien el indicador mide cumplimiento en términos de fechas proyectadas de las actividades del Plan, no ofrece resultados de nivel de madurez en la implementación del Modelo de Seguridad y Privacidad de la Información, toda vez que el plan adolece de los elementos que constituyen su articulación, implementación de controles, verificación de efectividad e integración al SIG. Las debilidades en esta materia se evidencian en el numeral 5.1.4 del presente informe.  Dado que el plan de seguridad y privacidad de la información no representa el alcance real de una implementación MSPI, este indicador resulta confuso, ya que puede trasmitir un dato errado sobre el nivel de madurez de la entidad en implementar seguridad de la información. Evidencia de ello, es que este mismo indicador se reporto en el 2019 con resultados por encima del 100% pese a que los resultados de la auditoría 2019 evidenciaron graves fugas de seguridad. Ver imagen inferior: fuente indicadores 2019 publicados en la página de la entidad. |
|  | | |

 En términos generales el tablero de indicadores en las dos vigencias auditadas (2019 y 2020) no atiende las directrices que en esta materia ha emitido el manual de Gobierno Digital, toda vez que orienta su creación en los 7 dominios del MRAE tales como: desempeño de la gestión de TI, de efectividad del uso y apropiación, componentes de información asegurados, disponibilidad de servicios tecnológicos y avance en implementación de controles MSPI entre otros. (ver documento Lineamientos del Marco de Referencia de AE para la gestión de TI).

#### 5.1.1.1 Seguimiento a Recomendaciones 2019

|  |  |  |  |
| --- | --- | --- | --- |
| **N°.** | **Recomendación 2019** |  | **Seguimiento 2020** |
| 1 | Como insumo para la formulación del PETIC, adelantar un análisis DOFA sobre la plataforma tecnológica, recursos TIC y competencia y conocimiento de los recursos humanos del IDEP en relación con la capacidad de ofrecer continuidad, seguridad de la información y desempeño aceptable para soportar los requisitos externos, requisitos de la entidad, proyectos propios TIC y oportunidades de innovación.  El análisis DOFA ofrecerá elementos para identificar necesidades de conocimiento y proyectos estratégicos además de proyectos orientados al mantenimiento de la plataforma tecnológica. Aprovechar la nueva formulación del PEDI para la vigencia 2020 - 2024 para proyectar el PETIC a 4 años como lo recomienda el Marco de Referencia de Arquitectura  Empresarial para la Gestión de TI del Estado colombiano. |  | En el PETI actualizado a la vigencia 2020, se incluye el análisis DOFA, donde los siguientes elementos se relacionan con proyectos:  **MIGRACION HUMANO A SAAS**  -Interés de los directivos(as) de innovar y aplicar herramientas tecnológicas en cumplimiento de la misión Institucional. "Existe riesgo de indisponibilidad de los servicios de sistemas dada la  ubicación del centro de cómputo."  **CONTRATO 21 2020**  -Implementación de las políticas de Gobierno Digital y Seguridad Digital del MIPG.  -Implementación del Modelo de Seguridad y  Privacidad de la Información."  **ADQUIRIR HERRAMIENTA DE BACKUP**  -Ausencia de un sistema automático de copias de seguridad o de respaldo de la información y bases de datos institucionales. Procesos de backup de sistemas de información y bases de datos se realizan de manera manual. **IMPLEMENTACION IPV6**  Implementación de la versión del protocolo IPv6. |

|  |  |  |  |
| --- | --- | --- | --- |
| **N°.** | **Recomendación 2019** |  | **Seguimiento 2020** |
| 1 | Realizar un análisis de los lineamientos del MIPG y del MSPI para construir un plan de proyecto proyectado al 2020 que permita dar cumplimiento a las políticas de "Seguridad digital", "Gobierno digital" y "Transparencia acceso a la información y lucha contra la corrupción" de MIPG y al MSPI. De ser posible contratar consultoría especializada o en su defecto fortalecer los conocimientos del funcionario de planta a través de procesos de formación.  Para la implementación del MSPI es recomendable que el oficial de seguridad tenga conocimientos en implementación de los controles de seguridad de la información con base  en la norma ISO 27001:2013 y dedicación suficiente al proyecto. |  | Las debilidades identificadas en el Plan de seguridad y privacidad de la información (5.1.4), en el PETI y en el Plan de Tratamiento de Riesgos (5.1.3), evidencian que no hay un conocimiento profundo de los requisitos de implementación. Se mantiene la recomendación de asignar como oficial de seguridad y/o persona responsable de la implementación del MSPI a un ingeniero de sistemas con conocimientos técnicos de seguridad de la información, ya que a diferencia de otras normas como ISO9001, la ISO 27001 y en especial su anexo 27002, requieren de conocimiento especializado para que no se limite a una implementación documental. |
| 2 | Incorporar en los Indicadores y Riesgos del PETIC indicadores asociados a la medición de cumplimiento, productividad y calidad en los servicios  TIC y proyectos, seleccionando aquellos que sean pertinentes entre los recomendados por el Marco de  Referencia de Arquitectura Empresarial de TI, especialmente en el dominio Gobierno de TI:  Antes de formular el cálculo de indicadores se recomienda atender las recomendaciones de centralización de mesa de servicio del numeral 3.5.2 informe 2019 |  | No se observa avance en la optimización de indicadores conforme a los lineamientos de Gobierno Digital para la Gestión de TI, Gobierno de TI, MSPI y tratamiento efectivo de riesgos.    Ver observaciones en este numeral |
| 3 | Con relación a los Cronogramas para Control del Proyecto se recomienda:  • Garantizar que para cada proyecto del PETIC se establezcan planes de acción tácticos que incluyan las actividades a ser ejecutadas por personal interno o por terceros para garantizar que los activos de información adquiridos queden debidamente configurados de acuerdo a las mejores prácticas y que el conocimiento para su |  | Los siguientes son los cronogramas entregados a la auditoría:   1. Plan Tratamiento de riesgos info 2020   Seguimiento II.xlsx   1. Plan Seguridad y Privacidad de la Info 2020 Seguimiento II.xlsx 2. Plan de Mejoramiento Seguimiento II trimestre OCI.xlsx     Sobre los cuales se emiten las siguientes observaciones con respecto al seguimiento a las recomendaciones: |

|  |  |  |  |
| --- | --- | --- | --- |
| **N°.** | **Recomendación 2019** |  | **Seguimiento 2020** |
|  | operación y administración quede transferido al instituto.   * Para todos los planes tácticos establecer las fechas y responsables con base en un análisis de estimación de esfuerzo por tareas versus la capacidad de trabajo instalada. Esto con el fin de identificar necesidades de recurso humano y establecer fechas viables de cumplimiento. * Antes del cálculo de capacidad disponible deben sustraerse los tiempos requeridos por cada recurso para la atención de funciones de rutina. * Establecer criterios de aceptación de las actividades programadas para determinar su verdadero estado de cierre. De ser posible implementar pruebas cruzadas para verificar la calidad de los resultados. * Asignar tareas de manera individual con el fin de medir cumplimiento y productividad por recurso. * Priorizar las tareas de acuerdo con:   + Prioridad 1: requisitos   regulatorios o normativos   * + Prioridad 2: de valor agregado para los   procesos misionales   * + Prioridad 3: de valor agregado para el desempeño o seguridad de la plataforma tecnológica   + Prioridad 4: de valor agregado para los procesos de apoyo   + Prioridad 5: relevancia   particular del solicitante |  | * No hay actividades detalladas por cada uno de los proyectos del PETI, tal es el caso de RENATA y Migración Humano, que, si bien están a cargo de terceros, si incluye actividades de seguimiento, control y recepción que implican esfuerzo. * Las fechas se presentan en bloques de meses paralelizados, sin análisis de esfuerzo vs capacidad instalada, lo cual impide el calculo de indicadores de cumplimiento y/o productividad. (Ver imagen abajo consolidada) * No se han incluido los criterios de aceptación por entregables de cada actividad, lo cual impide obtener indicadores de calidad. * Las tareas no están asignadas de manera individual. De las 47 actividades, solo 11 están asignadas de manera individual, lo cual impide la medición por recurso. * Las siguientes actividades están repetidas en dos cronogramas:   + Crear Servidor Web Virtual   + Divulgar y gestionar los boletines informativos de seguridad, Integrar con CSIRT de Gobierno   + Identificar y actualizar los inventarios con los nuevos AI del Área de Tecnología.   + Reportar al director de la Entidad la información recolectada en el instrumento de AI que se identifica y corresponde a las bases de datos del Área de Tecnología.   + Revisar la guía GU-GT-12-01 Guía para la gestión de incidentes de seguridad de la información y el formato FT-GT-12-21 Registro de incidentes de seguridad de la información |
| CRONOGRAMAS CONSOLIDADOS POR LA AUDITORIA COMO PAPEL DE TRABAJO | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **N°.** | **Recomendación 2019** |  | **Seguimiento 2020** |
|  | | | |



|  |  |  |  |
| --- | --- | --- | --- |
| **N°.** | **Recomendación 2019** |  | **Seguimiento 2020** |
| 4 | Adelantar la estructuración de los proyectos de uso y apropiación de tecnología una vez hayan sido documentadas y formalizadas todas las políticas de seguridad de la información del MSPI de manera integrada con el control 7.2.2 Concientización, educación y capacitación sobre la seguridad de la información de la norma ISO 27002:2013 |  | En el PETI 2020, se encuentra declarado, mas no desarrollado como proyecto, sin embargo, en los cronogramas entregados se incluyen las actividades de “*Divulgar y gestionar los boletines informativos de seguridad, Integrar con CSIRT de Gobierno*” y se han adelantado capacitaciones en diversos temas tal como Goobi y Meets.    En cuanto al *PL-GTH-13-01 Plan Inst Capacit V7.pdf*, se observa que aún no está articulado con el dominio de uso y apropiación, por las siguientes razones:     * Los resultados de la mesa de servicio no son insumo para la identificación de necesidades. * En la tabla de necesidades de aprendizaje, no se incluyen los temas de Gobierno Digital y MSPI. * No se han articulado el eje de gestión del conocimiento, con planes de trasferencia de conocimiento interno y con terceros TIC, ni con la mesa de servicio. |

**5.1.1.2 Nuevas Recomendaciones 2020**

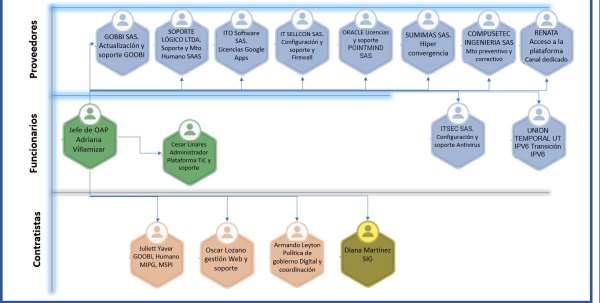
|  |  |
| --- | --- |
| **N°.** | **Recomendación 2020** |
| 1. | Actualizar el Plan Estrategico de Tecnología de Información conforme a los lineamientos de Gobierno Digital (manual V7) y demás guías emitidas por MINTIC, de manera articulada con los demás planes de la entidad.    De suscribirse un nuevo contrato con el objeto del contrato 21 de 2020, se recomienda establecer el listado de entregables de acuerdo a lo requerido por Gobierno Digital y MSPI junto con los criterios de aceptación en cada caso. |

**2.** Se recomienda por parte de esta Oficina, organizar las actividades inherentes al proceso de TI de acuerdo con los siguientes roles, de forma tal que permita mayor articulación con los lineamientos emitidos por MINTIC.



### 5.1.2 Estructura Organizacional y Gobierno de TI

La estructura organizacional corresponde al siguiente esquema, donde se evidencia la segregación de Funciones de los recursos de TI en modalidad de funcionarios, contratistas y proveedores, con una alta participación de terceros en la prestación de los servicios TIC, lo cual es perfectamente válido, siempre y cuando se lleven controles estrictos desde la etapa precontractual, pasando por la ejecución y posibles garantías o soportes, que ofrezcan el mayor beneficio para la entidad por la inversión realizada.



* Con respecto al proveedor de Goobi IT GOP SAS, se observa que permanece nivel de insatisfacción con la calidad del servicio, toda vez que no atiende de manera diligente los requerimientos del IDEP y los problemas funcionales persisten sin que se evidencia interés por dar cumplimiento a las obligaciones del contrato. Como medida correctiva, el día 30 de abril de 2020 se realizó el estudio del mercado y análisis del sector para la contratación cuyo objeto es “***Adquisición de un sistema ERP para el manejo administrativo y financiero del IDEP****”*, de igual manera se adelantó la ficha técnica buscando una solución en la nube, lo cual resulta en la alternativa más conveniente para el IDEP, lo que se sustenta en el documento *“Caso de Negocio Análisis de la migración de los sistemas de información del IDEP a la nube*”. Si bien no se ha diseñado un formato RFP para adquisiciones con requerimientos funcionales, no funcionales y de soporte y garantía, se realizó y el correcto levantamiento de requerimientos funcionales con las áreas, al igual que la solicitud de cotizaciones y demostraciones del software.

* El IDEP cumple con el debido registro de contratos vigentes con terceros, lo cual fue verificado en las plataformas de SECOP I y II.

* Con respecto a los contratos con proveedores, se observa el debido cumplimiento de los requisitos de control: acuerdo de confidencialidad, transferencia de conocimiento, ANS si aplica y requisitos de seguridad en cumplimiento del dominio 15 Gestión de Terceros del MSPI. La siguiente tabla muestra la trazabilidad.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **N°**  **Contr ato** | **Nombre Tercero** | **OBJETO** | **Observaciones Auditoría** | **Acuerdo Confidencialidad** | **ANS** | **Trasferencia de conocimiento** | **Requisitos de seguridad** |
| 110- 2017 | SUMIMAS  SAS | Prestación del servicio para el suministro, instalación, configuración, licenciamient o, soporte técnico y puesta en marcha de una solución tecnológica hiperconverg ente | Dentro de la información suministrada para el análisis, solo se recibió el contrato original del 2017, el cual tenía una duración de un año a partir de la aprobación de la garantía. El plan de adquisiciones del 2020 contempla el Servicio de renovación de la garantía y soporte de la solución de hiperconvergencia. | La Clausula 7 del contrato, Obligaciones generales del contratista, numeral 2 hace referencia a que el contratista debe mantener la reserva de la información. Así mismo, la Clausula 7 numeral 9 menciona de manera general la confidencialidad de la información. Sin embargo, no se observó acuerdos de confidencialidad donde se detalle el tema y se especifique que la confidencialidad debe ser extienda después de la terminación del contrato. | No se encontró referencia | Este tema se aborda en varios apartes de la Clausula 7ma del contrato, Obligaciones específicas: Numeral 2: se hará transferencia de conocimiento dentro de los 10 días después del afinamiento, Numeral 13:  transferir conocimiento de la configuración, administración y  manejo de la solución, y el Numeral 14 Compromiso de entrega de manuales básicos de instalación y configuración de la solución hiperconvengente y el mapa de red | La Clausula 7ma del contrato, Ítem B Obligaciones generales del contratista, numeral 12 indica sobre el cumplimiento de las políticas de seguridad de activos de información y el uso adecuado de internet. |
| 134- 2018 | IT SELCON  SEGURIDA  D  COSULTO  RIA  SOLUCION  ES S.A.S | Prestación de servicios para el suministro, instalación, configuración, soporte técnico y puesta en marcha de  las licencias de antivirus y renovación de las licencias de firewall del IDEP. | Contrato a máximo el 31 de diciembre de 2019. Garantía y soporte 5x8 directamente con el fabricante durante mínimo tres (3) años, contados a partir de la fecha de inicio del soporte. | La Clausula 7ma del contrato, del contratista Numeral 2 hace referencia a que el contratista debe mantener la reserva de la información. También el numeral 9 hace alusión al manejo de confidencialidad de la información. | Los estudios previos, numeral 3.3 especificaciones generales señala que se dará soporte 5x8 durante 3 años para el caso de las licencias de firewall, y durante el tiempo contratado para el caso de la licencia de antivirus. | Según la cláusula 2da. del contrato, denominada alcance del  objeto, y la cláusula 7ma obligaciones específicas del contratista, Numerales12, 14, 15 y 17. | La Clausula 7ma del contrato, numeral 14 indica sobre el cumplimiento de las políticas de seguridad de activos de información, el uso adecuado de internet y del correo electrónico.    Los estudios previos, numeral 3.3: La herramienta debe permitir el acceso al instituto, mediante políticas, para equipos que no pertenecen al instituto. |
| 60- 2019 | ITO-  SOFTWAR  E | Adición del contrato 060- 2019 con Orden de  Compra  37.163 del acuerdo marco de precios Google II | Solo está la orden de compra asociada al contrato. Está incluido en el plan de inversión 2020. | No aplica |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **N°**  **Contr ato** | **Nombre Tercero** | **OBJETO** | **Observaciones Auditoría** | **Acuerdo Confidencialidad** | **ANS** | **Trasferencia de conocimiento** | **Requisitos de seguridad** |
| Orde n de Servi cios    105- 2019 | COMPUSE  RTEC  INGENIERI  A SAS | Prestación de los servicios para realizar  el  mantenimient o preventivo y  correctivo de la  infraestructur a tecnológica del IDEP. | El contrato cuya vigencia databa de abril de 2020, fue objeto de suspensión el 6/04/2020 en atención a la situación de fuerza mayor generada por la crisis sanitaria del coronavirus  COVID-19 y las medidas adoptadas por el gobierno nacional mediante el decreto 457 de 2020 | De acuerdo con los estudios previos, numeral 4.3 obligaciones generales se debe mantener la  confidencialidad de la información.    Suscripción del acuerdo de confidencialidad (si aplica) | Según el numeral 3.2.1.2 de los estudios previos. | No aplica | Los estudios previos, numeral 3.2.1.3 para el mantenimiento correctivo componente lógico de la infraestructura TIC, el servicio se prestará siguiendo los protocolos de seguridad de la entidad.  4.2. se deben atender los procedimientos establecidos por la entidad.  4.3. Dar cumplimento a las políticas de seguridad de los activos de información y el uso adecuado de internet y del correo electrónico. |
| Orde n de  Comp ra  107- 2019 | POINTMIN  D SAS | Suscripción al servicio de soporte de Oracle Linux y VM y migración de  la licencia del motor de base de datos a Oracle SE 2 y su correspondie nte soporte. | Suscrito en octubre de 2019 con vigencia de licencia de dos años. | Los estudios previos, numeral 4.2 indican que el contratista debe Guardar y mantener la debida reserva frente a temas y asuntos tratados y conocidos con ocasión de la ejecución del presente contrato.    Guardar y mantener la debida reserva frente a temas y asuntos tratados y conocidos con ocasión de la ejecución del presente contrato.  Suscripción del acuerdo de confidencialidad (si aplica) | No hay referencia explicita | La suscripción a los soportes por parte del fabricante de OVM y OL, permitirá al instituto contar con soporte telefónico o en línea 7 días a la semana durante las 24 horas del día, así como el acceso a 'as actualizaciones y parches de seguridad para ambas herramientas, entre otros servicios adicionales | Los estudios previos, numeral 4.2 indican que el contratista debe Dar cumplimento a las políticas de seguridad de los activos de información y e' uso adecuado del ¡internet y de' correo electrónico. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **N°**  **Contr ato** | **Nombre Tercero** | **OBJETO** | **Observaciones Auditoría** | **Acuerdo Confidencialidad** | **ANS** | **Trasferencia de conocimiento** | **Requisitos de seguridad** |
| Orde n de  Comp ra  115- 2019 | ITSEC SAS | Prestación de servicios para la renovación de licencias  de antivirus  Kaspersky  Endpoint  Security for  Business –  Select  Educacional License y los servicios de actualización, migración y depuración de la Consola  Kaspersky  Security  Center | Carta de aceptación de la oferta 115 de 2019, renovación por 3 años | Según estudios previos del contrato, numeral 4.2 ítem 9. | Según estudios previos del contrato, numeral 3.1 Especificaciones técnicas establece soporte 5x8 durante el tiempo de renovación del contrato. | Los estudios previos del contrato, numeral 4.1 obligaciones específicas establece que ésta se realizará una vez finalice la actualización, migración y depuración de la Consola  Kaspersky Security Center. | Según estudios previos del contrato, numeral 4.2 ítem 14 indica sobre el cumplimiento de las políticas de seguridad de activos de información, el uso adecuado de internet y del correo electrónico. |
| 26- 2020 | SOPORTE  LOGICO | Prestación de servicio de soporte, actualización y  mantenimient o al sistema de información  HUMANO. | El contrato se encuentra vigente desde el 13 de marzo de 2020 | El numeral 8.1 de los estudios previos establece: El contratista debe guardar y mantener la debida reserva frente a temas y asuntos tratados y conocidos con ocasión  de la ejecución del presente contrato.    Mantener la confidencialidad de la información suministrada por EL INSTITUTO, la cual solo podrá ser utilizada para la correcta ejecución del servicio contratado.    Suscripción del acuerdo de confidencialidad. | El numeral 8.1 de los estudios previos:    Disponibilidad de servicio 7 x 24 durante los 365 días del año.    Garantizar que el software soporte el IPv6 nativo en coexistencia con el lPv4.    Realizar el Monitoreo en el Datacenter que tiene dispuesto Soporte Lógico Ltda. en una disponibilidad de 7x24x365. | El numeral 8.1 de los estudios previos: Proporcionar la capacitación sin ningún costo adicional a los servidores públicos que se requieran por parte del lDEP, en las  instalaciones de Soporte Lógico,  previa programación acordada en  {re la supervisión del contrato y el contratista. | El numeral 8.1 de los estudios previos establece que el contratista debe dar cumplimento a las políticas de seguridad de los activos de información y el uso adecuado del internet y del correo electrónico que fije la entidad en cualquier sentido. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **N°**  **Contr ato** | **Nombre Tercero** | **OBJETO** | **Observaciones Auditoría** | **Acuerdo Confidencialidad** | **ANS** | **Trasferencia de conocimiento** | **Requisitos de seguridad** |
|  | CORPORA  CIÓN RED  NACIONAL  ACADÉMIC  A DE  TECNOLO  GÍA  AVANZAD  A –  RENATA | “Afiliar al  Instituto para la  Investigación  Educativa y el  Desarrollo  Pedagógico - IDEP a la  Red  Nacional Académica de  Tecnología  Avanzada – RENATA y  contar con los servicios de conectividad  a la  comunidad  científica y de tecnología avanzada y la conectividad  avanzada  (internet 1:1 sin reuso + atributos de redes  académicas)”  , | Vigente desde el 29 mayo de 2020 | Si, según los estudios previos. | Según los estudios previos hay la disponibilidad es 7x24 y están establecidos los acuerdos de niveles de servicio. | Existe evidencia de la capacitación dada por el contratista. | Los estudios de mercado RENATA del 12/02/2019 señalan que "... es indispensable contar con servicios y herramientas tecnológicas  que provean servicios de conectividad avanzada a través de una plataforma WEB que cuente con interacción de manera remota en tiempo real con atributos de seguridad y velocidad de la red avanzada y que permita el acceso a los servicios desde cualquier lugar del mundo. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **N°**  **Contr ato** | **Nombre Tercero** | **OBJETO** | **Observaciones Auditoría** | **Acuerdo Confidencialidad** | **ANS** | **Trasferencia de conocimiento** | **Requisitos de seguridad** |
| 50- 2020 | GOOBI  SAS | Prestación de servicios de actualización, mantenimient o y soporte del sistema de información que soporta la gestión administrativa  y  financiera del  IDEP | Vigente desde el 1 de julio de 2020 | Con base en el ítem 9 del informe de avance del 13 de agosto del 2020, el contratista llevó a cabo la formalización del acuerdo de confidencialidad con el IDEP. | Según la propuesta del 25 de junio de 2020, numeral 2.5 establece los niveles de soporte. | Obligación 6. Proporcionar la actualización y …Cada actualización del software debe incluir el servicio de instalación, revisión de procedimientos, migración, asistencia de configuración, capacitación a los usuarios finales sobre los cambios en el aplicativo y actualización de la documentación asociada | Obligación 14. Dar cumplimiento a las políticas de seguridad de los activos de información y el uso adecuado del internet y del correo electrónico que fije la entidad en cualquier sentido. |
| 53  2020 | UNIÓN  TEMPORA  L UT IPV6  BG  2020 | Realizar el análisis, diseño, adopción, implementaci  ón y transferencia de conocimiento del protocolo ipv6 en coexistencia con el protocolo ipv4, para el Instituto para la  Investigación  Educativa y el  Desarrollo Pedagógico – IDEP. | Vigente hasta el 31 de diciembre de 2020 | Según el objeto descrito en el  Anexo técnico y el numeral 8  Obligaciones contractuales | Según el objeto descrito en el Anexo técnico y el numeral 8 Obligaciones contractuales Debe garantizar un nivel de servicio siete (7) días a la semana, veinticuatro (24) horas al día durante la vigencia del contrato, con tiempos de respuesta no superior a dos (2) horas en caso de incidentes relacionados con la implementación del protocolo IPv6 o las configuraciones en Dual Stack. | En el objeto del contrato  Realizar el análisis, diseño, adopción, implementación y transferencia de conocimiento del protocolo ipv6 en coexistencia con el protocolo ipv4, para el Instituto para la Investigación Educativa y el Desarrollo Pedagógico – IDEP. | Según el objeto descrito en el Anexo técnico y el numeral 2.1 Plan para la Dirección del desarrollo del proyecto. El tipo de servicio incluye todas las condiciones de seguridad. |



