UNIDAD ADMINISTRATIVA ESPECIAL DE ORGANIZACIONES SOLIDARIAS

INFORME DE AUDITORÍA DE EVALUACIÓN INDEPENDIENTE AL PROCESO:

GESTIÓN INFORMÁTICA

OFICINA DE CONTROL INTERNO

JUNIO 2022

INFORME DE AUDITORÍA DE EVALUACIÓN INDEPENDIENTE AL PROCESO

GESTIÓN INFORMÁTICA

OBJETIVOS DE LA AUDITORIA

- Verificar las estrategias, planes y procedimientos definidos por el proceso, en pro de garantizar la disponibilidad y confiabilidad de los servicios y productos TIC, así como las actividades adelantadas para asegurar la infraestructura tecnológica, en el marco de la normatividad vigente garantizando la seguridad de los activos de información de cada uno de los procesos de la Unidad Administrativa Especial de Organizaciones Solidarias.

OBJETIVOS ESPECIFICOS:

- Verificar los riesgos del proceso con mayor nivel de riesgo inherente, verificar la eficacia de los controles y la implementación de las acciones de mitigación planteadas.
- Verificar el cumplimiento de los parámetros expresados en la política de seguridad de la información haciendo énfasis en los Backups de la información y en la funcionalidad de los aplicativos desarrollados por la Unidad.
- Verificar el cumplimiento de la Política de gestión de tecnológicas de la información y comunicaciones
- Verificar el cumplimiento de los requisitos del MSPI (Modelo de seguridad y privacidad de la información)
- Verificar cumplimiento de los numerales 3 (requisitos de nivel de conformidad) y 4 (Conformidad), de la norma NTC 5854:2011 Accesibilidad a páginas web.
- Verificar los controles de seguridad, acceso y gestión en la administración de usuarios de los sistemas de información que utiliza la Unidad.
- Verificar el cumplimiento de las actividades de préstamo y retiro de equipos tecnológicos
- Verificar el avance del plan de acción del grupo TICS con corte a 30 de abril 2022
- Verificar reporte de indicadores del proceso
- Verificar inventario de bienes devolutivos

ALCANCE

El seguimiento al plan de acción cubre las actividades desarrolladas entre el 1 de enero de 2022 y el 30 de abril. Las demás actividades del proceso pueden contemplar información y evidencias de la vigencia 2021.

GRUPO / PROCESO A AUDITAR

Grupo de Gestión de tecnologías de la Información / Proceso Gestión Informática

OBJETIVOS INSTITUCIONALES RELACIONADOS CON LA DEPENDENCIA:

- Fomentar la cultura asociativa solidaria para generar conocimiento de los principios, valores y bondades del sector solidario
- Promover la generación de ingresos y la inclusión social y productiva de la población a través del emprendimiento solidario
- Fortalecimiento a la institucionalidad pública y la participación ciudadana para el desarrollo del modelo asociativo solidario en esquemas de buen gobierno, gobernanza y gobernabilidad.

CRITERIOS DE AUDITORÍA

- Política de gestión de tecnológicas de la información y comunicaciones – tic
- Política de préstamo y retiro de equipos tecnológicos – tic
- Política de seguridad y privacidad de la información
- Caracterización del proceso
- Ntc 5854 accesibilidad a páginas web
- Ley 1712 de 2014 ley de transparencia y acceso a la información pública
- Resolución 1519 de 2020 del Ministerio de la información y las comunicaciones
- Procedimientos del proceso

METODOLOGÍA UTILIZADA

La Oficina de control interno realizó auditoría basada en los riesgos, identificados en el mapa de riesgos del proceso y en el mapa de riesgos de corrupción, y verificó las acciones de mitigación, su actualización con respecto a la nueva política de administración de riesgos y el tratamiento dado a los riesgos materializados.

Adicionalmente, se realizó seguimiento a las actividades establecidas en el plan de acción del grupo de gestión informática con corte a 30 de abril de 2022.