En cuanto al control y seguimiento a contratos, se observa que, si bien se registra la ejecución contractual con respecto al Plan de Adquisiciones, no se cuenta con un tablero centralizado de control de contratos vigentes que permita hacer seguimiento técnico a su ejecución de pagos y cumplimiento en términos de calidad, tiempos y acuerdos de niveles de servicio. Se elaboró durante la auditoría el documento “*Contratos en ejecución Sistemas.xlsx”*, el cual contiene un listado de contratos vigentes con algunas columnas de caracterización, pero no es claro en cuanto a finalización del servicio, supervisor responsable, enlace Secop y porcentajes de ejecución física y financiera. De igual manera se observa que las pestañas de seguimiento a los pagos solo se diligencian para los proyectos Goobi y Humano a cargo de la contratista Julieth Yaver, pero no se aplica de manera estándar para los demás contratos y solo incluye la relación de pagos, mas no el cumplimiento de criterios de aceptación.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **N°.** |  | **Recomendación 2019** |  | **Seguimiento 2020** |
| 1. | • | Adelantar una matriz de Cargos vs Funciones vs documentos, que incluya para cada cargo cuales son los conocimientos específicos que deben ser trasferidos, que documentos de procedimientos e instructivos deben incorporarse a la transferencia y el cargo de contingencia. |  | A la fecha no se han adelantado los planes de  trasferencia de conocimiento y el documento PL-GT-12-02  Plan Contingencia Tecno |







La entidad cuenta con el Res 052-2020\_Manual Especifico de Funciones IDEP.pdf, actualizado al 15 de abril de 2020 para los empleados de planta de personal del IDEP (Resolución 222 del 2015), que incluye al Técnico operativo del proceso de gestión tecnológica, cabe anotar que para el cargo de jefe de la Oficina de Planeación no se incluyen funciones asociadas a la gestión tecnológica, sistema de gestión de seguridad de la información, ni Gobierno Digital.

#### 5.1.2.1 Seguimiento a Recomendaciones 2019



|  |  |  |  |
| --- | --- | --- | --- |
| **N°.** | **Recomendación 2019** |  | **Seguimiento 2020** |
|  | • Formalizar un Plan de Transferencia de Conocimiento especifico especialmente entre funcionarios y contratistas, que haciendo uso de un número de horas a la semana por colaborador se ejecute:   * La elaboración de los instructivos y procedimientos (que aún no existan) correspondientes a sus funciones de acuerdo con Matrices de Cargos vs Funciones vs documentos. * Capacitación en las funciones de su cargo, incluyendo incidentes y recuperaciones para el funcionario identificado como contingencia. o Elaborar un plan de rotación de funciones temporal, entre colaboradores principales y de contingencia. Evaluar resultados.     Este ejercicio puede incorporarse a la documentación de Plan de continuidad de negocio y al desarrollo del dominio 17 (continuidad) del Modelo de Seguridad y Privacidad de la Información (MSPI) ya que conforme a la norma ISO 27001:2013 el personal con conocimientos específicos también es un activo de información y es objeto de tratamiento de riesgos por ausencia temporal o permanente. |  | V11\_0.pdf, aun no incluye la contingencia por recurso humano de conocimiento especifico.    Sin embargo, se observa un aumento en la construcción de instructivos y manuales que son instrumentos de gestión de conocimiento.  De igual manera se han solicitado documentos a proveedores con este mismo propósito. |
| 2. | De ser posible, adelantar procesos de capacitación al funcionario de sistemas de la OAP para disminuir la dependencia de conocimiento de los proveedores del firewall, antivirus y hiperconvergencia y otros elementos de gestión de operaciones TIC. En los estudios previos de contratistas fortalecer los requisitos de conocimientos en seguridad |  | No se evidencia mejora en el conocimiento específico del Tecnico del área.  La recolección de evidencias de configuración fue atendida por un contratista.    Vale anotar como mejora, la elaboración de manuales de administración de las  herramientas administrativas. |
| 3. | De ser posible incluir en las obligaciones de los contratistas la elaboración de instructivos de transferencia de conocimiento y un servicio de empalme al IDEP asociado al último producto del contrato que incluya por lo menos registros documentales de cambios, seguimiento a los contratos y procedimientos de operación. |  | En los contratos 21, 24 y 25 de 2020 no incluye instructivos. |
| 4. | Adelantar acuerdos de confidencialidad con los contratistas. |  | Se están aplicando  acuerdos de  confidencialidad |
| 5. | Adelantar un análisis de capacidad de los recursos humanos actuales con que cuenta la OAP con respecto a los requisitos de esfuerzo para adelantar las funciones de la gestión TIC, de Gestión de Seguridad de la Información y la |  | No se evidencia avance al respecto.    Existen obligaciones y |

|  |  |  |  |
| --- | --- | --- | --- |
| **N°.** | **Recomendación 2019** |  | **Seguimiento 2020** |
|  | atención de proyectos.  Esto con el fin de determinar si los recursos actuales son suficientes para atender la demanda funcional. De ser posible, mejorar los perfiles de los contratistas o vincular uno adicional para la implementación MSPI. |  | productos repetidos en los contratos con personas naturales. |
| 6. | De ser posible, continuar con la búsqueda de alternativas para la adquisición de un sistema ERP en remplazo de Goobi.  Analizar la opción de un sistema por servicio, lo cual podría resultar más económico que la instalación local. De igual manera no sesgar las especificaciones técnicas a una interfaz preexistente con el sistema Humano, sino a la capacidad de cargar archivos planos con información de nómina para su procesamiento contable. |  | La recomendación fue atendida correctamente.    La contratista a cargo realizo un análisis correcto y suficiente. |
| 7. | Establecer como política de seguridad del MSPI dominio 15 la inclusión de criterios de aceptación de entregables, políticas de gestión de cambios y requisitos de seguridad para futuros contratos con terceros |  | El dominio 15 del MSPI no ha sido desarrollado. |
| 8. | Diseñar y aplicar anualmente encuestas de satisfacción a usuarios finales, sobre los servicios de TI, orientados a identificar mejoras con respecto a: servicio de soporte, disponibilidad de los recursos, uso responsable de los recursos, conocimiento de las políticas de seguridad, necesidades de capacitación, subutilización de herramientas, redundancia en fuentes de información, requerimientos para minimizar las labores operativas y almacenamiento y disponibilidad de documentos. Con base en los resultados diseñar acciones correctivas e incluirlas en el PETIC del siguiente periodo |  | No se aplican encuestas de satisfacción en la mesa de servicio, las únicas encuestas están orientadas a identificación de intereses de capacitación.    Se mantiene la recomendación en el marco del MSPI. |

**5.1.2.2 Nuevas Recomendaciones 2020**

|  |  |
| --- | --- |
| **N°.** | **Recomendación 2020** |
| 1 | Atender las recomendaciones que se encuentran con flecha roja y/o amarilla del tablero de seguimiento a las recomendaciones 2019. |
| 2 | En las renovaciones de contratos con personas naturales, optimizar las obligaciones especificas y los productos con el fin de garantizar entregables distintos o complementarios. Esto con el fin de optimizar la inversión. Solicitar al responsable del contrato 21 de 2020 la entrega de la declaración de aplicabilidad del MSPI, para identificar productos puntales. |

### 5.1.3 Plan de Administración de Riesgos y Contingencias

#### 5.1.3.1 Administración y tratamiento de Riesgos

 En el marco de la estrategia anticorrupción el IDEP cuenta con los instrumentos *PO- MIC-03-02\_Politica\_Admon\_riesgo\_V1.pdf e IN-MIC-03-04 Instructivo para la administración del riesgo del 2018,* este último menciona los riesgos tecnológicos, pero no los articula con los activos de información de la entidad, conforme a los lineamientos de Gobierno Digital y en especial al MSPI que se basa en la norma ISO 27001:2013, que se adopta en el MANUAL DEL SISTEMA INTEGRADO DE GESTIÓN, con referencia al Subsistema de Gestión de Seguridad de la Información.

 A su vez, el *Seguimiento I Mapa Riesgos Institucional y de Corrupción por Proceso 2020 abril-1\_1.xlsx*, se encuentra diligenciado para el proceso de Gestión Tecnológica y la vigencia 2020 y es objeto de seguimiento trimestral a la implementación de los controles establecidos para el tratamiento de cada uno de los riesgos y su valoración en términos de probabilidad de ocurrencia e impacto de su materialización. En el documento se observa que solo existen cuatro riesgos los cuales no dan cubrimiento a la totalidad de los riesgos tecnológicos y de seguridad de la información de manera alineada con la implementación MSPI, que establece la relación entre los riegos, los activos de información y los controles de la norma ISO 27002:2013. Esto es fundamental para garantizar que se diseñan controles efectivos para dar tratamiento al riesgo y planes de contingencia efectivos en caso de la materialización de los riesgos. Sobre los controles propuestos se emiten algunas observaciones

|  |  |  |
| --- | --- | --- |
| **Riesgo** | **Descripción del control Existente** | **Observación (ver desarrollo en 4.2)** |
| Interrupción en la prestación de servicios tecnológicos a usuarios internos y externos en la entidad | Ejecutar el Plan de contingencia tecnológica | Este control no es de tratamiento sino de contingencia en caso de materialización.    Esto se evidencia en las notas reportadas por la OAP en el monitoreó.    Es preciso resolver la causa raíz de manera definitiva, incrementando el tiempo de autonomía de la UPS de manera proporcional al tiempo requerido en el plan de continuidad para la acción de contingencia.    No se observa la inclusión de un control asociado a planes de continuidad en contratos de servicios SAAS. |
| Realizar Mantenimiento a la infraestructura tecnológica de acuerdo al procedimiento establecido | Aplica ya que es un control preventivo.    Se observa mejora en la construcción de instructivos y manuales sobre cada activo de gestión de operación y seguridad tales como Firewall, Antivirus, Seguridad de dominio y seguridad local de PC´s |

|  |  |  |
| --- | --- | --- |
| **Riesgo** | **Descripción del control Existente** | **Observación (ver desarrollo en 4.2)** |
|  | Realizar seguimiento a los acuerdos de nivel de servicio establecido con cada uno de los proveedores de los sistemas de información | Aplica ya que es un control preventivo.    Se presentan evidencias de seguimiento manual a los ANS, pero no de su integración a la mesa de servicio, ni de las acciones correctivas frente a su incumplimiento. |
| Realizar seguimiento a las actividades programada a ejecutar en la vigencia en el plan de tecnología | Aplica ya que es un control preventivo. |
| La inclusión de garantías del fabricante en los contrates. | Aplica ya que es un control preventivo.    Pero resulta insuficiente, ya que deben incluirse condiciones de contingencia y continuidad en la prestación de servicios por terceros. |
| Acceso restringido a los data center, donde se ubican los servidores, switch, appliance firewall. | Aplica ya que es un control preventivo. |
| Efectuar los pagos de energía de la empresa ENEL - CONDENSA de forma individual por oficina. | No es un control TIC |
| Implementar conexiones tipo VPN y mantener portátiles en óptimas condiciones como elementos que pueden ser prestados | Aplica ya que es un control preventivo.    Sin embargo, no se incluyen los controles de seguridad en los equipos ajenos al IDEP que se conectan a la VPN. |
| Tener ataques informáticos a bases de datos, red de  comunicaciones, sistemas de información y/o página web de la entidad. | Revisar que las políticas del dominio configuradas para que no se permita la instalación de programas en los equipos o servidores del Instituto por un perfil diferente al administrador, está funcionando correctamente. | Los controles aplican ya que son de carácter preventivo y son consecuentes con las recomendaciones del informe de auditoría 2019.    Sin embargo, falta incluir controles de monitoreo tales como los registros de consolas del antivirus, alertas para red y los controles sobre bases de datos y sistemas de información    Las verificaciones de su efectividad de implementación se presentan en el numeral 5.2 |
| Gestionar la consola de administración del antivirus y tomar las acciones correctivas necesarias para garantizar que la herramienta está funcionando correctamente. |
| Configurar el firewall adoptando las categorías identificadas por el fabricante (fortinet), como potencialmente riesgosas, de tal forma que los equipos conectados a la red LAN no tengan acceso a los sitios o aplicaciones que estén en dichas categorías |
| Trámite de reclamos ante la Superintendencia de Industria y Comercio por parte de usuarios del IDEP por no dar respuesta a consultas o reclamos con respecto a la corrección, | Aplicar los lineamientos establecidos en el PRO-GD-07- 14 Atención peticiones, quejas, reclamos y solicitudes y el MN- AC-10-03 Manual para la gestión de peticiones y el MANUAL INTERNO DE POLÍTICAS Y | El control establecido no es de carácter tecnológico, toda vez que el procedimiento no garantiza la protección de las fuentes de datos donde reposan los datos personales.    No se incluyen acciones de protección sobre las bases de datos y archivos que alojan los datos. |

|  |  |  |
| --- | --- | --- |
| **Riesgo** | **Descripción del control Existente** | **Observación (ver desarrollo en 4.2)** |
| actualización o eliminación de datos personales, contraviniendo el artículo el artículo numeral 10  "PROCEDIMIENTO PARA  EL EJERCICIO DE LOS  DERECHOS" | PROCEDIMIENTOS DE  PROTECCIÓN DE DATOS  PERSONALES MN-AC-10-02. |  |
| Actuaciones en contra de la entidad a partir del uso indebido de la información objeto de custodia por el IDEP. | Firma del compromiso de cumplimiento de las políticas TIC del IDEP, en el No. 21. Cumplir con las políticas de seguridad y privacidad y tratamiento de datos personales. | El control establecido no es de carácter tecnológico, toda vez que el procedimiento no garantiza la protección de las fuentes de datos que deben ser custodiados y no se incluyen acciones de protección criptográfica sobre las bases de datos y archivos que alojan los datos. |

La OAP cuenta con el PL-GT-12-05 Plan Tratamiento de riesgos info V5.pdf, de enero de 2020 y el documento de seguimiento al *Plan Tratamiento de riesgos info 2020 Seguimiento II.xlsx* (entregados al auditor). Sobre las actividades de estos documentos se emiten observaciones:

 Las actividades están programadas en la misma franja de tiempo entre junio y diciembre del 2020, sin discriminación de esfuerzo, a excepción de la actividad 1 que inicia en abril de 2020.

 Hay 4 actividades repetidas en este plan y en el Plan de seguridad y Privacidad de la Información:

* Divulgar y gestionar los boletines informativos de seguridad, Integrar con CSIRT de

Gobierno o Identificar y actualizar el inventario con los nuevos AI del Área de Tecnología. o Reportar al director de la Entidad la información recolectada en el instrumento de AI que se identifica y corresponde a las bases de datos del Área de Tecnología.

* Revisar la guía GU-GT-12-01 Guía para la gestión de incidentes de seguridad de la información y el formato FT-GT-12-21 Registro de incidentes de seguridad de la información

 Las actividades incluidas en el Plan no corresponden con los lineamientos del Manual de Gobierno Digital y en especial con el modelo nacional de gestión de riesgos de seguridad digital que establece una interacción con el Modelo de Privacidad y Seguridad de la Información (MPSI); así como la relación con los activos de información que soportan la operación de cualquier Entidad … en todas sus fases o componentes del ciclo PHVA, ya que se centra exclusivamente en una actualización del inventario de activos de información y en el procedimiento de gestión de incidentes de seguridad que atiende únicamente el dominio 16 del MSPI.

 La actividad “Realizar el seguimiento a los riesgos relacionados con seguridad de la información contenidos en el Mapa de Riesgos del IDEP”, resulta insuficiente, toda vez que los 4 riesgos presentados no dan cobertura a la totalidad de los riesgos tecnológicos y/o de seguridad de la información articulados a los activos de información y a los controles MSPI.

 En cuanto a la Revisión y actualización del instrumento de levantamiento de Activos de Información (AI) del Área de Tecnología, se entrego el documento *Base de Datos de Activos de Información Hardware - Software - Servicios.xlsx*, que incluye hardware, software, sistemas de información y servicios, además de incluir la calificación de criticidad, sin embargo, el proceso manifiesta que su actualización está planeada para ser realizada en el tercer trimestre de 2020. Se entrega también el documento *Activos IDEP consolidado VerAdjustada.xlsx,* pero esta mas completo el *Base de Datos de Activos de Información Hardware - Software - Servicios.xlsx.*

 Están correctamente incluidos y catalogados los activos tipo información, en las tres dimensiones de Confidencialidad, Disponibilidad e Integridad, sin embargo, está pendiente el desarrollo del dominio 10 Criptografía del MSPI para su protección en alojamiento y tránsito (correos, carpetas compartidas, etc.)

 Sobre las demás actividades no se presenta evidencia de su cumplimiento y se informa que serán atendidas en el tercer trimestre, pese a que su inicio esta definido para junio de 2020 y la auditoría se realizó en septiembre de 2020.

 La declaración de aplicabilidad del MSPI es el documento que estructura cuales de los 114 controles deberán ser implementados para los riesgos identificados en los 33 Objetivos de control y ese documento no se ha construido en el IDEP, ni su construcción está en los planes de tratamiento de riesgos ni en el de seguridad y privacidad de la información.

 No se incluyen actividades de verificación de la efectividad de controles para el tratamiento de los riesgos, ni acciones de mejora frente a desviaciones. No se incluyen actividades de articulación entre los riesgos aceptados sobre activos críticos, para los cuales deben incluirse planes de contingencia y recuperación en caso de materialización.

#### 5.1.3.2 Plan de Continuidad

La OAP cuenta con el *PL-GT-12-02 Plan Contingencia Tecno V11\_0.pdf* de mayo de 2020 en proceso de actualización, sobre el cual se emiten las siguientes observaciones:

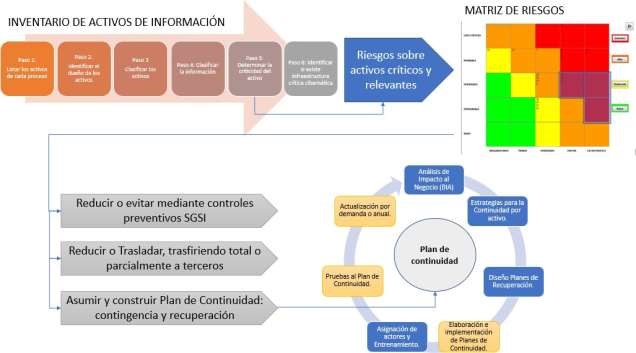
* Se evidencia una mejora en la actualización del documento entre la auditoría 2019 y 2020, específicamente en la inclusión de los demás servicios tecnológicos de la entidad.

* Se han adelantado acciones efectivas de contingencia con el paso de Humano a servicio SAAS (Software as a Service) y de su ambiente contingente al arreglo de hiperconvergencia, además de la unificación de Windows server. Esta nueva estrategia traslada la continuidad del servicio y la generación de backups al proveedor y elimina la dependencia de la infraestructura del IDEP, además de disminuir la carga operativa a los recursos actuales que son limitados para la operación.



Se observa que si bien la obligación 16. del contrato de Humano cita: “Realizar el Monitoreo en el Datacenter que tiene dispuesto Soporte Lógico Ltda. en una disponibilidad de 7x24x365”, la administradora no tiene un usuario de esta plataforma de monitoreo, que permita verificar la disponibilidad contratada y los niveles de ocupación de los recursos para proveer oportunamente requisitos de aprovisionamiento, que si bien se solicita disponibilidad, el contrato no es explicito en cuanto a desempeño e incremento de aprovisionamiento.

Se observa que el *PL-GT-12-02 Plan Contingencia Tecno V11\_0.pdf*, no incluye la relación entre el tratamiento de riesgos y los planes de continuidad, teniendo en cuenta la correlación entre activos – riesgos y planes de contingencia y continuidad. La siguiente imagen presenta un ejemplo de correlación:



 No se ha adelantado un Análisis de Impacto al Negocio BIA como primer paso de la implementación del Plan de Continuidad una vez seleccionados los riesgos extremos asumidos, con el fin de identificar los activos o servicios tecnológicos críticos, y los posibles impactos que se tendrían si éstos no se encuentran disponibles y en correcto funcionamiento:

* + Estimar los tiempos de contingencia y recuperación de los procesos esenciales a su operación normal después que ha ocurrido el incidente invalidante, de acuerdo a la tolerancia de la entidad para operar sin el servicio TIC.

* + Los puntos de recuperación de los datos y condiciones de registro alterno durante contingencia

Evidencia de la falta del análisis BIA, es que para los servicios de BIBLIOTECA DIGITAL

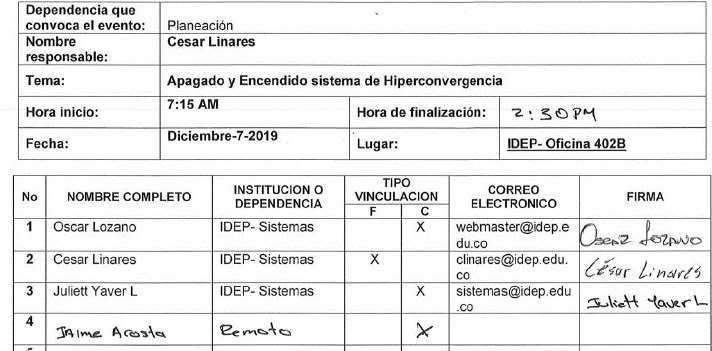
KOHA, SISTEMA WEB OJS, ADMINISTRATIVO Y FINANCIERO GOOBI, SISTEMA DE

INFORMACIÓN NÓMINA HUMANO y DSPACE, se establecen tiempos de entre 21 y 31 días para un proceso de contingencia, sin que estos tiempos hayan sido validados con el negocio.

 Se observa que los planes de acción incluyen tareas de instalación de ambientes y configuración de servicios desde cero, lo cual no corresponde a una contingencia, ya que esta por definición corresponde a “tener listo” un ambiente que permita operar de manera alternativa frente a la falla invalidante y que solo requiera el montaje de datos y gestión de accesos, esa es una causa de los tiempos extremos.

 Se registran tiempos de entre 2 y 3 días para la contingencia de Hiperconvergencia, pese a que las pruebas realizadas en el 2019 evidencian que el proceso tarda aproximadamente 1 día.

Se observa que pese a que los servicios KOHA, OJS Y DSPACE se encuentran sobre la solución de Hiperconvergencia, se establecen planes de continuidad de entre 21 y 31 días, cuando frente a un incidente invalidante la solución más ágil es recuperar la



Hiperconvergencia, dado que al contener snapshot, su recuperación es más ágil y efectiva.

 El anexo 5 incluye un plan de acción para el sistema HUMANO, pese a que actualmente opera como un servicio SAAS y por lo tanto es el proveedor quien garantiza

la continuidad, como se observa en los siguientes apartes de los documentos contractuales:

* ESTUDIOS PREVIOS: Se garantizaría la disponibilidad del servicio de la aplicación Humano 7x24x365, iv) El lDEP contaría con el servicio de Backup Full diario de la información almacenada en disco, Liberando de esta carga a la entidad, v) El lDEP tendría disponible un servidor alterno en las instalaciones de la entidad para atender los eventos de indisponibilidad y para instalar el backup mensual de la información que entregaría el proveedor como parte de sus obligaciones de servicio.
* OBLIGACIONES ESPECIFICAS EP: 14. Disponibilidad de servicio 7 x 24 durante los 365 días del año, 15. Garantizar que el software soporte el IPv6 nativo en coexistencia con el lPv4., 16. Realizar el Monitoreo en el Datacenter que tiene dispuesto Soporte Lógico Ltda. en una disponibilidad de 7x24x365., 17. Realizar la entrega de backup mensual para almacenamiento local. 18. Realizar Backup Full diario de la información almacenada en disco y que pertenece al lDEP.
* OFERTA: La garantía de disponibilidad de la aplicación, es parte de la responsabilidad que Soporte Lógico Ltda. se compromete a ofrecer a sus clientes.

 Los planes de contingencia tanto para fallos en la configuración o fallo total del firewall incluyen las actividades adecuadas y los tiempos estimados son pertinentes. Es importante que en la renovación de los contratos del firewall se mantenga la condición de tener equipos temporales como contingencia en caso de daños en el hardware

 En cuanto al plan de contingencia de la consola del antivirus, es correcto en su plan de acción, pero no se especifica la supervisión y acompañamiento del IDEP a las actividades del proveedor que acceso remoto del antivirus al servidor de dominio.

 El Plan de contingencia no incluye los resultados de los informes de cada plan de acción, como insumos para la actualización y mejora continua del Plan y de la matriz de riesgos.

 Los instructivos relacionados en los planes de contingencia del firewall y base de datos

Oracle: IN-GTH-12-09 INSTRUCTIVO RESTAURACIÓN ARCHIVO DE LA

CONFIGURACIÓN DEL FIREWALL e IN-GTH-12-05 INSTRUCTIVO PARA RESTAURAR

BACKUP MAQUINA – SERVIDOR G4PRUEBAS BASE DE DATOS. no

están publicados, ni fueron entregados a la auditoria, adicionalmente su codificación

"GTH", no concuerda con los instructivos del Gestión Tecnológica "GT”, presumiendo un error de tipografía tampoco concuerda ya que el IN- GT-12-05 publicado, hace referencia al INSTRUCTIVO PARA CAMBIO DE CONTRASEÑA DE INGRESO AL SISTEMA DE INFORMACIÓN GOOBI. De igual manera en el Seguimiento al Plan de Mejoramiento 2019 "*PMX Seguim Control Int 2019 -2 .xls*" se hace referencia al instrutivo:IN-GT-12-04 Instructivo Para Restaurar Backup Maquina – Servidor G4- Pruebas Base De Datos, lo cual confirma la inconsistencia con el código IN-GTH-12-05. Los códigos tampoco coinciden en el FT-MIC-03-08 Listado Maestro Documentos 2019.xls.

Esta situación resulta riesgosa, ya que parte de la efectividad de un plan de contingencia es que los instrumentos y protocolos de operación sean claros y estén disponibles, sin que exista dependencia de personas en particular.

 No se han adelantado las pruebas del plan de continuidad que incluyan simulacros totales de operación en contingencia y (BCP, DRP) para ofrecer evidencia de la verificación, revisión y evaluación de la continuidad de la operación y la seguridad de la información. El proceso manifiesta que se planea realizar una vez se supere la contingencia COVID 19, la cual ha permitido probar la efectividad de los accesos remotos para teletrabajo, cuyos resultados deben ser documentados y presentados como evidencia del Plan de Continuidad.

El plan no incluye las actividades, tiempos y responsables para los planes de recuperación de la operación normal una vez superada la falla que origino la activación de la contingencia.

 El plan debe ser evolucionado a la construcción de los guiones o protocolos de contingencia y recuperación para los diferentes actores, y la sincronización de datos entre los ambientes de contingencia y el retorno a productivo.

#### 5.1.3.3 Procedimientos de Backup y Recuperación

* Se han documentado adecuadamente los procedimientos de Backup y recuperación en el MN-GT-12-08 Manual gestión de backup V1, en el cual se definen correctamente las políticas para backups de las bases de datos de los Servicio Informáticos del IDEP, a los aplicativos de los sistemas de información del IDEP, al dominio Windows, al Firewall, al Sistema de Control Biométrico, a la Consola de antivirus, a carpetas Institucionales. Además de detallar los pasos para la generación y gestión de copias de seguridad para Backup para el Portal WEB Institucional (PWI), a las bases de datos del Portal WEB Institucional (PWI), los Micrositios y las Revistas, las bases de datos Oracle, el aplicativo GOOBI, la biblioteca virtual KOHA, las bases de datos de la biblioteca virtual KOHA, la configuración del Firewall Fortinet, la configuración de la Consola de Antivirus, las carpetas institucionales y al Sistema de Control de Acceso Biométrico.

* En manual para la gestión de backup, también se encuentran detallados correctamente los procedimientos para realizar las pruebas de recuperación de las copias de seguridad que se generan.

* Las copias de seguridad se están almacenando en los propios servidores donde se generan, en las carpetas de backups del servidor de archivos y en medios externos, lo que garantiza la posibilidad de obtener las copias desde diferentes medios. Se documentó de forma adecuada el almacenamiento de la información que generan los usuarios en las carpetas compartidas (IN-GT-12-02 Instructivo para el almacenamiento de información en Carpetas Compartidas V1), teniendo en cuenta la estructura definida en las tablas de retención documental, donde se define las reglas, condiciones y proceso de almacenamiento de esta información y que además es objeto de copia de seguridad semanal.



El tiempo de realización de las pruebas de restauración es el mismo para todos los elementos a los que se les genera copias de seguridad: “*por lo menos una vez en cada vigencia”*, esto implica muy pocas pruebas para objetos de backups que deben verificarse por lo menos una vez al mes, tales como las bases de datos que contienen información y transacciones diarias, que en caso de contingencia al no verificar si hay daños en las copias de seguridad podrían ocasionar perdida de información y/o retrabajos para su restauración. Para objetos tales como firewall, consola de antivirus, dominio, objetos que no tienen alta modificación es pertinente una única prueba anual.

 Si bien la documentación y estrategias de copias de seguridad es correcta, debe complementarse con un formato de Plan de Backups único que permita identificar, en un único documento, de forma rápida y clara todos los objetos a los que se les está generando copias de seguridad, sus frecuencias, tiempos de retención, responsables, etc. que además permita encontrar la disposición final de todas las copias de seguridad de la información respaldada rápidamente para así poder recuperarla en forma ágil y oportuna. Un ejemplo de lo que debe tener este formato es el siguiente:





La generación de las copias de seguridad depende en su gran mayoría a procesos manuales, ejecución de scripts y copia de información por parte de los funcionarios y contratista de OAP, lo cual implica una asignación y disponibilidad por parte de ellos para su ejecución, estos tiempos y disponibilidad podría disminuirse con el uso o adquisición de herramienta automatizadas, que a su vez garanticen la ejecución completa de estos procesos, sin depender de la disponibilidad del personal. Cabe anotar que esto no implica que actualmente no se estén realizando correctamente estas labores.



Si bien se cuenta con un almacenamiento externo para las copias de seguridad en la sede de la SDE, no existe un registro y codificación documentada de los medios que se trasladan a esta sede. Al tener espacio ilimitado en las unidades de nube con Google (Drive), y debido a que el almacenamiento en la nube implica una disponibilidad y acceso a la información permanente, debería utilizarse este recurso como complemento de la estrategia de actual, programando tareas nocturnas de sincronización de la carpeta de Backups del servidor de archivos y así tener otro medio de almacenamiento alterno y con disponibilidad permanente y sin restricciones geográficas.

**5.1.3.4 Seguimiento a Recomendaciones 2019**



|  |  |  |  |
| --- | --- | --- | --- |
| **N°.** | **OBSERVACIÓN** |  | **SEGUIMIENTO** |
| 1. | Se establezcan actividades de prueba y verificación sobre los controles establecidos en la matriz de riesgos y las acciones del Plan de mejoramiento como requisito para dar por cerrada una acción o una actividad de control.    Priorizar las acciones de acuerdo con el impacto para la entidad de su no ejecución, aplicar el mismo criterio para las decisiones de eliminación de acciones. |  | Si bien se registran las acciones en el caso de los riesgos materializados, no se presentó evidencia de trazabilidad con pruebas técnicas.  No ha avanzado |
| 2. | En el marco de la implementación del MSPI actualizar la identificación de la matriz de riesgos de acuerdo con los activos de información y depurar las acciones y controles reportados de acuerdo con las configuraciones de dichos controles en la plataforma TIC. Seguir los lineamientos de la Guía 7.    Actualizar el Plan de Continuidad para que coincida en lo relacionado con el plan de tratamiento de riesgos, el formato de matriz de riesgos y la tipología de los riesgos.    Cabe anotar que el Plan de Continuidad está directamente relacionado con los riesgos que la entidad ha decidido tratar mediante aceptación |  | La recomendación puntual no ha sido atendida.    Cabe anotar que el Plan de Continuidad ha tenido mejoras, relacionadas en este capítulo |
| 3. | De ser posible fortalecer el conocimiento en seguridad de la información del funcionario de la OAP o mejorar el perfil en esta materia para los contratistas. |  | En el plan de mejoramiento 2019, se registran evidencias de capacitaciones recibidas por parte de los proveedores, sin embargo, en las entrevistas realizadas, se observa que el conocimiento no es aún del 100% y debe continuarse su fortalecimiento, aún más teniendo en cuenta que le ha sido asignado rol de oficial de Seguridad. |
| 4. | Ajustar el Plan de contingencias para que incluya como mínimo:   * Todos los activos de información   críticos   * Los acuerdos ANS alcanzados con los responsables de procesos * Incluir respaldo de elementos de configuración de la plataforma TIC que permitan ya sea contar con |  | Se observan mejoras en la cobertura de servicios tecnológicos en la versión 2020.    Están pendientes los otros elementos de la recomendación. |



|  |  |  |  |
| --- | --- | --- | --- |
| **N°.** | **OBSERVACIÓN** |  | **SEGUIMIENTO** |
|  | ambientes replica o agilizar los tiempos de puesta en operación de la contingencia.   * Ajustar las actividades y planes de contingencia específicos conforme a los acuerdos alcanzados con el negocio * Incluir los planes de recuperación a la operación normal con tiempos y responsables |  |  |
| 5. | Adelantar las pruebas integrales al Plan de Continuidad y documentar los protocolos y resultados, contemplar los lineamientos de  ISO 27002:2013 en el control 17.1.3  Verificación, revisión y evaluación de la continuidad de la seguridad de la información |  | En el año 2019 se realizaron pruebas de hiperconvergencia y con el sistema Goobi, pero no pruebas integrales del Plan de Contingencia y recuperación.  A la fecha no ha sido desarrollado el control MSPI 17.1.3. |
| 6. | Incluir en el inventario de programación de copias de respaldo el Backup de los archivos de configuración de los sistemas manejadores de bases de datos (RDBMS) |  | Al contar con los *snapshots* de las máquinas virtuales de la hiperconvergencia en donde se encuentran las bases de datos y sus manejadores se está cumpliendo con esta recomendación, el proceso esta  correctamente documentado en el manual de gestión de backups. |
| 7. | En el marco de la implementación MSPI dominio 12.3 documentar las políticas, procedimientos e instructivos de gestión de copias de respaldo y recuperación. |  | Se adelantaron los siguientes documentos como cumplimiento de esta recomendación:   * MN-GT-12-08 Manual gestión de backup V1 * IN-GT-12-02 Instructivo para el almacenamiento de información en Carpetas Compartidas V1   Se hace referencia a los instructivos no publicados, ni entregados a la auditoria:   * IN-GT-12-03 Instructivo Para Realizar El Backup Del Servidor Hp Ml370 G4 - Base De Datos Oracle * IN-GT-12-04 Instructivo Para Restaurar Backup Maquina – Servidor G4- Pruebas   Base De Datos |
| 8. | Incluir en los estudios previos de la adquisición de la herramienta de Backup, la configuración optima de la consola por parte del proveedor y la transferencia de conocimiento para establecer procedimientos efectivos de programación de copias de respaldo, suficiencia en la cobertura, control y monitoreo de logs, acciones correctivas oportunas y pruebas de restauración. |  | En el PETI actualizado a la vigencia 2020, se incluye el análisis DOFA del proyecto para adquirir herramienta de backup debido a la ausencia de un sistema automático de copias de seguridad o de respaldo de la información y bases de datos institucionales. Los procesos de backup de sistemas de información y bases de datos se realizan de manera manual.  Sin embargo, aún no se ha adquirido la herramienta |

#### 5.1.3.5 Nuevas Recomendaciones 2020

|  |  |
| --- | --- |
| **N°.** | **Recomendación 2020** |
| 1. | Actualizar los documentos relacionados con el tratamiento de riesgos para que se articule con las directrices del MSPI, especialmente en la relación de los riesgos TIC con los activos de información críticos y los controles ISO 27002:2013.    De igual manera, relacionar el cumplimiento del tratamiento de riesgos TIC y de seguridad digital como parte inherente del sistema de gestión de seguridad de la información que hace parte integral del Sistema integrado de gestión de la entidad. |
| 2. | Actualizar la matriz de riesgos dando cobertura a los activos críticos y su relación con los objetivos de control MSPI |
| 3. | Actualizar el Plan de tratamiento de riesgos, con las actividades tendientes a dar cumplimiento a los lineamientos del Manual de Gobierno Digital y en especial con el modelo nacional de gestión de riesgos de seguridad digital que establece una interacción con el Modelo de Privacidad y Seguridad de la Información (MPSI); así como la relación con los activos de información que soportan la operación de la Entidad … en todas sus fases o componentes del ciclo PHVA |
| 4. | Articular el Plan de Continuidad al Plan de tratamiento de Riesgos y garantizar que los instrumentos documentales e insumos sean consecuentes en su nominación y su ubicación. |
| 5. | Adelantar el Análisis de Impacto al Negocio BIA para establecer los tiempos, los protocolos de contingencia y recuperación y las estrategias de fidelidad de la data entre ambientes.  Actualizar el Plan de continuidad de acuerdo con los resultados del BIA y con las inconsistencias relacionadas en el presente informe.  El siguiente es un modelo de tiempos a establecer |
| 6. | En los futuros contratos de sistemas de información en modalidad SAAS, incluir el acceso del IDEP a la s plataformas de monitoreo, el aprovisionamiento sin costo para mantener el desempeño esperado y condiciones de contingencia frente a siniestros. Si es posible solicitar certificaciones TIER de los ambientes en hosting. |
| 7. | Atende las recomendaciones 2019, que se reportan en rojo o amarillo. |

### 5.1.4 Modelo de Seguridad y Privacidad de la Información

El modelo de seguridad y privacidad de la información en adelante MSPI, cuyos lineamientos establecen las directrices para la implementación del habilitador trasversal de Seguridad de la información de la Política de Gobierno Digital, busca la implementación de los lineamientos de seguridad de la información en todos sus procesos, servicios tecnológicos,

sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad y disponibilidad y privacidad de los datos, mediante la aplicación de un proceso de gestión efectiva del riesgo.