Por otra parte se revisaron los temas de:

- Cumplimiento de los parámetros expresados en la política de seguridad de la información
- Verificar el cumplimiento de la Política de gestión de tecnologías de la información y comunicaciones.
- Requisitos del MSPI (Modelo de seguridad y privacidad de la información)
- Norma NTC 5854:2011
- Controles de seguridad, acceso y gestión en la administración de usuarios de los sistemas de información
- Préstamo y retiro de equipos tecnológicos
- Indicadores de gestión del proceso
- Inventario de bienes devolutivos

- Proyecto de inversión “Fortalecimiento de la infraestructura tecnológica de la unidad administrativa especial organizaciones solidarias a nivel nacional”
- Seguimiento a recomendaciones emitidas por la OCI en anteriores auditorías

COMUNICACIÓN DE RESULTADOS

RIESGOS DEL PROCESO

La Oficina de control interno verificó el mapa de riesgos de procesos publicado en la página web, identificando aquellos que en su valoración de riesgo inherente presenten calificación más alta, de lo cual evidenció:

Identificación del Riesgo		Análisis del Riesgo Inherente	Evaluación del riesgo - Nivel del riesgo residual	
Causa Raíz	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo	Tratamiento
Debido a la no contratación de los procesos indispensables (mantenimiento preventivo y correctivo de hardware y software, obsolescencia de equipos tecnológicos) para el funcionamiento de la UAEOS.	Posibilidad de pérdida reputacional y económica, debido a la no contratación de los procesos indispensables (mantenimiento preventivo y correctivo de hardware y software, obsolescencia de equipos tecnológicos) para el funcionamiento de la UAEOS.	Alto	Alto	Reducir
Debido a un inadecuado manejo y mantenimiento de los equipos, fallas por factores internos o externos (Falta de cuidado en la manipulación y cuidado de equipos por personal de mantenimiento y funcionarios en general, suministro de energía eléctrica, fallas en internet, desastre natural, equipos obsoletos, o adecuaciones físicas de infraestructura no planeadas).	Posibilidad de pérdida económica y reputacional, debido a un inadecuado manejo y mantenimiento de los equipos, fallas por factores internos o externos (Falta de cuidado en la manipulación y cuidado de equipos por personal de mantenimiento y funcionarios en general, suministro de energía eléctrica, fallas en internet, desastre natural, equipos obsoletos, o adecuaciones físicas de infraestructura no planeadas).	Bajo	Bajo	Reducir
Debido a uso de software sin licencia, a fallas en la seguridad informática, de sus redes y bases de datos por manejo de personal no autorizado.	Posibilidad de pérdida económica y reputacional, debido al uso de software sin licencia, a fallas en la seguridad informática, de sus redes y bases de datos por manejo de personal no autorizado.	Alto	Alto	
Debido a sistemas de información susceptibles de manipulación o adulteración por personal no autorizado.	Posibilidad de pérdida económica y reputacional, debido a sistemas de información susceptibles de manipulación o adulteración por personal no autorizado.	Alto	Alto	Reducir

La Oficina de control Interno realizo seguimiento a los riesgos del proceso evidenciando lo siguiente:

DESCRIPCIÓN DEL RIESGO	DESCRIPCIÓN DEL CONTROL	SEGUIMIENTO
Posibilidad de pérdida reputacional y económica, debido a la no contratación de los procesos indispensables (mantenimiento preventivo y correctivo de hardware y software, obsolescencia de equipos tecnológicos) para el funcionamiento de la UAEOS.	Realizar planeación (establecer prioridades y necesidades) de los recursos presupuestales necesarios para adelantar las actividades de contratación.	Con el fin de tener claras las prioridades y necesidades en software y hardware de la entidad, existen contratos para cada uno de estos. Allí se hace una revisión previa que permite establecer qué necesidades tiene la entidad para la contratación y así planificar anticipadamente.
Posibilidad de pérdida económica y reputacional, debido a un inadecuado manejo y mantenimiento de los equipos, fallas por factores internos o externos (Falta de cuidado en la manipulación y cuidado de equipos por personal de mantenimiento y funcionarios en general, suministro de energía eléctrica, fallas en internet, desastre natural, equipos obsoletos, o adecuaciones físicas de infraestructura no planeadas).	Verificar informes ejecución del Plan de mantenimiento de software y hardware	De la información suministrada con el grupo de gestión informática, se logró evidenciar que hay contratos de mantenimiento del software, hardware y desarrolladores en la entidad. Esto con el fin de determinar la vida útil de la infraestructura informática.
Posibilidad de pérdida económica y reputacional, debido al uso de software sin licencia, a fallas en la seguridad informática, de sus redes y bases de datos por manejo de personal no autorizado.	Verificar el software instalado en los equipos de cómputo de la Entidad.	El contrato de mantenimiento ayuda en la revisión de los softwares instalados. Se hace una verificación de que los equipos tengan únicamente software licenciados. Si el funcionario hace una solicitud en la mesa de ayuda, relacionado con el funcionamiento de sus equipos, desde el grupo de informática se revisa los programas que allí se encuentran, desinstalando aquellos que no estén permitidos e informando la novedad al usuario. No es necesaria la solicitud a mesa de ayuda para estos análisis, en cualquier momento esa dependencia lo realiza.
Posibilidad de pérdida económica y reputacional, debido a sistemas de información susceptibles de manipulación o adulteración por personal no autorizado.	Actualizar los Usuarios con accesos, permisos de Administrador y contraseñas, para los diferentes aplicativos, Servidores y equipos de Cómputo.	El grupo de gestión informática manifiesta que existe un apoyo en el contrato de mantenimiento para realizar actualización de contraseñas. Respecto de acceso a los aplicativos, esta dependencia tiene un protocolo de cambio de contraseñas. Cada 4 meses generan alertas de cambios y/o actualización de accesos, usuarios, contraseñas y demás necesidades.