Este habilitador tiene como resultado el Sistema de Gestión de Seguridad de la Información, basado en la norma ISO 27001:2013 y que debe estar articulado con el Sistema de Gestión Integral de la entidad, pero también implica la configuración tecnología de los controles en la plataforma de servicios tecnológicos y un proceso de concientización y sensibilización que garanticen la apropiación de la seguridad como un componente de la cultura organizacional.

Así las cosas, el IDEP adopta el MSPI basado en la norma ISO 27001:2013, en el MANUAL

DEL SISTEMA INTEGRADO DE GESTIÓN, con referencia al Subsistema de Gestión de Seguridad de la Información.

Se emiten a continuación las observaciones de cumplimiento a este habilitador de Gobierno Digital y subsistema declarado por la entidad:

 El IDEP cuenta con una política general de seguridad de la información *PO-GT-12-01 Política seguridad privacidad info V3.pdf*, con fecha de mayo de 2019, cuyo contenido aún no se encuentra articulado a los lineamientos establecidos por MINTIC en el MSPI. El documento no describe las políticas de seguridad adoptadas por la entidad, únicamente menciona un listado de instrumentos que no coinciden con el listado del *FT- MIC-03-08 Listado Maestro Documentos 2019.xls* publicado por la entidad, no incluye marco normativo, no hace referencia a Gobierno digital y Seguridad Digital y adolece de los elementos puntuales que direccionan la actuación de los funcionarios, contratistas y proveedores en el uso y responsabilidad sobre los activos de información y privilegios.

 Por otra parte, el documento “*FT-GT-12-20 Compromiso política tic V2.docx*”, si incluye algunas políticas validas y ha sido objeto de socialización y suscripción por parte de los usuarios, lo cual representa un avance importante en la concientización, educación y capacitación sobre la seguridad de la información (control 7.2.2 ISO 27002:2013). Vale aclarar que, si bien la concientización es importante, también lo es que las políticas registradas sean consecuentes con los controles implementados en la plataforma tecnológica. Los hallazgos en esta materia se señalan en el numeral 5.2

 Como instrumentos de planeación y seguimiento se cuenta con el PL*-GT-12-04 Plan Seguridad y Privacidad de la Info V5.pdf* de enero de 2020 y el *Plan Seguridad y Privacidad de la Info 2020 Seguimiento II.xlsx* revisado de manera trimestral. Estos documentos en primera instancia no son coincidentes y si bien incluyen unas primeras actividades de acercamiento a la implementación del MSPI, que hacen parte de la implementación, adolecen de las siguientes etapas requeridas para la implementación de MSPI:

* Documentación de la Declaración de Aplicabilidad con la elaboración del marco documental de políticas, procedimientos, instructivos y formatos, incluyendo claramente las justificaciones y soportes para la exclusión de controles.

* El levantamiento y planeación de los documentos comunes en el sistema integrado de gestión y la planeación de la salida escalonada de documentos de acuerdo al avance en implementación. o Un programa de programa de concientización, educación y capacitación sobre la seguridad de la información (control 7.2.2 ISO 27002:2013). Junto a un plan de gestión del cambio asociado a las restricciones de las políticas y los nuevos procedimientos. Esto articulado con el dominio de uso y apropiación del MRAE.
* Implementación de los controles de seguridad de la información en la plataforma TIC de manera incremental y verificación técnica de vulnerabilidades.

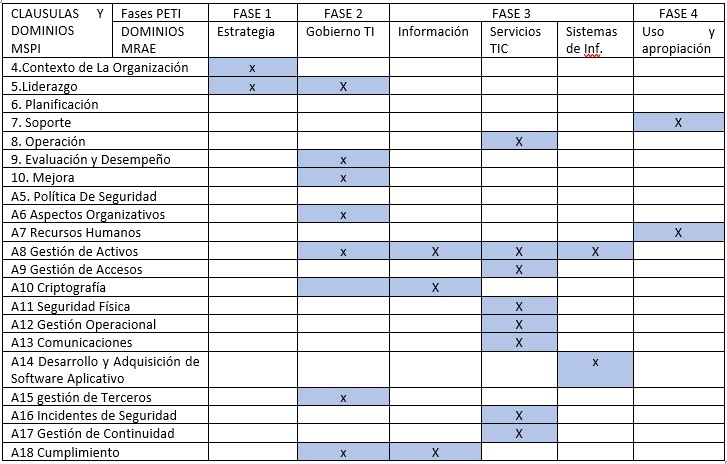
 El Plan solo incluye las siguientes actividades para las cuales no se observa un análisis de esfuerzo ya que están programadas en bloques de tiempo. Las acciones aportan más no cubren a 9 elementos del MSPI, que está conformado por 6 clausulas principales y 14 dominios con 114 controles. Sobre ellas se emiten las siguientes observaciones y las que presentan avance se muestran sombreadas:

|  |  |  |
| --- | --- | --- |
| **ACTIVIDAD PLAN V5 EN PDF** | **ACTIVIDAD SEGUIMIENTO PLAN EN**  **EXCEL** | **OBSERVACION DE AUDITORÍA** |
| Socializar la política de seguridad de la información del IDEP | Revisar y Actualizar la Política de Seguridad de la Información | Dado que la política de seguridad de la información ya publicada, está incompleta, se requiere de una actividad previa de actualización. |
|  | Publicar la política de seguridad de la información del IDEP en el portal web de la entidad |
| Gestionar la suscripción del compromiso de cumplir con las políticas de seguridad de la información por parte de los nuevos funcionarios y contratistas del IDEP | Gestionar la suscripción del compromiso de cumplir con las políticas de seguridad de la información por parte de los  nuevos funcionarios y contratistas del IDEP | Esta actividad es relevante para las acciones de concientización, sensibilización y capacitación del MSPI. Clausula 7 norma principal  Se entregan evidencias de avance |
|  | Determinar el nivel de madurez en el que se encuentra la entidad en cuanto al Modelo de Seguridad y Privacidad de la  Información en cada ítem de Gestión | No se obtuvo evidencia del diligenciamiento del instrumento de autoevaluación MSPI dispuesto por Mintic. |
| Mantener actualizado el inventario de activos de información | Revisión y actualización del instrumento de levantamiento de AI del Área de Tecnología. | Esta actividad es relevante, pero se informa que el documento Base de Datos de  Activos de Información  Hardware - Software - Servicios.xlsx se actualizará en el tercer trimestre. |
| Socializar el instrumento de levantamiento de AI del Área de Tecnología al jefe de la oficina de planeación. |
| Identificar y actualizar el inventario con los nuevos AI del Área de Tecnología. |
| Realizar informe de actualización a los AI del Área de Tecnología, indicando la novedad de la modificación según sea (Actualizaciones al proceso al que pertenece el AI, Incluir un nuevo AI, |

|  |  |  |
| --- | --- | --- |
| **ACTIVIDAD PLAN V5 EN PDF** | **ACTIVIDAD SEGUIMIENTO PLAN EN**  **EXCEL** | **OBSERVACION DE AUDITORÍA** |
|  | Cambios o migraciones de Sistemas de Información (SI) en donde se almacenan o reposan AI, Materialización de riesgos que cambien la criticidad del AI). |  |
| Publicar el Registro AI del Área de  Tecnología en el portal web del IDEP. |
| Reportar al director de la Entidad la información recolectada en el instrumento de AI que se identifica y corresponde a las bases de datos del Área de Tecnología. |
| Instalar y poner en funcionamiento la solución de copias de respaldo para la información del IDEP | Instalar y poner en funcionamiento la solución de copias de respaldo para la información del IDEP | Esta actividad aporta a la implementación del objetivo de control 12.3 del MSPI, pero debe acompañarse de los procedimientos y formatos de planeación, bitácora de eventos y restauración. |
| Ejecutar el plan para la transición de servicios de TIC, del protocolo de  internet IPV4 a IPV6 en el IDEP | Ejecutar el plan para la transición de servicios de TIC, del protocolo de internet IPV4 a IPV6 en el IDEP | Esta actividad aporta a la implementación de los dominios 12 y 13 del MSPI |
| Implementar una solución para cubrir los fallos de energía en el centro de cómputo del IDEP Implementar el plan para renovación de la infraestructura TIC del IDEP clasificada como obsoleta o aquella que no tenga respaldo del fabricante (servidores) | Implementar el plan para renovación de la infraestructura TIC del IDEP clasificada como obsoleta o aquella que no tenga respaldo del fabricante  (servidores) | Esta actividad aporta a la implementación del dominio  11 y 17 |
| Realizar la migración de las bases de datos Oracle a un servidor con soporte del fabricante |
|  | Revisar la guía GU-GT-12-01 Guía para la gestión de incidentes de seguridad de la información y el formato FT-GT-12-21 Registro de incidentes de seguridad de la información | Esta actividad aporta a la implementación del dominio 16 |
| Socializar el procedimiento a los colabores del IDEP |
|  | Divulgar y gestionar los boletines informativos de seguridad, Integrar con CSIRT de Gobierno | Aporta a la clausula 7 de la norma principal |
|  | Revisar y actualizar la documentación relacionada con la recolección de bases | Esta actividad aporta a la implementación del dominio 8 |

|  |  |  |
| --- | --- | --- |
| **ACTIVIDAD PLAN V5 EN PDF** | **ACTIVIDAD SEGUIMIENTO PLAN EN**  **EXCEL** | **OBSERVACION DE AUDITORÍA** |
|  | de datos personales de acuerdo a los estándares emitidos por la SIC |  |
| Revisar la información de las bases de los datos registrados en la SIC con los responsables de las mismas, para definir si requieren o no modificaciones. |
| Actualizar y registrar la información de las bases de datos modificadas, registradas en el SIC |
|  | Revisar los indicadores del PSPI del IDEP | Aporta a la cláusula 9 de la norma principal |
| Reportar indicadores del PSPI del IDEP |
|  | Definir un formato para documentar las Necesidades del Usuario. | Aporta al dominio 14 del MSPI. |
| Definir un procedimiento para llevar a cabo el proceso de mantenimiento al Ciclo de Vida del Software que realizarán los proveedores de los sistemas de información en coordinación con el IDEP. |
| Definir un Formato para el levantamiento de Requerimientos. |
| Realizar un procedimiento para la puesta en producción de los sistemas de información en el IDEP. |
| Definir un formato para el control de cambios del sistema de información que se da por cambios normativos o necesidades de los usuarios a una funcionalidad en producción. |
|  | Crear Servidor Web Virtual | Aporta al dominio 12 del  MSPI |
| Instalar Sistema Operativo Linux |
| Instalación Govimentum 2 / Drupal 8 |
| Afinamiento Instalación Govimentum 2- FURAG Accesibilidad y Usabilidad. |

 Los Planes entregados no evidencian articulación entre el MSPI y el MRAE como se espera en Gobierno digital. La siguiente imagen muestra este tipo de articulación.





Los siguientes documentos identificados en la auditoria, no han sido asociados a una Declaración de Aplicabilidad del MSPI, el cual se constituye en el instrumento que determina el alcance de la implementación. A continuación, se presenta la asociación del dominio al que podría relacionarse cada documento, con la salvedad de que los documentos que se enuncian deben ser revisados y articulados al MSPI. Se incluye además una columna que especifica si el documento estaba publicado o si por el contrario fue incluido en la presente relación:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CÓDIGO** | **NOMBRE DEL DOCUMENTO** | **Publicado** | **MSPI**  **Dominio/**  **Clausula** | **ESTADO** |
| CR-GT-12-01 | Caracterización de Gestión Tecnológica | Si | 6 | Vigente |
| PRO-GT-12-01 | Administración de Servidores | Si | 12 | Obsoleto |
| PRO-GT-12-02 | Asignación de Usuarios | Si | 9 | Obsoleto |
| PRO-GT-12-04 | Protección del intercambio de información | Si | 12 | Obsoleto |
| PRO-GT-12-05 | Mantenimiento de Infraestructura y Servicios de  Tecnología | Si | 12 | Vigente |
| PRO-GT-12-07 | Registro de Activos de Información Tipo Software, Hardware y Servicios | Si | 8 | Vigente |
| PRO-GT-12-08 | Formulación y Seguimiento del PETIC | Si | Cláusula 5 | Vigente |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CÓDIGO** | **NOMBRE DEL DOCUMENTO** | **Publicado** | **MSPI**  **Dominio/**  **Clausula** | **ESTADO** |
| PRO-GT-12-09 | Monitoreo Uso de los Medios de Almacenamiento | Si | 12 | Obsoleto |
| PRO-GT-12-10 | Mesa de Servicios | Si | 12 | Vigente |
| PO-GT-12-01 | Política de seguridad y privacidad de la información | Si | 5 | Vigente |
| PL-GT-12-01 | Plan Estratégico de Tecnologías de la Información y Comunicaciones 2017 | Si | 6 | Vigente |
| PL-GT-12-02 | Plan de Contingencia Tecnológica IDEP | Si | 17 | Vigente |
| PL-GT-12-03 | Plan de monitoreo anual de uso de recursos tecnológicos | Si | 12 | Obsoleto |
| PL-GT-12-04 | Plan de Seguridad y Privacidad de la Información - IDEP | Si | 5 | Vigente |
| PL-GT-12-05 | Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – IDEP | Si | Cláusula 8, 9 | Vigente |
| MN-GT-12-01 | Manual del soporte de primer nivel y administración del antivirus | Si | 12 | Vigente |
| MN-GT-12-02 | Manual del soporte de primer nivel y administración del firewall | Si | 12 | Vigente |
| MN-GT-12-03 | Manual del soporte del primer nivel y administración para la hiperconvergencia | Si | 12 | Vigente |
| MN-GT-12-04 | Manual para la administración de usuarios que se vinculan a los sistemas de información o servicios tecnológicos del IDEP | Si | 9 | Vigente |
| MN-GT-12-05 | Manual para la administración del dominio Windows directorio activo y DNS del IDEP | Si | 12 | Vigente |
| MN-GT-12-06 | Manual del proceso actualización servidores  Linux (parches del sistema operativo) de los servicios web, micrositios, Koha y ojs. | Si | 12 | Vigente |
| MN-GT-12-07 | Manual para la administración de la red LAN del IDEP y políticas de seguridad | Si | 13 | Vigente |
| MN-GT-12-08 | Manual para la gestión de back up del IDEP. | Si | 12 | Vigente |
| MN-GT-12-09 | Manual para la administración y soporte de primer nivel del sistema de información humano | Si | 14 | Vigente |
| MN-GT-12-10 | Manual para la gestión del servicio tecnológico misional OJS | Si | 14 | Vigente |
| MN-GT-12-11 | Manual para la gestión del servicio tecnológico misional KOHA | Si | 14 | Vigente |
| MN-GT-12-12 | Manual para la administración y soporte de primer nivel del sistema de información GOOBI | NO | 14 |  |
| MN-GT-12-13 | Manual para la gestión del servicio tecnológico misional Dspace | NO | 14 |  |
| MN-GT-12-14 | Manual para la gestión y administración de los servidores físicos y virtuales del IDEP | NO | 12 |  |
| IN-GT-12-01 | Instructivo para la Asignación de Usuarios | Si | 9 | Vigente |
| IN-GT-12-02 | Instructivo para el almacenamiento de la información en carpetas compartidas | Si | 8 | Vigente |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CÓDIGO** | **NOMBRE DEL DOCUMENTO** | **Publicado** | **MSPI**  **Dominio/**  **Clausula** | **ESTADO** |
| IN-GT-12-03 | Instructivo Para Realizar El Backup Del Servidor Hp Ml370 G4 - Base De Datos Oracle | Si | 12 | Vigente |
| IN-GT-12-04 | Instructivo Para Restaurar Backup Maquina – Servidor G4- Pruebas Base De Datos | Si | 12 | Vigente |
| IN-GT-12-05 | Instructivo Para Cambio De Contraseña De Ingreso Al Sistema De Información Goobi | Si | 9 | Vigente |
| IN-GT-12-06 | Instructivo para cambio de contraseña Sistema Humano. | Si | 9 | Vigente |
| IN-GT-12-07 | Instructivo proceso de actualización sistemas Goobi y humano. | Si | 14 | Vigente |
| GU-GT-12-01 | Guía para la gestión de incidentes de seguridad de la información. | Si | 16 | Obsoleto |
| FT-GT-12-07 | Reporte de garantías de equipos | Si | 15 | Obsoleto |
| FT-GT-12-08 | Reporte de fallas en aplicativos y/o servidores | Si | 17 | Obsoleto |
| FT-GT-12-09 | Hoja de vida de computador - actualización de datos | Si | 8 | Obsoleto |
| FT-GT-12-12 | Hoja de vida de impresoras | Si | 8 | Obsoleto |
| FT-GT-12-16 | Control backups y revisión de servidores | Si | 12 | Vigente |
| FT-GT-12-17 | Reporte mantenimiento equipos | Si | 11 | Obsoleto |
| FT-GT-12-18 | Reporte mantenimiento impresoras | Si | 11 | Obsoleto |
| FT-GT-12-19 | Inventarios activos de información Tipo Software, Hardware y Servicios IDEP | Si | 8 | Vigente |
| FT-GT-12-20 | Compromiso de cumplimiento de las políticas  TIC del IDEP | Si | 6 | Vigente |
| FT-GT-12-21 | Registro de incidentes de seguridad de la información | Si | 16 | Vigente |
| FT-GT-12-22 | Levantamiento Necesidades SI. | NO | 14 |  |
| FT-GT-XX-XX | Especificación Requerimientos SI. | NO, en proceso de construcción. | 14 |  |

 Aunque los anteriores documentos no han sido articulados al MSPI, se destaca el avance en su construcción y en el aporte que significan a la gestión de conocimientos de la función tecnológica de la entidad. Se evidencia el interés y dedicación de los recursos del área por construir instrumentos.



En las inspecciones de seguridad realizadas por el auditor se identificaron algunas debilidades que se presentan en la plataforma tecnológica (ver 5.2)

**5.1.4.1 Seguimiento a Recomendaciones 2019**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **N°.** | **Recomendación 2019** |  | **Seguimiento 2020** | | | |
| 1. | Continuar la implementación del modelo MSPI dando prioridad a:   * Optimización del inventario de activos * Identificación y valoración de riesgos por objetivos de control * Levantamiento de la declaración de   aplicabilidad   * La elaboración del marco documental de políticas, procedimientos, instructivos y formatos alineados a los controles aplicables * Fortalecer la política de seguridad de la información con los elementos puntuales que direccionan la actuación de los funcionarios, contratistas y proveedores en el uso y responsabilidad sobre los activos de información y privilegios. * Adelantar un programa de programa de concientización, educación y capacitación sobre la seguridad de la información (control 7.2.2 ISO 27002:2013) y entregar formalmente la política. * Adelantar los planes de Implementación de los controles de seguridad de la   información en la plataforma TIC  Se recomienda adelantar una inspección de análisis de vulnerabilidades una vez finalizada la implementación para verificar su eficacia. |  | Se evidencian algunas mejoras en la construcción de instrumentos documentales y en el formato y valoración del inventario de activos.    De igual manera, se han realizado acciones para socializar y formalizar el cumplimiento de políticas de seguridad.    Sin embargo, todavía no se evidencia la existencia de un Plan de Implementación de MSPI detallado para lograr las 4 dimensiones.  Tener en cuenta que la implementación de los dominios no se realiza por orden de la norma, sino de acuerdo a los esfuerzos de su implementación, sensibilización y puesta en operación real. | | | |
|  | Declaración de aplicabilidad para el alcance de instrumentos | Identificación de elementos de articulación con  SIG y con el  MRAE |  |
| Gestión del cambio y del conocimiento | Implementación tecnológica de los controles |

#### 5.1.4.2 Nuevas Recomendaciones 2020

|  |  |
| --- | --- |
| **N°.** | **Recomendación 2020** |
| 1. | Atende las recomendaciones 2019, que se reportan en rojo o amarillo. |
| 2. | En el marco de atención del MSPI, al elaborar la declaración de aplicabilidad, definir el inventario de documentos que deben ser elaborados para atender los controles de la norma que sean aplicables. A continuación, se adjunta una relación resumen de los controles ISO 27002:2013 |

**ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES**

1. **POLÍTICAS DE SEGURIDAD.** 5.1 Directrices de la Dirección en seguridad de la información.

5.1.1 Conjunto de políticas para la seguridad de la información.

5.1.2 Revisión de las políticas para la seguridad de la información.

1. **ASPECTOS ORGANIZATIVOS DE**

**LA SEGURIDAD DE LA INFORMAC.**

* 1. Organización interna.
     1. Asignación de responsabilidades para la segur. de la información.
     2. Segregación de tareas.
     3. Contacto con las autoridades.
     4. Contacto con grupos de interés especial.
     5. Seguridad de la información en la gestión de proyectos.
  2. Dispositivos para movilidad y teletrabajo.

* + 1. Política de uso de dispositivos para movilidad. 6.2.2 Teletrabajo.

1. **SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.** 
   1. Antes de la contratación.
      1. Investigación de antecedentes. 7.1.2 Términos y condiciones de contratación.
   2. Durante la contratación.
      1. Responsabilidades de gestión. 7.2.2 Concienciación, educación y capacitación en segur. de la informac.

7.2.3 Proceso disciplinario.

* 1. Cese o cambio de puesto de trabajo.
     1. Cese o cambio de puesto de trabajo.

1. **GESTIÓN DE ACTIVOS.** 
   1. Responsabilidad sobre los activos.
      1. Inventario de activos.
      2. Propiedad de los activos.
      3. Uso aceptable de los activos.
      4. Devolución de activos.
   2. Clasificación de la información.
      1. Directrices de clasificación.
      2. Etiquetado y manipulado de la información. 8.2.3 Manipulación de activos. 8.3 Manejo de los soportes de almacenamiento.
      3. Gestión de soportes extraíbles.
      4. Eliminación de soportes.
      5. Soportes físicos en tránsito.
2. **CONTROL DE ACCESOS.** 
   1. Requisitos de negocio para el control de accesos. 9.1.1 Política de control de accesos.

9.1.2 Control de acceso a las redes y servicios asociados. 9.2 Gestión de acceso de usuario. 9.2.1 Gestión de altas/bajas en el registro de usuarios.

* + 1. Gestión de los derechos de acceso asignados a usuarios.
    2. Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios.
    3. Revisión de los derechos de acceso de los usuarios.
    4. Retirada o adaptación de los derechos de acceso 9.3 Responsabilidades del usuario.

9.3.1 Uso de información confidencial para la autenticación.

9.4 Control de acceso a sistemas y aplicaciones.

* + 1. Restricción del acceso a la información.
    2. Procedimientos seguros de inicio de sesión.
    3. Gestión de contraseñas de usuario.

* + 1. Uso de herramientas de administración de sistemas.
    2. Control de acceso al código fuente de los programas.

1. **CIFRADO.** 
   1. Controles criptográficos.
      1. Política de uso de los controles criptográficos. 10.1.2 Gestión de claves.
2. **SEGURIDAD FÍSICA Y AMBIENTAL.** 
   1. Áreas seguras.
      1. Perímetro de seguridad física.
      2. Controles físicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos.

11.1.4 Protección contra las amenazas externas y ambientales. 11.1.5 El trabajo en áreas seguras.

11.1.6 Áreas de acceso público, carga y descarga. 11.2 Seguridad de los equipos.

* + 1. Emplazamiento y protección de equipos.
    2. Instalaciones de suministro.
    3. Seguridad del cableado.
    4. Mantenimiento de los equipos. 11.2.5 Salida de activos fuera de las dependencias de la empresa.
    5. Seguridad de los equipos y activos fuera de las instalaciones.
    6. Reutilización o retirada segura de dispositivos de almacenamiento.
    7. Equipo informático de usuario desatendido.
    8. Política de puesto de trabajo despejado y bloqueo de pantalla. **12. SEGURIDAD EN LA OPERATIVA.** 12.1 Responsabilidades y procedimientos de operación. 12.1.1 Documentación de procedimientos de operación.
    9. Gestión de cambios.
    10. Gestión de capacidades.
    11. Separación de entornos de desarrollo, prueba y producción. 12.2 Protección contra código malicioso.

12.2.1 Controles contra el código malicioso. 12.3 Copias de seguridad.

12.3.1 Copias de seguridad de la información.

12.4 Registro de actividad y supervisión.

* + 1. Registro y gestión de eventos de actividad.
    2. Protección de los registros de información.
    3. Registros de actividad del administrador y operador del sistema.
    4. Sincronización de relojes. 12.5 Control del software en explotación.

12.5.1 Instalación del software en sistemas en producción.

12.6 Gestión de la vulnerabilidad técnica.

* + 1. Gestión de las vulnerabilidades técnicas.
    2. Restricciones en la instalación de software.

12.7 Consideraciones de las auditorías de los sistemas de información.

12.7.1 Controles de auditoría de los sistemas de información.

1. **SEGURIDAD EN LAS**

**TELECOMUNICACIONES.**

* 1. Gestión de la seguridad en las redes. 13.1.1 Controles de red.

13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.1.3 Segregación de redes.

* 1. Intercambio de información con partes externas.
     1. Políticas y procedimientos de intercambio de información.
     2. Acuerdos de intercambio.
     3. Mensajería electrónica.
     4. Acuerdos de confidencialidad y secreto.

1. **ADQUISICIÓN, DESARROLLO Y**

**MANTENIMIENTO DE LOS SISTEMAS**

**DE INFORMACIÓN.**

* 1. Requisitos de seguridad de los sistemas de información.
     1. Análisis y especificación de los requisitos de seguridad. 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.

14.1.3 Protección de las transacciones por redes telemáticas.

* 1. Seguridad en los procesos de desarrollo y soporte.
     1. Política de desarrollo seguro de software.
     2. Procedimientos de control de cambios en los sistemas.
     3. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
     4. Restricciones a los cambios en los paquetes de software.
     5. Uso de principios de ingeniería en protección de sistemas.
     6. Seguridad en entornos de desarrollo.
     7. Externalización del desarrollo de software.
     8. Pruebas de funcionalidad durante el desarrollo de los sistemas.
     9. Pruebas de aceptación.
  2. Datos de prueba.
     1. Protección de los datos utilizados en pruebas.

1. **RELACIONES CON SUMINISTRADORES.** 
   1. Seguridad de la información en las relaciones con suministradores.

INSTITUTO PARA LA INVESTIGACIÓN EDUCATIVA Y EL DESARROLLO PEDAGÓGICO, IDEP

Avenida Calle 26 No. 69D - 91. Oficinas 805, 806. Torre 2 - Código Postal: 110931

PBX (57-1) 263 0603 - Línea de atención al ciudadano 195 Bogotá DC - Colombia

* + 1. Política de seguridad de la información para suministradores.
    2. Tratamiento del riesgo dentro de acuerdos de suministradores.
    3. Cadena de suministro en tecnologías de la información y comunicaciones.
  1. Gestión de la prestación del servicio por suministradores.
     1. Supervisión y revisión de los servicios prestados por terceros.
     2. Gestión de cambios en los servicios prestados por terceros.

1. **GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.** 
   1. Gestión de incidentes de seguridad de la información y mejoras. 16.1.1 Responsabilidades y procedimientos.
      1. Notificación de los eventos de seguridad de la información.
      2. Notificación de puntos débiles de la seguridad.

* + 1. Valoración de eventos de seguridad de la información y toma de decisiones.
    2. Respuesta a los incidentes de seguridad.
    3. Aprendizaje de los incidentes de seguridad de la información. 16.1.7 Recopilación de evidencias.

1. **ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.** 
   1. Continuidad de la seguridad de la información.
      1. Planificación de la continuidad de la seguridad de la información.
      2. Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
   2. Redundancias.
      1. Disponibilidad de instalaciones para el procesamiento de la información.
2. **CUMPLIMIENTO.** 
   1. Cumplimiento de los requisitos legales y contractuales.
      1. Identificación de la legislación aplicable.
      2. Derechos de propiedad intelectual (DPI).
      3. Protección de los registros de la organización.
      4. Protección de datos y privacidad de la información personal.
      5. Regulación de los controles criptográficos.
   2. Revisiones de la seguridad de la información.
      1. Revisión independiente de la seguridad de la información.
      2. Cumplimiento de las políticas y normas de seguridad.
      3. Comprobación del cumplimiento.

## 5.2 Administración de accesos y Seguridad Lógica

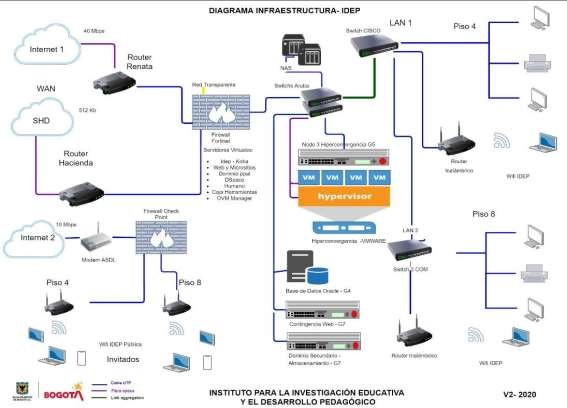
### 5.2.1 Seguridad de la red

* Ya se cuenta con un diagrama de infraestructura actualizado en el cual se puede visualizar correctamente la ubicación del Firewall, redes inalámbricas, servidores, canales de comunicación, elementos de red (switches, routers, etc.) y servicios de red.

 Es importante tener en cuenta que este diagrama es perfecto para la información pública, sin embargo, se debe tener una versión de este diagrama para la OAP en la cual se relacionen y se puedan identificar claramente los rangos de direcciones IpV4 tanto de servidores como de los segmentos de red configurados (incluyendo los de WIFI). Este diagrama se debe actualizar cuando se termine la implementación de IPv6 y debe permitir identificar las claramente las equivalencias de IPv4 a IPv6. Y que permita identificar los equipos de DHCP y DNS, conexiones VPN y elementos de contingencia.

El objetivo de este diagrama es permitir a actuales y nuevos funcionarios del área y/o a proveedores, contratistas conocer en un único documento la disposición de la infraestructura TIC de la entidad.

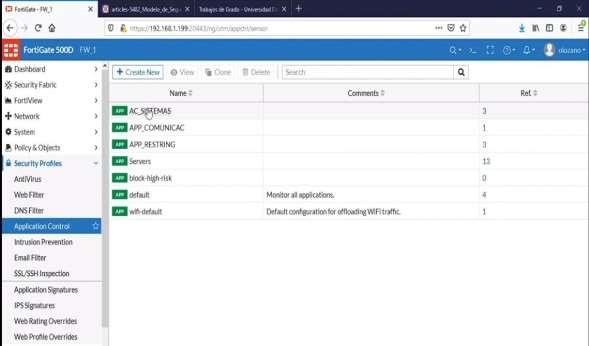
Con respecto a la implementación del protocolo IPv6 en atención a los lineamientos emitidos por MINTIC mediante Resolución 2710 del 2017, la OAP se inició el contrato 53 de 2020 con el proveedor UNIÓN TEMPORAL UT IPV6 BG 2020, en el cual se incluye correctamente la planeación de esta implementación y las acciones realizadas son adecuadas, la actividad general ya está incluida en el Plan de seguridad y Privacidad de la Información. Es importante que como parte de la ejecución de este contrato se actualice toda la documentación de la infraestructura de TI y se realice la transferencia de conocimiento necesaria para que los funcionarios y contratistas del área puedan soportar y monitorear todos los servicios, sistemas y equipos de red.



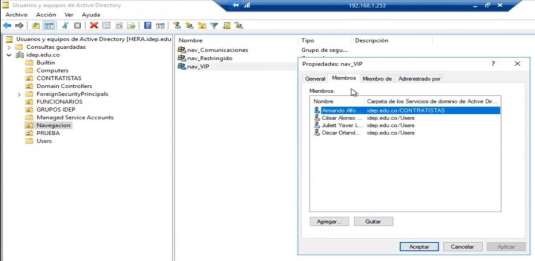
* El firewall se encuentra correctamente configurado en cuanto a las protecciones implementadas, el control de ancho de banda de internet, definición de interfaces y políticas de conexión, filtros web, control de Navegación y de aplicaciones.

* En cuanto al control de aplicaciones y navegación, se encuentran configurados 4 grupos principales: AC\_SISTEMAS, APP\_COMUNICAC, APP\_RESTING y Servers, sobre los cuales se definen las aplicaciones permitidas por el firewall a grupos de usuarios dependiendo de sus necesidades laborales. Basados en esto grupos de usuarios creados en el directorio activo para definir sus respectivos permisos, de navegación, de bloqueos y de conexión, en la siguiente imagen se evidencia la configuración del control de aplicaciones para estos grupos, los otros 3 grupos (block-high-risk, default, wifi-default)

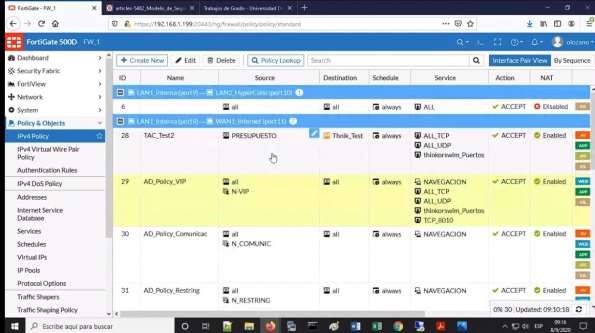
son los recomendados y viene configurados por defecto por el fabricante del firewall y su función es bloquear aplicaciones consideradas como riesgosas:



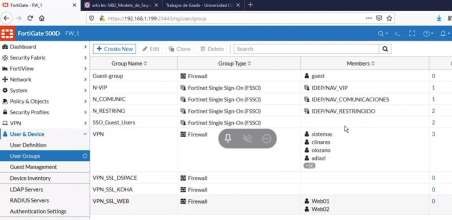
* En la siguiente imagen se evidencia la adecuada creación de tres grupos en el directorio activo para el control de navegación en internet: *nav\_Comunicaciones, nav\_Restringido y nav\_VIP*, y los integrantes del grupo *nav\_VIP*, cuyos usuarios son los del area de TI de la OAP:



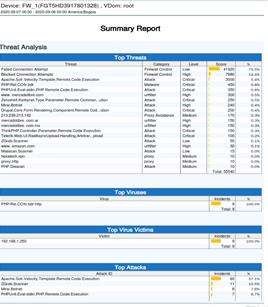
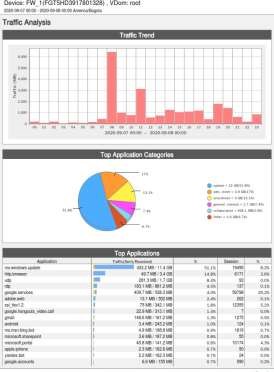
* En la imagen se muestra la correcta definición de las politicas aplicadas a los grupos de usuarios:



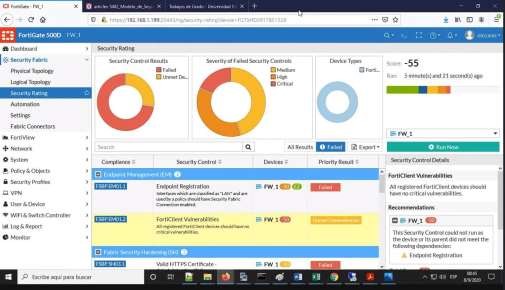
* La configuración de estos grupos de usuarios en el firewall y su relacion con los grupos del directorio activo se muestra en la siguiente imagen, en donde tambien se muestran los grupos de usuarios de VPN que se encuentran correctamente identificados en el firewall:



* En general se puede concluir que la configuración y funcionamiento del firewall es adecuada y cumple con su principal objetivo: proteger la seguridad perimetral del IDEP, es decir asegurar la red local (LAN) de ataques y posibles riesgos externos. Se denota un conocimiento adecuado de estas configuración y características del firewall de la entidad, por parte del contratista Oscar Orlando Lozano. En la revisión de informes y logs del se evidencia el correcto funcionamiento del mismo, como se aprecia en la siguiente imagen, en donde se muestra el informe resumido de la actividad del firewall entre el 7 y el 8 de septiembre verificando la detección de amenazas, bloqueos de aplicaciones y navegación entre otras:



 Si bien las configuraciones y protecciones en el firewall son las adecuadas, se debe fortalecer las acciones de corrección de alertas que indica el firewall es sus tableros de control e informes de monitoreos, ya que están son parte esencial del mantenimiento de la seguridad en la entidad, en el informe de clasificación de seguridad del firewall generado durante la auditoria, se detectan 8 controles de seguridad recomendados Con resultados fallido y tres con dependencias no cumplidas que da una puntuación de -55:



 Los controles de seguridad que deben recomendados para conformidad y que deben atenderse son los siguientes:

**Conformidad Control de seguridad Dispositivo Resultado**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | |  |
| FSBP EM01.2 | Vulnerabilidades de FortiClient: todos los dispositivos FortiClient registrados  no deben tener vulnerabilidades críticas. FW\_1 | | dependencias no cumplidas |
| FSBP SH05.2 | Seguridad de la contraseña del administrador: la política de contraseñas debe hacer cumplir las contraseñas seguras. | FW\_1 | dependencias no cumplidas |
| FSBP ND04.1 | Servidores de segmento LAN: los servidores deben colocarse detrás de  interfaces clasificadas como "DMZ". FW\_1 | | dependencias no cumplidas |
| FSBP EM01.1 | Registro de punto final: las interfaces que están clasificadas como "LAN" y son utilizadas por una política deben tener habilitada la conexión de Security Fabric. | FW\_1 | fallido |
| FSBP SH03.1 | Certificado HTTPS válido - GUI administrativa: la GUI administrativa debe  utilizar un certificado válido y seguro. FW\_1 | | fallido |
| FSBP SH05.1 | Política de contraseña de administrador: se debe configurar una política de contraseña para los administradores del sistema. | FW\_1 | fallido |
| FSBP FS03.1 | Clasificación de seguridad: la suscripción a la clasificación de seguridad debe  ser válida. FW\_1 | | fallido |
| FSBP ND03.1 | Políticas no utilizadas: se deben utilizar todas las políticas de IPv4. | FW\_1 | fallido |
| FSBP ND07.1 | Detección de dispositivos: las interfaces que se clasifican como "LAN" o    "DMZ" y son utilizadas por una política deben tener habilitada la detección  de dispositivos. FW\_1 | | fallido |
| FSBP ND09.1 | Detectar conexiones de botnet: las interfaces que están clasificadas como "WAN" y son utilizadas por una política deben usar un sensor IPS que bloquee o supervise las conexiones salientes a los sitios de botnet. | FW\_1 | fallido |
| FSBP TV01.1 | Protección avanzada contra amenazas: los archivos sospechosos deben enviarse a FortiSandbox Appliance / FortiSandbox Cloud para su inspección. FW\_1 | | fallido |

* Ya se encuentra documentado el manual de soporte de primer nivel y administración del firewall: *MN-GT-12-02 Manual soporte 1 nivel Admón. Firewall V1*, en el cual se detallan adecuadamente las principales configuraciones y funcionalidades del firewall, garantizando así la transferencia de conocimiento necesaria para el mantenimiento básico de su operación.

 Si bien en el documento *MN-GT-12-07 MANUAL PARA LA ADMINISTRACIÓN DE LA RED LAN DEL IDEP Y POLÍTICAS DE SEGURIDAD,* se hace referencia a la actividad de revisión semanal que los porcentajes del panel de control (DashBoard) del firewall no sobrepase el 80% , para los control de seguridad en el mismo debería ajustarse para que no el 40%, además se debe incluir la referencia a un formato que permita evidenciar el desarrollo de esta actividad y sus respectivas acciones de remediación.

* La estrategia para la implementación del trabajo remoto se basa en la configuración de PC’s (Redes privadas virtuales) en el firewall, para controlar el acceso remoto a los servicios de red de la entidad y para conexiones de escritorio remoto a los equipos de trabajo de los usuarios, previo análisis de las necesidades de cada uno.

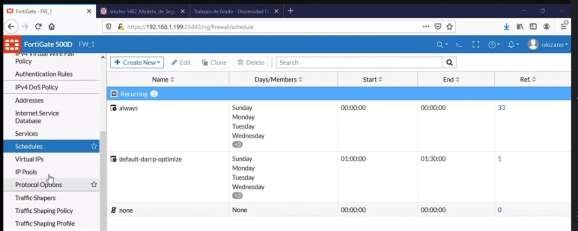
 Si bien la configuración implementada para las conexiones a través de la red privada virtual protege a la entidad de posibles ataques, intercepciones y captura de información por parte de terceros a la conexión remota, la versión del cliente de conexión de la VPN: “FortiClient”, no asegura que los equipos de cómputo desde los que se conectan los usuarios sean equipos seguros, debido a que no se obliga en la ejecución del análisis de vulnerabilidades y su respectiva corrección para poder realizar la conexión VPN. Debido a esto, no hay restricciones para que, si un equipo que tiene un virus, malware y/o alguna vulnerabilidad conocida pueda conectarse y por ende aumentar la posibilidad de generar un ataque a través de la conexión VPN ‘segura’ otorgada al equipo y/o funcionario. Las siguientes imágenes muestran como desde un equipo del auditor con vulnerabilidades criticas reconocidas (Software de Hacking) por el cliente de VPN es posible la conectarse, esta es una de las alertas que informa el DashBoard del firewall:

En el documento MN-GT-12-07 MANUAL PARA LA ADMINISTRACIÓN DE LA RED LAN

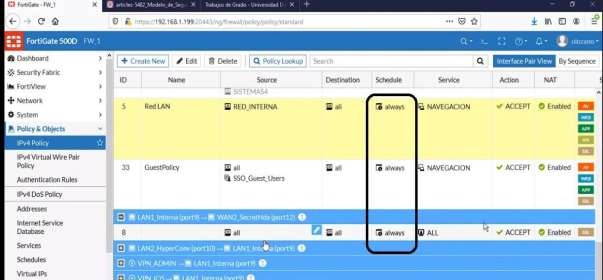


DEL IDEP Y POLÍTICAS DE SEGURIDAD, numeral 6.11.7 se define: “El horario de acceso a VPN será de lunes a viernes de 6:00 am a 6:00 pm, si requieren ingreso en horario diferente deberá dejarlo registrado en la solicitud inicial por mesa de ayuda.”, pero en el firewall no se tiene definidas estas restricciones de horario, como se puede ver en

la siguiente imagen, en la cual se muestra que el horario: *allways* está sin límite de días, ni de horas:



Y es el que aplica a todas las politicas y conexiones:



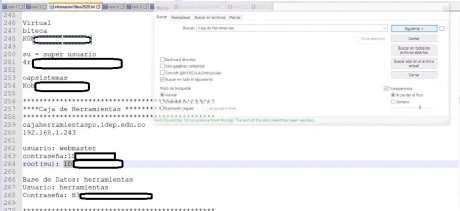
 Como medida de seguridad se debe incluir en el manual de administración de la red LAN, la revisión del mapa de localización de las conexiones VPN para identificar posibles accesos no autorizados, en la revisión realizada por el auditor se encontró un acceso por la VPN administrativa desde Barranquilla, lo cual en medio de la contingencia por COVID19 no es normal y por ende debe ser revisada y validada:



* El servidor principal de dominio cuenta como sistema operativo el Windows Server 2016 sobre el cual se encuentra configurado el directorio activo y el DNS, se cuenta con un servidor de dominio secundario con replicación y soporte del directorio activo en el servidor principal, este esquema es adecuado como contingencia a problemas en cualquiera de los dos servidores.
* La red inalámbrica WIFI de invitados se tiene correctamente aislada de la red local y está protegida por un firewall Checkpoint, cabe anotar que debido a la contingencia de Covid- 19 no fue posible realizar las pruebas necesarias para verificar esta configuración.



Se observa que aún se manejan claves de administrador para el Dominio, root y superusuarios de sistemas de información, Firewall, etc., en un archivo planos “txt” sin encriptación, lo cual es un riesgo de seguridad en caso de que uno de estos archivos sea capturado. En la siguiente imagen se ve como en una de las entrevistas se abre un archivo con información de usuarios y contraseñas de root y webmaster para los servicios de Koha y caja de herramientas en el equipo del entrevistado, las contraseñas se ocultan en la imagen para efectos de seguridad:



Si bien son archivos en equipos de usuarios de la OAP, por seguridad se debería utilizar alguna herramienta de administración de contraseñas que garantice su confidencialidad y evite posibles descubrimientos no permitidos. Este tipo de herramientas permiten la recordación de las mismas sin necesidad de ser reveladas al momento de consultarlas.



Se cuenta con el archivo en Excel: “Plan de mantenimiento y monitoreo.xls”, en el cual se registran las acciones de mantenimiento y monitoreo a la infraestructura de TI, en donde se referencian informes sobre estas acciones. Sin embargo, aún no se tiene una herramienta única de monitoreo sobre todos los servicios e infraestructura que complemente las actividades actuales de los encargados, además de facilitar un control ágil y oportuno sobre posibles incidentes y/o actuar de forma preventiva ante ellos. En las manuales documentados de administración de servidores, red LAN, dominio, firewall, etc., se hace referencia a labores de monitoreo sobre estos servicios, pero no se detallan las mismas que deberían incluirse en un procedimiento único para tener un control y seguimiento periódico de estas acciones. Existen herramientas de monitoreo gratuitas que deben ser evaluadas para implementar estos controles automatizados, como por ejemplo el **Zabbix,** que en su versión gratuita incluye todas las funcionalidades para plataformas de menos de 100 nodos.

* En cuanto al antivirus en las pruebas realizadas en el equipo asignado a la auditoría, se evidencio que la configuración y protecciones del cliente del antivirus es la adecuada y bloqueo el intento de ejecución de archivos maliciosos desde la unidad del auditor.

* Se cuenta con el MN-GT-12-01 Manual de soporte de primer nivel y administración del antivirus en el cual se detallan correctamente las configuraciones, características y gestión de administración de la consola de antivirus Kaspersky Security Center, también se incluye la revisión, instalación y actualización de los agentes, modificación y creación de directivas y tareas.

* En los informes generados durante la auditoria desde la consola del antivirus se evidencia que se cumplen con las labores de administración y seguimientos de las alertas informadas en la consola, solo se detectan 3 equipos con las bases de datos desactualizadas y 3 con problemas de conexión y de protección desactivada. Lo cual probablemente se debe al trabajo remoto por la contingencia de Covid-19.

No se encuentran configuradas en la consola del antivirus, controles y/o restricciones para el uso de medios extraíbles tales como USB, cd ´s, discos duros externos, celulares, etc., que son los medios más utilizados para la trasmisión de virus y extracción de información no autorizada. Si bien en el compromiso de cumplimiento de las políticas TIC del IDEP que firman los funcionarios y contratistas, se comprometen a: ejecutar y permitir que el antivirus complete la revisión de todos los archivos del medio extraíble”, esto no garantiza que estos medios extraíbles (USB ´s, etc.), contenga software de hacking portable y/o scripts maliciosos que no son detectados o considerados como virus, y por ende comprometan la seguridad de los PC’s de la entidad. Desde la consola de Kaspersky Security Center en la funcionalidad de control de dispositivos es posible configurar este control sobre estos y habilitar el uso solo de los dispositivos autorizados por el área de TI.



#### 5.2.1.1 Pruebas de seguridad

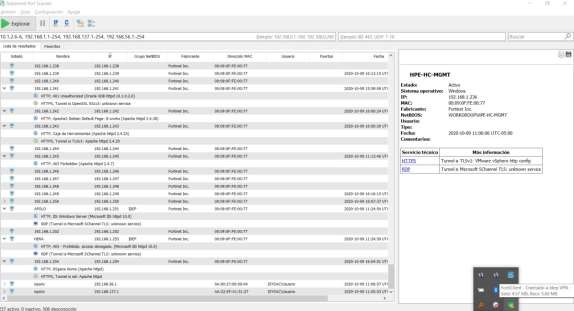
Vale aclarar que la presente auditoría no contempla ataques de penetración ni de hacking etico, las pruebas fueron ejecutadas remotamente a traves de la VPN y unicamente en el equipo asignado a la auditoria, por lo tanto los resultados son de carácter parcial y nos son concluyentes a la totalidad de la red interna de la Entidad.

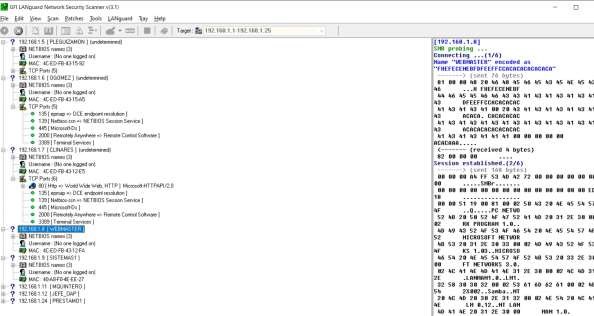
 En cuanto a la red WIFI de invitados de acuerdo al nuevo diagrama de red se puede determinar que se encuentra debidamente protegida para evitar accesos no autorizados y aislada de la red local administrativa evitando que se pueda obtener información de servidores, equipos activos de red y de PC’s. Las pruebas necesarias para garantizar la correcta configuración de lo representado en el diagrama de red solo son posibles presencialmente y que no están incluidas en el alcance de esta auditoría.

 De acuerdo a la revisión de la configuración en el firewall y al documento: MN-GT-12-02 Manual soporte de primer nivel Administración del Firewall V1, no se especifica que la asignación de direcciones Ip automática (DHCP), este habilitado únicamente a equipos con su dirección de tarjeta de red (Mac Address) registrada, para así evitar posibles conexiones no autorizadas desde puntos de red local. Esta configuración debe estar incluida en el manual de administración del Firewall para asegurar la continuidad de la misma en cualquier cambio que se realice a la configuración o plataforma.



Los equipos de usuario y servidores se encuentran en un mismo segmento de red (192.168.1.x), por lo cual se permite realizar escaneos, descubrimiento de puertos y servicios activos, y captura de paquetes internos hacia los servidores de la Entidad, que pueden ser usados para planificar ataques o interceptar información, comprometiendo así la seguridad de la infraestructura de la entidad. Cabe aclarar que esto solo puede ser realizado desde un equipo de la red local o con acceso remoto conectado a la VPN. El auditor logro realizar escaneos de red desde su equipo conectado a la VPN, obteniendo información de servidores, equipos y puertos disponibles en la infraestructura de red, como se muestra en las siguientes imágenes:



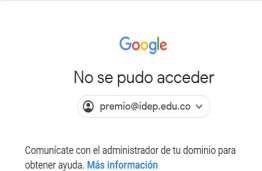


### 5.2.2 Seguridad servicios de correo

* En el documento MN-GT-12-04 Manual para la administración de usuarios que se vinculan a los sistemas de información o servicios tecnológicos del Idep v1, se detalla correctamente el proceso de creación y eliminación de cuentas de correos electrónicos de usuarios desde la consola de administración de G Suite y la trasferencia de datos de las cuentas. Se tiene configurado la longitud mínima de 8 caracteres en la contraseña de los correos.

Si bien el servicio de correo electrónico es el principal medio de comunicación entre los funcionarios, contratistas y proveedores del Idep, no se cuenta con un manual que detalle la administración y gestión de estas cuentas, en cuanto a parámetros y políticas de seguridad y protecciones desde la consola administrativa de Google, tampoco se hace referencia a este servicio en el plan de contingencia, por lo cual se puede afirmar que no se tiene contempladas acciones de contingencia en caso de fallo o ausencia de este servicio.

* En las pruebas realizadas por el auditor se comprobó que todas las contraseñas de cuentas capturadas en la auditoría anterior ya se modificaron, y no se están utilizando contraseñas que puedan ser fácilmente capturadas.
* Se encuentran correctamente configurados las opciones de recuperación de contraseña, con validación de ultima contraseña recordada, teléfono de recuperación y/o correo electrónico alterno para recuperar las contraseñas. En las siguientes imágenes se evidencia que un intento de captura de contraseña por medio de recuperación, se bloqueó correctamente:



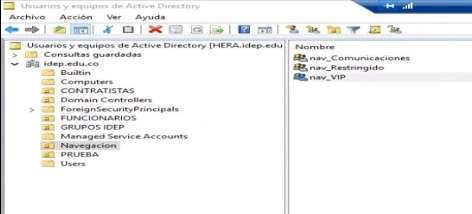
 Las cuentas y contraseñas de correo electrónico no se encuentran sincronizadas con las cuentas del directorio activo del Idep, lo cual dificulta su administración y no permite que se apliquen todas las apliquen automáticamente todas las políticas de seguridad configuradas para las cuentas de usuarios en el dominio. De acuerdo a las mejores prácticas para facilitar la gestión de cuentas de correos electrónicos se recomienda esta sincronización para facilitar y disminuir el uso de varias contraseñas a los usuarios y para unificar la generación de controles de seguridad. Existen herramientas gratuitas de Google aplicables a G Suite que permiten esta sincronización y que deberían evaluarse para simplificar el proceso, la seguridad y administración de las cuentas de usuario.

* Ya se encuentra configurado correctamente el cambio periódico de contraseña cada 90 días, para las cuentas de correo electrónico y la no reutilización de las mismas, como se muestra en la siguiente imagen tomada de la consola de administración de G Suite:



### 5.2.3 Seguridad de Internet y PC ´s

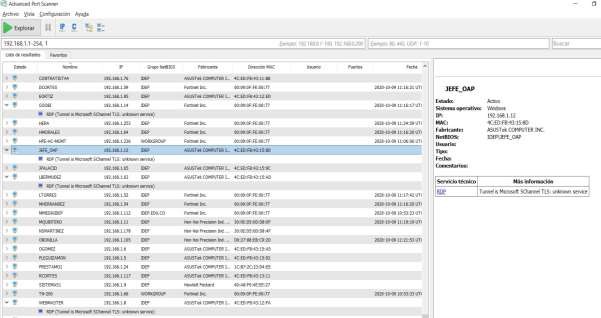
* Se encuentran correctamente configuradas las restricciones de navegacion en el firewall que ademas se encuentran correctamente sincronizadas con la unidad organizativa: *”Navegacion”* en el directorio activo para la adecuada y simplificada gestion de usuarios en las tres grupos de navegación: “nav\_Comunicaciones”, “nav\_restringido” y “nav\_VIP”, como se aprecia en la siguiente imagen:



* Las pruebas realizadas sobre el equipo asiganado a la auditoria con el usuarios creada para las mismas: “lyvelosa”, permiten evidenciar que estas restricciones funcionan correctamente en cuanto a la navegación en sitios peligrosos y que se estan bloqueando correctamente las descargas de software malisioso o considerado como virus.

 A pesar de las restricciones para descargas de sitios prohibidos y de software potencialmente peligroso, aun es posible descargar versiones portables de software de descubrimientos desde unidades de almacenamiento en la nube, debido a esto el auditor logra ejecutar el software de escaneo: “advanced port scanner”, para asi tener la información de equipos, y servicios de la entidad. Como se ve en la siguiente imagen:

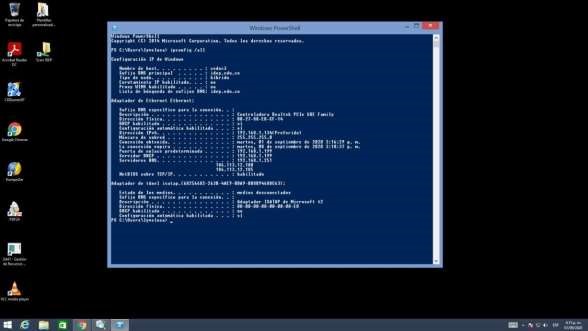
En el equipo de pruebas asignado al auditor se observa que continúan debidamente configurados el control de cuentas de usuario, la restricción a recursos compartidos.



* Se configuraron en las políticas de dominio las restricciones de acceso en los equipos de usuarios al panel de control, centro de redes y recursos compartidos, restricción de adición y búsqueda de impresoras, protector de pantalla, bloqueo de ejecución de comandos “*cmd*”, entre otros recomendados en el informe de auditoría anterior. El correcto funcionamiento de estas políticas se evidencio en las pruebas realizadas en el equipo asignado a la auditora. En la siguiente imagen se muestra la evidencia de la configuración de estos parámetros:



 Se debe adicionar a las políticas de dominio del punto anterior, la restricción de ejecución de comandos desde el PowerShell de los equipos de usuario y el acceso al registro de Windows (Regedit), ya que estos accesos permiten ejecutar *scripts* de descubrimiento o ingresar comandos para activar software espía o malicioso. En la imagen se evidencia la ejecución de comandos del PowerShell para identificar los parámetros de red del equipo asignado a la auditoria:



Como se menciona en la revisión del antivirus aún no se encuentran bloqueados y configurados los permisos de conexión de dispositivos de almacenamiento externo (USB, discos duros externos, CD, etc.), que además de ser origen de trasmisión de virus permiten ejecutar programas para cambio de contraseñas de administradores de equipos locales para evadir los controles de seguridad del firewall y antivirus.

### 5.2.4 Seguridad de Archivos Fuentes y Documentos

* El esquema utilizado para el alojamiento y respaldo de los documentos de usuario final es el uso de carpetas compartidas en la unidad TRD es el adecuado, se generó y publico el instructivo: IN-GT-12-02 INSTRUCTIVO PARA EL ALMACENAMIENTO DE LA

INFORMACIÓN EN CARPETAS COMPARTIDAS, en el cual se detallan claramente todas las condiciones y reglas para el correcto almacenamiento y clasificación de la información que generan los usuarios de acuerdo a la tabla de retención documental definida para la entidad.

* El auditor pudo evidenciar que los recursos compartidos de la red del IDEP continúan debidamente protegidos por contraseña.

 No se han adoptado métodos, ni instructivos de protección de archivos, documentos o unidades de almacenamiento mediante el uso de protección de contraseñas o encriptación de medios o archivos que permitan garantizar la confidencialidad de la información así clasificada en caso de pérdida de unidades de almacenamiento o equipos portátiles.

### 5.2.5 Gestión de accesos

* Se encuentra correctamente publicados y socializados los instructivos para la gestión de cuentas de acceso, administración y cambios de contraseña para los sistemas GOOBI y

Humano en los manuales: MN-GT-12-12 Manual soporte 1 nivel GOOBI V1, MN-GT-12- 09 Manual de administración soporte HUMANO V1 y los instructivos: IN-GT-12-06 - instructivo para cambio de contraseña sistema Humano y IN-GT-12-05 Instructivo Para Cambio De Contraseña De Ingreso al Sistema de Información GOOBI. En donde se describe detalladamente los procedimientos para la gestión de usuarios y el cambio de contraseña.

* También se describen correctamente en los documentos mencionados las funcionalidades para la asignación de usuarios por perfiles, con el fin de segregar los privilegios sobre los sistemas de información y la gestión de los mismos.

* Se implemento de forma adecuada el formato de Compromiso de cumplimiento de las políticas TIC del Idep, en el cual los usuarios se comprometen al buen uso y manejo de sus cuentas de usuario y el adecuado control de sus contraseñas.
* Ya se encuentran implementadas las políticas de cambio periódico de contraseña para el correo electrónico, cuentas de dominio, e instructivos en el sistema Humano y Goobi.
* Si bien aun en algunos correos de creación de cuentas de usuarios se siguen exponiendo contraseñas, en las pruebas realizadas se evidencia que se realiza el cambio de contraseña asignada ya que el auditor no logro acceder con la contraseña expuesta en el correo, como se ve en la siguiente imagen:



 Para los servicios de página web y micrositios, si bien permiten adecuadamente el cambio de contraseña y perfilamiento de usuarios, se está esperando la actualización de Govimentum, para implementación del cambio periódico obligatorio de contraseñas.



* Las directivas de contraseña en el dominio se encuentran bien configuradas en cuanto a la complejidad y longitud.



La vigencia máxima de la contraseña se aumentó a 210, (90 días en la auditoria anterior), lo cual es un tiempo excesivo ya que el tiempo promedio de ataques de fuerza bruta a contraseñas de Windows es de 90 días. Y aún no se ha configurado el umbral de bloqueo de cuentas por intentos fallidos como se aprecia en la siguiente imagen tomada del informe de políticas de seguridad del dominio:



# 5.2.6 Seguimiento a Recomendaciones 2019

|  |  |  |  |
| --- | --- | --- | --- |
| **N** | **OBSERVACIÓN** |  | **SEGUIMIENTO** |
| 1. | Dados los resultados de las pruebas de seguridad adelantadas por el auditor, se recomienda fortalecer y replantear el *PL-GT- 12- 04 Plan Seguridad y Privacidad de la\_Info\_V1,* como un proyecto de implementación del MSPI atendiendo los controles establecidos por la norma ISO 27001:2013 que realmente garanticen el aseguramiento de la plataforma y no únicamente un cumplimiento documental parcial. Un sistema de gestión de seguridad de la información correctamente implementado es aquel que incluye los controles tecnológicos que aseguren la plataforma TIC y la información de la entidad. Se recomienda si es posible contratar consultoría especializada. |  | Si bien se presentado avance en la implementación de controles de seguridad y en el aseguramiento de la plataforma, aun no se ha implementado totalmente los controles requeridos para tener un sistema de gestión de seguridad de la información completo. |

|  |  |  |  |
| --- | --- | --- | --- |
| **N** | **OBSERVACIÓN** |  | **SEGUIMIENTO** |
| 2. | Incluir en el *PL-GT-12-04* la adopción IPV6 incluyendo el diagnostico que permita identificar el alcance y acciones para una correcta implementación. |  | Ya se encuentra contratado y en  implementación la adopción de IPV6, en la revisión de la documentación entregada se evidencia su correcto planteamiento. |
| 3. | Ajustar el diagrama de infraestructura de acuerdo con las observaciones emitidas en el presente informe. |  | Ya se realizaron las modificaciones al diagrama, sin embargo, no se incluyeron las identificaciones de direcciones IP ni se identifica el DHCP, se recomienda hacer un diagrama  alterno de uso del área con estas modificaciones, |
| 4. | Atender las debilidades en la configuración del Firewall con las siguientes acciones: activar las detecciones de seguridad para intrusos, virus, cambios de configuración de correo y exceso de cuota de disco. |  | Los controles implementados en el firewall son los adecuados. |
| 5. | Para mejorar el nivel de monitoreo y seguridad, se recomienda separar el grupo de servidores a un segmento de la LAN diferente al de los equipos de usuario y configurarlo para que el Firewall pueda monitorear la interacción de los usuarios con los servidores. |  | Aun no se ha realizado esta labor, en los escaneos realizados por el auditor se evidencia que los servidores continúan en el mismo segmento que los equipos de usuarios. |
| 6. | Configurar el sistema de protección de intrusos habilitando los filtros basados en firmas que permiten bloquear ataques de denegación de servicios y/o de fuerza bruta |  | Ya se encuentran configurados y en funcionamiento los principales filtros basados en firmas en el firewall. |
| 7. | Como parte de la implementación del MSPI Dominio 12 Gestión de Operaciones, adelantar y poner en funcionamiento un procedimiento de registro, monitoreo y medición de capacidad y desempeño, que incluya las siguientes acciones y sus responsables:  -Identificar los recursos tecnológicos y los sistemas operacionales que generarán logs de eventos de acuerdo con el nivel de criticidad establecido en el inventario de activos (incluyendo el firewall, antivirus, SO Red, sistemas de información, procesos de Backup, etc.)  -Establecer las pautas requeridas para habilitar el registro de eventos, excepciones y fallas, utilizando logs y/o sistemas de registro. -Realizar un monitoreo periódico de los logs y/o sistemas de registro que sean generados en la operación diaria de los activos de información, para identificar vulnerabilidades técnicas emergentes  -Prevenir la modificación y eliminación de los logs y/o datos administrados en sistemas de |  | Si bien se está utilizando y gestionando las herramientas de monitoreo del firewall y antivirus y se registran acciones de monitoreo en una hoja de Excel, aún no existe un procedimiento, ni herramienta única de monitoreo que permita la medición de capacidad y desempeño de la infraestructura de TI y que incluya las acciones mencionada en la recomendación.    Todavía no se tiene control sobre los logs de todos los sistemas. |

|  |  |  |  |
| --- | --- | --- | --- |
| **N** | **OBSERVACIÓN** |  | **SEGUIMIENTO** |
|  | registro por parte de usuarios con credenciales de acceso, incluyendo aquellos que tengan “acceso privilegiado”  -Establecer y ejecutar tareas automáticas de respaldo de logs mediante su programación en el plan de copias respaldo  -Definir un repositorio exclusivo donde se centralicen todos los logs generados a los cuales debe aplicarse mecanismos de encriptación durante la centralización, esto con el propósito de adelantar labores de monitoreo y análisis de eventos  -Finalmente tomar control sobre los logs de auditoría generados por los sistemas de información Humano y Goobi. |  |  |
| 8. | Como parte de la implementación del MSPI dominio 10. Cifrado, hacer el levantamiento de los activos de información en custodia o transito que requieren de algoritmos de encriptación. Atender como mínimo:   * Aplicar un algoritmo de encriptación para el archivo que contiene las claves de administrador y establecer una política de cambio mensual y en caso del retiro de algún funcionario o contratista conocedor de las claves. Este elemento también hace parte del MSPI dominio 9 Gestión de accesos- accesos privilegiados * Archivos de alta confidencialidad almacenados en Drive o carpetas compartidas o en tránsito como adjuntos de correo electrónicos. * Dispositivos móviles o de almacenamiento externo que puedan tener información confidencial. |  | Ya se adelantó el levantamiento de activos de información con su respectiva clasificación de confidencialidad y se adecuo en el plan de adopción IPV6. Pero aún no se han seleccionado algoritmos o herramientas de encriptación que permitan completar esta recomendación. |
| 9. | Hacer extensivas las configuraciones de los equipos Windows a los equipos Mac en todo lo referente a políticas de seguridad de dominio, firewall y antivirus. |  | Queda pendiente de su verificación, debido a la contingencia de Covid-19, no se pudieron realizar pruebas presenciales en los equipos Mac. |
| 10. | Configurar las reglas de red de aplicación máximas del antivirus para aplicaciones de alta peligrosidad como sniffers, man in the middle, etc. Revisar las reglas de restricción mínima contra los listados de software permitido. |  | En las pruebas realizadas y en la revisión de las políticas del firewall y antivirus se evidencio el bloqueo de este tipo de software. |
| 11. | Como parte de la implementación del MSPI dominio 8 Gestión de Activos, fortalecer el inventario de activos de información del instituto ya que el inventario actual se limita a Hardware y Software base y no incluye otros activos de información críticos tales como: |  | Ya se actualizo FT-GT-12-19 inventario activos de información tipo software, hardware y servicios Idep, en el cual se incluyen la clasificación y características mencionadas en la recomendación, sin embargo, se debe complementar con todo el software autorizado e |

|  |  |  |  |
| --- | --- | --- | --- |
| **N** | **OBSERVACIÓN** |  | **SEGUIMIENTO** |
|  | bases de datos, documentos confidenciales, ficheros, aplicaciones, herramientas de desarrollo, publicación de contenidos, entre otros.  Cada uno de los activos mencionados debe tener un responsable y calificación de criticidad de la información con base en su: Disponibilidad (importancia que tiene la ausencia del activo), Integridad (qué repercusiones tendría la modificación de este activo sin autorización) y confidencialidad. Vale aclarar que el inventario de activos de acuerdo con los lineamientos MSPI en concordancia con ISO 27001:2013 debe incluir todo aquel software autorizado para ser usado en la empresa  independientemente de que sea software libre. |  | instalado en los equipos de la entidad. En los reportes de aplicaciones instaladas generado durante la auditoria desde la consola del antivirus se evidencia la presencia de software no incluido en este formato. |
| 12. | Configurar correctamente las VLAN´s para evitar que se realicen escaneos a direcciones IP diferentes a la del segmento en la que se encuentra configurado cada equipo, incluyendo el segmento de la WIFI de invitados. |  | Aun se pueden hacer escaneos sobre los servidores como se muestra en las imágenes de escaneos registradas en este informe. En cuanto a la WIFI publica de acuerdo al esquema de red se muestra correctamente aislada. |
| 13. | Configurar la red y el DHCP para restringir la conexión al dominio solo a equipos cuya Mac Address este registrada en la lista autorizada |  | En la configuración del DHCP en el firewall no se evidencia la restricción a Mac Address autorizadas de equipos de usuario. |
| 14. | Configurar las restricciones de seguridad de G Suite en cuanto a:   * Cambio periódico de contraseñas * No repetición de las ultimas 8 contraseñas * Alertas de ingreso en equipos distintos a los usuales a un correo alternativo * Configurar correctamente la autenticación de doble factor (pre-registro) |  | Ya se encuentran implementadas las restricciones recomendadas. |
| 15. | Fortalecer la configuración de las políticas de firewall y las políticas de dominio para impedir descargas de archivos ejecutables. La restricción debe ser general independientemente del cargo del usuario. Todo archivo ejecutable que se requiera debe ser autorizado por la OAP. |  | En el equipo y con el usuario asignado a la auditoria se evidencia en funcionamiento de las políticas recomendadas. No se realizaron pruebas a otros equipos y/o usuarios debido a la imposibilidad de realizar visitas presenciales. |
| 16. | Instalar una herramienta gratuita que escanee periódicamente los recursos compartidos en la red e identifique cuales se encuentran sin protección y configurar las debidas restricciones de acceso (ejemplo:  esencial nettools, NetShareWatcher, etc.) |  | No se evidencio el uso de este tipo de herramientas como parte de las revisiones de seguridad del área. |
| 17. | Restringir en todos los equipos de escritorio y portátiles el acceso al panel de control y en especial al centro de redes. |  | En la pruebas y revisión de las políticas de dominio se comprobó el funcionamiento de esta recomendación. |

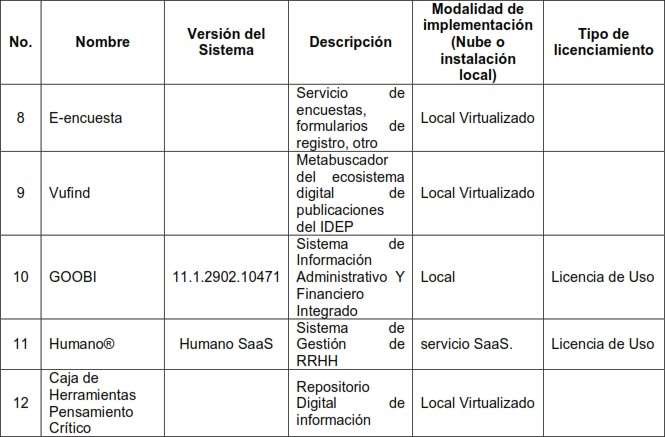
|  |  |  |  |
| --- | --- | --- | --- |
| **N** | **OBSERVACIÓN** |  | **SEGUIMIENTO** |
| 18. | Por ningún motivo exponer información de claves de acceso en el sistema de help desk o en correos sin la verificación inmediata del cambio de credenciales. |  | Si bien aún se expone algunas contraseñas en correos, se está validando y obligando el cambio de contraseña en los sistemas de información que lo permiten, cumpliendo con el objetivo de esta recomendación |
| 19. | Revisar los niveles de acceso a la navegación en internet con el fin de garantizar que todos los usuarios tengan privilegios acordes con las funciones de su cargo. No es recomendable que en las oficinas se ingrese a correos personales, redes sociales, etc. a menos de que sean necesarios para la ejecución de sus funciones |  | Se restructuraron los permisos en tres grupos de navegación, en el grupo de comunicaciones y VIP se permiten el uso de algunas redes sociales y de streaming, necesarias para labores de las áreas.  En cuanto al uso de correos personales no se pudo realizar la verificación debido a la imposibilidad de revisar equipos diferentes al asignado a la auditoria. |
| 20. | Establecer un plan para tomar control de la administración, configuración y control de cambios del sistema Goobi.  Replantear la autorización de conectividad por VPN restringiendo el horario de conexión, asegurando el monitoreo durante la conexión y solicitar autorización antes de la conexión. Establecer un protocolo de cambios para que el IDEP ejecute los despliegues en producción con base en una entrega de  objetos de despliegue, minutograma y procesos de rollback. |  | Aun no se muestra avance en esta recomendación |
| 21. | Configurar todas las directivas de seguridad del dominio de acuerdo con las recomendaciones de Microsoft para entornos corporativos y las recomendaciones emitidas por el auditor.  Implementar medidas automáticas o  manuales para aplicar complejidad de contraseñas en el acceso a servicios TIC y para su cambio periódico y no reutilización |  | Si bien se realizaron reconfiguraciones en las políticas del dominio y se activaron medidas automáticas y/o manuales para el control de contraseñas. La vigencia de las contraseñas del dominio se aumentó a 210 días, lo cual no cumple con las buenas prácticas en directivas de contraseña. |
| 22. | Diseñar y formalizar un acta de entrega de activos TIC que incluya como mínimo: Equipos, Periféricos especiales, Software instalado, Accesos concedidos y privilegios, Controles de verificación de cambio de credenciales y accesos exitosos y Entrega de políticas de seguridad |  | Si bien se implementó el acta de compromiso con el buen uso de activos tic y cumplimiento de la políticas tic, no se cuenta con un acta que incluya todos los puntos recomendados. |

## 5.3 Desarrollo y Adquisición de Software Aplicativo

* El PETI 2020 incluye correctamente el listado de sistemas de información en su numeral

5.4, solo está pendiente la inclusión de RENATA.





 En cuanto al desarrollo del catálogo de sistemas de información, se ha realizado el registro en el Inventario de activos *Base de Datos de Activos de Información Hardware - Software - Servicios.xlsx*, pero no se han atendido los lineamientos de la Guía G.SIS.03 Guía para la construcción del catálogo de Sistemas de Información, que arroje como resultado un catálogo caracterizado con los siguientes atributos:

* + Nombre del sistema - Sigla o Descripción del sistema
  + Versión o Categoría o Tipo de desarrollo o Fabricante
  + Proveedor de soporte y/o implementación o Enlace a contratos y Fecha de vencimiento del soporte o Responsable técnico o Responsable funcional o Estado: en implementación, en mantenimiento, fuera de productivo. o Soporte de Licenciamiento y cumplimiento con derechos de autor o Sistema Operativo o Lenguaje de programación o Plataforma de Base de datos

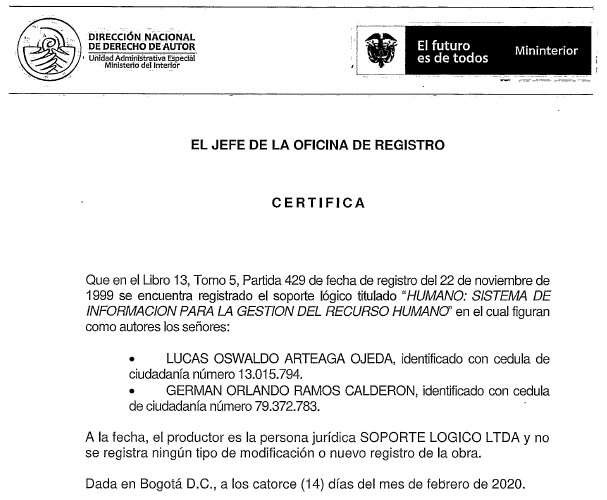
* + Documentación técnica y funcional para trasferencia de conocimiento. o Arquitectura tecnológica

En cuanto a la legalización de uso del sistema GOOBI, fueron presentados por el proceso las siguientes evidencias de legalización de su uso:

* GOOBI S.A.S - Certificado de Derechos de autor: trasferencia de derechos patrimoniales a GOOBI SAS
* GOOBI S.A.S - Certificado de exclusividad y único proponente.pdf: que establece el derecho de GOOBI SAS a distribuir el sistema como nuevo propietario de los derechos.

 Contrato 2016-0034 Licenciamiento Goobi.pdf: el cual data del 2016 y debe ser actualizado con la firma de GOOBI SAS

 En el caso del sistema Humano no fueron entregados al auditor las evidencias de las licencias de uso expedidas por el propietario, pero si el registro de derechos de autor del producto que en el caso de Soporte Lógico se encontraba correcto.



 En cuanto a la confiabilidad en los sistemas de información, la percepción es positiva en todos los sistemas a excepción de GOOBI, en el cual se han presentado inconvenientes de integridad de datos que generan desconfianza e incrementan el interés del IDEP por adquirir una nueva solución tecnológica. El auditor pudo observar la siguiente situación:

o La falla corresponde a inconsistencias en los consolidados y boletín de inventarios, presuntamente basados en errores de datos y clasificación durante la migración de datos para transición a las NIIF, que han venido evidenciándose desde el año 2018 en cada proceso de generación del boletín. Sobre este particular cabe anotar que las condiciones de soporte del contrato 26 de 2020 no da cobertura a fallas de datos que no están directamente relacionadas con la operación del sistema, por lo cual no es viable una reclamación de incumplimiento al proveedor.

* Si bien estas inconsistencias no reflejan impacto en contabilidad, el proveedor de GOOOBI manifestó en su informe de auditoría del mes de septiembre de 2020, que se han realizado notas contables con el propósito de ajustar los saldos, lo cual en caso de ser evidenciado por el proveedor implica que deben revisarse dichas notas contables, ya que no corresponden a la corrección de fondo de la problemática y podrían empeorar la situación al “ajustar” la causa raíz en lugar de resolverla.

* Si bien el área usuaria presenta un inventario de inconsistencias, este no puedo considerarse el universo completo de casos, ya que al no resolverse la causa raíz, no se puede suponer que no aparecerán nuevos casos a lo largo del tiempo.

* Se observa que, tras la aparición de cada caso, el área usuaria se comunica directamente con el proveedor sin mediar al proceso de gestión TIC, lo cual ocasiona que se ajusten casos individuales, sin un análisis que permita establecer una solución de fondo.

* Se observa que, si bien el sistema cuenta, con funcionalidades de ajuste de clasificación, el proveedor ha intervenido en hacer ajustes a nivel de bases de datos, lo cual puede poner en riesgo la integridad de los datos.

* A la fecha, no se ha realizado un plan de depuración de la data basado en un diagnóstico de casuística para el diseño de estrategia de corrección en tres frentes:

* + Construcción de scripts de diagnostico masivo sobre la base de datos que permitan clasificar cada caso donde los datos rompen la regla de negocio y/o condiciones de integridad referencial.

* + Construcción de scripts de actualización masiva (updates) que permitan ajustar casos, tal como reclasificar datos mal categorizados.

* + Identificación de los casos que requieren ajuste manual y la asignación de recursos para esta labor.

 En cuanto a la gestión del conocimiento para la supervisión y administrador de los sistemas de información, se observa una mejora con respecto al año 2019, ya que la contratista a cargo de los sistemas GOOBI y Humano ha gestionado capacitaciones de los proveedores que mejoren el conocimiento y apropiación de la funcionalidad, igualmente se han adelantado los manuales *MN-GT-12-09 Manual admón. soporte HUMANO V1.pdf* y *MNGT-12-12 Manual soporte 1 nivel GOOBI V1.pdf*. Sin embargo, aún es preciso fortalecer el conocimiento técnico de las soluciones, que permitan autonomía al IDEP en un proceso de migración de datos, frente al riesgo de que, al realizar el cambio del ERP, no se obtenga apoyo del proveedor de GOOBI para este proceso.

 Para efectos de soporte y mantenimiento con el proveedor de Humano, este servicio ha sido mejorado gracias a la modalidad SAAS a la cual fue migrada la solución. En este esquema se disminuye el riesgo de fallas en actualizaciones. Sin embargo, pese a que el módulo de Planta de personal incluye el “*Registro de los datos de cada empleado: la historial laboral y datos personales, competencias, capacidades, remuneraciones y Labores en la empresa*”, el contrato no es explicito en cuanto a la obligación del proveedor de garantizar la protección de estos datos del acceso indebido y las condiciones de seguridad de los ambientes de alojamiento tanto de los datos transaccionales como de los backups. (las obligaciones 20 y 21 no son explicitas)

 Por otra parte, el servicio de soporte y mantenimiento de GOOBI continúa presentando inconvenientes, tal es el caso del incidente de indisponibilidad total Caso #11- CPS31-2020) reportado el 16 de abril a las 1:56 pm, y originado por el incumplimiento del proveedor en una actualización programada para el 15 de abril y errores en el proceso, que originaron no solo la caída del sistema sino fallas de operación una vez recuperado el servicio. La situación fue resuelta el 17 de abril a las 9:37 am, lo cual significa que tomo 20 horas para la resolución, incumpliendo el ANS establecido en el contrato. Vale aclarar que el proveedor continúa teniendo acceso a los ambientes productivos y haciendo despliegues de manera autónoma, sin que medie un RFC y procesos de rollback. Dado que los incidentes no se gestionan en la mesa de servicio, las fechas entre el reporte del incidente (16 de abril) y el registro en la bitácora *Incidentes Contrato #31-2020 - GOOBI (3).xlsx* (17 de abril), no coinciden, lo cual dificulta llevar el control de ANS.

 Aunque no se cuenta todavía con una metodología documentada y formalizada de gerencia de proyectos de desarrollo interno o de implementación de software adquirido, debidamente articulada con el MRAE y con el MSPI (Dominio 14), se evidencian avances importantes en la estructuración de instrumentos, los cuales se relacionan a continuación.

|  |  |
| --- | --- |
| **INSTRUMENTO** | **OBSERVACIONES AUDTORIA** |
| CONTEXTO -  MANTENIMIENTO DEL  SISTEMA DE  INFORMACION.pdf | El documento ofrece un esquema general, pero es preciso ajustarlo a los tres frentes de Desarrollo y Adquisición de sistemas de información:   1. Adquisición de software comercial 2. Desarrollo de software por encargo a terceros propietarios 3. Desarrollos propios (ya sea in house o por encargo a   contratistas) |
| FT-GT-12-22 Levantamiento Necesidades SI V2 | Si bien tiene información completa de la necesidad, resulta dispendioso llevarlo en registros de Excel.  Se recomienda gestionarlo por la mesa de servicio como un requerimiento de mantenimiento o desarrollo de software. En este caso los ANS corresponde al tiempo para levantar la especificación. |
| FT-GT-XX-XX Especificación  Requerimientos SI.xlsx  FT-GT-XX-XX Requerimientos del Sistema de Información.xlsx | Si bien incluyen información relevante, se observa que hay datos repetidos en los dos formatos y criterios de aceptación que pueden ser llevados a un componente de pruebas de aceptación.  Se recomienda segmentarlos en tres formatos:   1. Especificación funcional y no funcional con mockups que permitan el total entendimiento del usuario quien debe firmarlo como condición para paso a diseño y desarrollo. Se recomienda manejarlo en Word para facilitar la trazabilidad de comentarios y ajustes entre analista, usuario y proveedor (cuando aplique). 2. Especificación técnica: que podría ser una versión extendida de la historia de usuario 3. Formato de pruebas de aceptación tanto funcionales como no funcionales. |
| PRO - GT - MANTENIMIENTO AL CICLO DE VIDA DE LOS  SISTEMAS DE INFORMACION  V1.xlsx | Debe ser ajustado al dominio 14 del MSPI, y actualizado en los registros una vez definidos y unificados.  Deben ser incluidos formatos de cambios RFC para los despliegues.  Deben ser incluidos los formatos de entrega de conocimiento. |

**5.3.1 Seguimiento a Recomendaciones 2019**

|  |  |  |  |
| --- | --- | --- | --- |
| **N°.** | **Recomendación 2019** |  | **Seguimiento 2020** |
| 1. | Como parte de la metodología de gestión de programas y proyectos TIC en atención al dominio de Gobierno Digital, elaborar, formalizar y poner en operación un procedimiento de control de cambios que permita llevar trazabilidad y control sobre los cambios impactados por los proveedores. Incluir formatos de documentación de cambios y medias de seguridad para mitigar las fallas en uso productivo por cambios no gestionados. |  | A la fecha no se ha adelantado el procedimiento de Gestión de cambios para dar cumplimiento a los lineamientos MSPI (12.1.2 Gestión de cambios, 14.2.2 Procedimientos de control de cambios en los sistemas, 14.2.3 Revisión    técnica de las aplicaciones tras efectuar cambios en la plataforma operativa y  14.2.4 Restricciones a los cambios en los paquetes de software)  Sn embargo, se reconoce que se adelantan |

|  |  |  |  |
| --- | --- | --- | --- |
| **N°.** | **Recomendación 2019** |  | **Seguimiento 2020** |
|  |  |  | actas para evidenciar los resultados de cambios en la infraestructura, las cuales si bien no corresponden al lineamiento MSPI si aportan memoria y formalidad sobre los impactos.    Tal es el caso de:     * Migración de humano      * Implementación IPV6      * Implementación Renata |
| 2. | Solicitar a los proveedores de los sistemas Humano y Goobi las licencias de uso a favor del IDEP y para el caso de IT GOP SAS solicitar el registro de derechos de autor actualizado. |  | El proceso de gestión TIC ha gestionado la actualización del registro de derechos de autor y de registro de distribución de GOOBI SAS.  Está pendiente la actualización de licencias de GOOBI y de Humano, las cuales no fueron presentadas a la auditoría. |

**5.3.2 Nuevas Recomendaciones 2020**

|  |  |
| --- | --- |
| **N°.** | **Recomendación 2020** |
| 1. | Adelantar el catálogo de sistemas de información, orientándose con la Guía G.SIS.03 Guía para la construcción del catálogo de Sistemas de Información. Versión 2019 de MINTIC. |
| 2. | Con respecto a la problemática del boletín de inventarios se recomienda adelantar las siguientes acciones:     1. Solicitar al proveedor de GOOBI evidencias de las presuntas notas contables con las que se ajustan saldos, y de ser cierto tomar medidas correctivas. 2. Adelantar un plan de depuración de la data basado en un diagnóstico de casuística para el diseño de estrategia de corrección en tres frentes:    1. Construcción de scripts de diagnóstico masivo sobre la base de datos que permitan clasificar cada caso donde los datos rompen la regla de negocio y/o condiciones de integridad referencial.    2. Construcción de scripts de actualización masiva (updates) que permitan ajustar casos, tal como reclasificar datos mal categorizados.    3. Identificación de los casos que requieren ajuste manual y la asignación de recursos para esta labor    4. Establecer un plan de depuración manual de casos.   Centralizar todos los incidentes por el proceso de Gestión TIC y una vez ejecutado del plan de depuración de datos, impedir el acceso del proveedor a los datos de producción. |
| 3. | La solución de depuración de datos se recomienda mientras permanece en operación el sistema  GOBBI, pero se reitera la recomendación de su remplazo por otro ERP preferiblemente en modalidad  SAAS.  Aprovechar los documentos del proceso adelantados por la contratista a cago de su supervisión, |

|  |  |
| --- | --- |
| **N°.** | **Recomendación 2020** |
| 4. | Fortalecer el conocimiento del IDEP en el modelo de datos de GOOBI, como contingencia en caso de que el proveedor actual no apoye el proceso de migración a un nuevo ERP. |
| 5. | Incluir en la renovación del contrato SAAS de Humano y en cualquier otra adquisición de sistema de información en modalidad SAAS clausulas específicas sobre la protección y propiedad de los datos alojados. Ver PROTECCIÓN EN LOS SERVICIOS COMPUTACIÓN EN LA NUBE (CLOUD COMPUTING) de la SIC. |
| 6. | Continuar con el proceso de construcción de una metodología de Desarrollo y Adquisición de software aplicativo, pero atendiendo las observaciones de la auditoría y en especial garantizando su articulación con el Dominio de sistemas de Información el Marco de Referencia de Arquitectura Empresarial y el Dominio 14 del MSPI ISO 27002:2013. |

## 5.4 Administración de Recursos de TI

### 5.4.1 Inventarios de activos y Mantenimiento de Hardware y Software

 Se adelanto la adecuada actualización del formato FT-GT-12-19 Inventario activos de información Tipo Software, Hardware y Servicios IDEP, en el cual se adicionaron las columnas correspondientes a la clasificación de los activos teniendo en cuenta su confidencialidad disponibilidad, integralidad y criticidad, además se relacionan sus responsables, custodios, fecha de adquisición y caducidad, y placa Goobi.

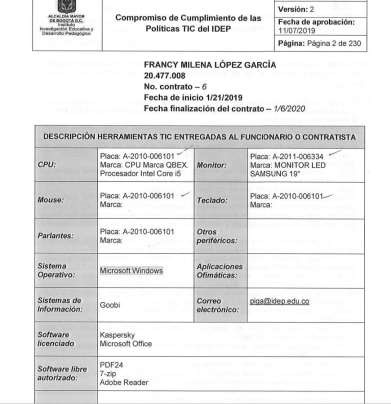
 Si bien el formato FT-GT-12-19 es considera el inventario oficial, todavía existen varios documentos con el inventario (Base de Datos de Activos de Información dic 2019.pdf, Activos IDEP consolidado Versión Ajustada, xls), en ninguno se tiene la totalidad del software instalado en los equipos de usuario de acuerdo al cruce de estos documentos con el Informe sobre las aplicaciones instaladas generado el 8-09-2020 10-50-53 a.m. desde la consola del antivirus, como se aprecia en la siguiente imagen, en la que se sobresaltan algunos que no se incluyen en los documentos mencionados:



 No se cuenta con una herramienta automatizada para la gestión de los inventarios de hardware y software, por lo cual el levantamiento de los mismos es dispendiosos y con alta probabilidad de errores, adicionalmente este inventario no esta sincronizado con el software de mesa de ayuda (HelpDesk), que permita tener un control de los incidentes presentados en los equipos o a causa del software instalado en el mismo y generar indicadores de capacidad y rendimiento de los mismos y tener una hoja de vida digital del hardware de la Entidad.

 No se cuenta con un seguimiento automatizado del licenciamiento en cada uno de los equipos de usuario, por lo tanto, no es posible identificar completamente los seriales y licencias instaladas, aumentando el riesgo de instalaciones o uso de software no autorizado, en las herramientas automatizadas de inventario de software existen funcionalidades para llevar en tiempo real el control de licenciamiento sobre todos los PC’s de la entidad.

 Al momento de entrega de activos se esta diligenciando el formato FT-GT-12-20 Compromiso de cumplimiento de las políticas TIC del Idep, en el cual se hace una descripción de las herramientas TIC entregadas a funcionarios o contratistas, pero no se detallan los accesos y perfiles de usuario en los sistemas de información asignados al usuario que firma el formato.



 En cuanto al mantenimiento se cuenta con un libro de Excel: “Plan de mantenimiento y monitoreo.xls” ene el cual se tiene programado el mantenimiento a los activos de la entidad y una columna de seguimiento en la cual se registran las observaciones a las acciones de mantenimiento y se relacionan con el proveedor responsable de las mismas. En la siguiente imagen se muestran los registros correspondientes a la vigencia de 2020:



 No se registra el plan de mantenimiento, ni el resultado de las acciones del mismo en la herramienta de mesa de ayuda, por ende, no es posible tener informes automatizados de estas acciones, ni relacionarlas con los soportes realizados a los equipos o sistemas instalados en ellos.

 No se han realizado actualizaciones al el *PRO-GT-12-05 Mantenimiento de Infraestructura Tecnológica* para incluir en el *Plan de Mantenimiento a la infraestructura y Servicios de Tecnología*, el uso del formato de mantenimiento preventivo y correctivo: *Formato Mantenimiento Preventivo a los Activos de Información IDEP,* que debe diligenciar el proveedor del servicio y que permite conocer el estado del equipo al momento del servicio y el software instalado.

#### 5.4.1.1 Seguimiento a Recomendaciones 2019

|  |  |  |  |
| --- | --- | --- | --- |
| **N°.** | **OBSERVACIÓN** |  | **SEGUIMIENTO** |
| 1. | Implementar una herramienta gratuita y de código abierto que permita hacer escaneo de hardware y software con el fin de mantener el control de los inventarios de manera centralizada y automatizada. Esta alternativa    disminuye carga operativa de mantener el control manual, facilita el chequeo de instalaciones ilegales de los equipos de red y permite llevar control de los usuarios responsables de los equipos para verificar |  | Aun no se cuenta con una herramienta que permita tener los inventarios de hardware y software automatizados, que permita cumplir con la recomendación dada. Se recomienda el uso del GLPI con la agente fusión Inventory de uso gratuito y de amplio uso en entidades del Distrito |

|  |  |  |  |
| --- | --- | --- | --- |
| **N°.** | **OBSERVACIÓN** |  | **SEGUIMIENTO** |
|  | autenticaciones de usuario en equipos que no le han sido asignados.  De ser implementada la herramienta mantener la trazabilidad de las placas de activos fijos |  |  |
| 2. | Como parte de la implementación del dominio  13 Gestión de comunicaciones, adelantar un formato de HV de servidores. |  | Aun no se cuenta con hojas de vida actualizadas de los servidores con todas las características técnicas necesarias para su adecuada identificación,  funciones y características |
| 3. | Optimizar el procedimiento administrativo y la comunicación entre las áreas de servicios generales y sistemas para disminuir las inconsistencias entre registros.  Incorporar en los registros de procesos y procedimientos de la OAP un acta de alta de activos de información que incluya equipos, software y accesos. Esta acta deberá suscribirse por el usuario una vez recibidos los activos y modificadas las claves de acceso a los sistemas y servicios. Esta acta es base para el control de devolución de activos de información al cese de la relación contractual de que habla el control ISO 27002:2013  9.2.6 Eliminación o ajuste de los derechos de acceso. Se sugiere usar un esquema similar al ejemplo presentado en el numeral 3.1.2 |  | Si bien se está diligenciando el formato  FT-GT-12-20 Compromiso de cumplimiento de las políticas TIC del  Idep, se debe complementar agregando las características faltantes definidas en la recomendación. |
| 4. | Incluir en el Plan de adquisiciones el escalamiento a las versiones de productos Microsoft que pierden soporte del fabricante. |  | Si bien no esta incluido en pal de adquisiciones este escalamiento ya se cuenta con el licenciamiento de servidores, el activo más crítico en cuanto a soporte del fabricante. Falta complementa el recambio de versiones en los equipos de usuario. |

#### 5.4.1.2 Nuevas Recomendaciones 2020

|  |  |
| --- | --- |
| **N°.** | **Recomendación 2020** |
| 1. | Atender las recomendaciones que se encuentran con flecha roja y/o amarilla del tablero de seguimiento a las recomendaciones 2019. |

### 5.4.2 Help Desk

 La configuración del sistema de registro incidentes y generación de tickets, OS tickets continua sin protecciones de acceso de usuario, y, por ende, cualquier persona que ingrese al vinculo en internet de la mesa de ayuda del Idep podría registrar un incidente o soporte.

En la siguiente imagen se muestra la funcionalidad en la herramienta para su

configuración, en donde se evidencia que no se encuentra activada para la autenticación para usuario final para poder generar tickets:

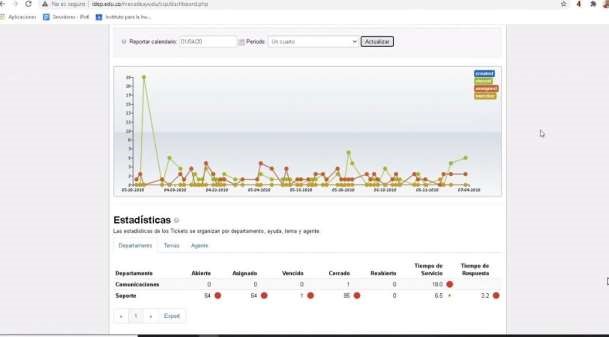


 Aún no se tiene configurados agentes de soporte para registrar y tramitar los incidentes a cargo de los proveedores de los sistemas de información, como medida de control de cumplimiento de los ANS y tampoco se han configurados agentes de soporte para registrar y tramitar los incidentes a cargo de los proveedores de los sistemas de información, como medida de control de cumplimiento de los ANS.

 No se tienen configurados los ANS (SLA) en el sistema por tipo de servicios y/o soporte, por tanto, no es posible determinar si se cumplen los tiempos de atención internos por tipo de soporte y la efectivad de atención del único agente de servicio creado en el sistema.



El único informe que se genera como control del servicio de la mesa de ayuda es de las estadísticas de tickets, como se aprecia en la siguiente imagen:



#### 5.4.2.1 Seguimiento a Recomendaciones 2019

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **N°.** | **OBSERVACIÓN** |  |  | **SEGUIMIENTO** | |  |  |
| 1. | Se debe configurar el sistema de tickets para que únicamente los usuarios registrados pueden crear solicitudes y así evitar posibles incidentes de seguridad o pérdida de tiempo de los agentes de soporte. |  | Aún no se recomendación. | muestra | avance | en | esta |
| 2. | Centralizar y clasificar todos los soportes relacionados con los sistemas y plataforma tecnológica del IDEP, incluyendo los sistemas de información y configurar el direccionamiento de estos soportes a los proveedores de los mismos, con el objeto de poder generar indicadores de todos los servicios y soportes del área y sus proveedores, incluyendo el cumplimiento de ANS. |  | Aún no se recomendación. | muestra | avance | en | esta |
| 3. | Se recomienda revisar los siguientes criterios para la configuración de la herramienta de tickets y o la implementación de una nueva herramienta gratuita y de código abierto como el GLPI: |  | Aún no se recomendación. | muestra avance | | en | esta |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **N°.** |  | **OBSERVACIÓN** |  | **SEGUIMIENTO** |
|  | • | Que permita configurar diferentes tipos de solicitudes hasta mínimo dos niveles jerárquicos: incidentes soporte, requerimientos de desarrollo, incidentes de seguridad, requisitos de adquisiciones de software o hardware, propuestas, etc. |  |  |
|  | • | Que permita configurar diferentes agentes de atención externos e internos clasificados por Agentes internos TIC, Agentes internos de negocio, agentes  externos proveedores |  |  |
|  | • | Que permita establecer ANS de acuerdo con la tipología de solicitudes y de agentes |  |  |
|  | • | Que permita una relación jerárquica entre solicitudes para aquellos casos en que una solicitud se segrega en varias tareas y de su cumplimiento dependa el estado de atención de la solicitud original |  |  |
|  | • | Que permita instalar un agente en los PC para que todas las solicitudes sean gestionadas por este medio con el fin de eliminar la carga operativa de la digitación de llamadas y correos y el riesgo de error humano. Adicionalmente la centralización de la información optimiza los tiempos de atención y la obtención de información estadística |  |  |
|  | • | Que permita generar reportes e  indicadores de gestión |  |  |
|  | • | Que permita instalar agente de escaneo de red para llevar la trazabilidad entre solicitud, usuario y equipo |  |  |
|  | • | Que permita adjuntar archivos tanto a la solicitud principal como a las tareas de la bitácora de atención |  |  |
|  | • | Que permita aplicar escalamientos. |  |  |
|  | • | Que integre un inventario de hardware y software por medio de agente. |  |  |

**5.4.2.2 Nuevas Recomendaciones 2020**

|  |  |
| --- | --- |
| **N°.** | **Recomendación 2020** |
| 2. | Atender las recomendaciones que se encuentran con flecha roja del tablero de seguimiento a las recomendaciones 2019. |

**6 CONCLUSIONES:**

La presente auditoría evidencia que la OAP ha adelantado un proceso de análisis de las recomendaciones emitidas en el informe de auditoría del 2019, cuyo resultado se refleja en la mejora de algunos de los componentes evaluados entre los que se destacan:

* Mejoramiento en la documentación e instructivos para la gestión y administración de la plataforma tecnológica del Idep para dar continuidad a la operación.
* Mejorar en entorno de contingencia de la plataforma TIC.
* Avances en materia de implementación tecnológica de controles en materia de seguridad informática y gestión de contraseñas.
* Avances en la adopción de IPv6

Sin embargo, la auditoría también pone en evidencia que algunos componentes presentan debilidades de control que requieren de atención prioritaria de las acciones de mejoramiento ya que exponen a la entidad a riesgos de fallas en la operación de servicios tecnológicos y seguridad informática.

Si bien se está adelantado el proceso de identificación y administración de riesgos TIC y de seguridad de la información en el marco de implementación del MSPI, este componente debe ser priorizado, ya que no solo ofrece elementos de cumplimiento documental, sino que es la base para determinar la manera de asegurar la plataforma tecnológica y la gestión TIC con controles efectivos y medibles, además de ser la base para la actualización de un plan de Continuidad efectivo.

## 7 RECOMENDACIONES

Las recomendaciones emitidas se presentan en cada ítem del capítulo 5 de este documento



**HILDA YAMILE MORALES LAVERDE**

Jefe de Control Interno

|  |  |  |
| --- | --- | --- |
|  | Nombre / Cargo | Firma |
| Aprobó | Hilda Yamile Morales Laverde – Jefe Oficina de Control Interno |  |
| Revisó | Hilda Yamile Morales Laverde – Jefe Oficina de Control Interno |  |
| Elaboró | Yadira Velosa Poveda – Profesional Contratista OCI. |  |
| Los arriba firmantes declaramos que hemos revisado el presente documento y lo encontramos ajustado a las normas y disposiciones legales y/o técnicas vigentes | | |