Se evidenció que la redacción de los riesgos, así como de los controles, se encuentran ajustados de conformidad con la política de administración de riesgos versión 2 del 25 de febrero de 2021 y su correspondiente metodología de identificación, valoración y control.

Se materializó el riesgo con el aplicativo NOVASOFT el cual entró en conflicto al generar la liquidación del retroactivo y el mes de mayo, por lo cual fue necesario regenerar la nómina en Excel y concertar mesa de trabajo con Novasoft para el soporte técnico, cargue de la información y revisión de ajustes, de lo cual se evidenció que actualmente la Unidad no cuenta con contrato de actualización y soporte técnico. Dicha materialización no se vio reflejada en mapa de riesgos de Gestión Informática. Se recomienda identificar, valorar y dar tratamiento a los riesgos que se generen con las aplicaciones ya sea de desarrollo interno o externo de la Unidad.

SEGUIMIENTO AL PLAN DE ACCIÓN

ACTIVIDAD GENERAL ASOCIADOS AL CUMPLIMIENTO DEL OBJETIVO INSTITUCIONAL	5. MEDICIÓN DE COMPROMISOS	
	5.1 % LOGRADO	**5.2 ANÁLISIS DE RESULTADOS**
1. Continuar la Implementación de la política de Gobierno Digital en la Entidad		
1.1. Revisión y actualización de la Arquitectura TI	0% de 2% 0 de 1 tablero de control para la gestión de TI diseñado e implementado	Se evidenció identificación de los aspectos de Tecnologías de la información que se monitorearan en el tablero de control, la cual incluye los siguientes aspectos: ✓ Medición de los servicios tecnológicos ✓ Medición de proyectos ✓ Medición de los procedimientos de gestión informática ✓ Medición del Plan Estratégico de Tecnologías ✓ Medición de la estrategia de uso y apropiación Se proyecta documento con la definición de la arquitectura y componentes del sistema de información SSIOS. Adicionalmente se evidenció que la entrega del tablero de control se tiene programada para el mes de julio 2022 con lo cuao se completaría el 100% de la actividad.
	1% de 1% 1 de 1 Documento de la Arquitectura de Solución del sistemas de información SSIOS	Se evidenció Documento de la Arquitectura de Solución del sistema de información SSIOS, el cual se encuentra en la siguiente ruta: Z:\ARCHIVO GTI_TRD_2022\124.03 PLANES\Plan Accion\4. Abril
1.2 Implementación, actualización y seguimiento a los planes integrados del Grupo de Tecnologías de la Información. (PETI, Plan de seguridad y privacidad de la información, Plan de tratamiento de riesgos de seguridad digital y Plan de Mantenimiento de servicios tecnológicos)	1.05% de 3% 35% de 100% de ejecución de las actividades de PETI 2022	De acuerdo a las actividades definidas el plan estratégico de tecnologías de la información UAEOS y el seguimiento realizado en el mes de abril, se evidencia un avance del 35%, correspondiente al avance de la ejecución contractual del proyecto de inversión que son tres desarrolladores, implementación gobierno digital, soporte nivel tres, avance de licencias, avance de la gestión del contrato de mantenimiento, compra de equipos, entre otros.
	0% de 1% 0 de Una (1) Actualización del Plan Estratégico de Tecnologías 2023	Se evidenció la proyección del Plan Estratégico de Tecnologías identificando necesidades tecnológicas de talento humano para los proyectos que se definirán para la siguiente vigencia Se evidenció que la actualización del plan estratégico se encuentra planeada para el mes de septiembre 2022, para lo cual se requiere conocer el presupuesto aprobado para la vigencia 2023.
	0.66% de 2% 35% de 100% de ejecución de las actividades del plan de seguridad y	La ejecución de las actividades del plan de seguridad de la información se presenta avance 35%, se evidenció en las siguientes rutas: Z:\ARCHIVO GTI_TRD_2022\124.03 PLANES\Plan de Seguridad de la información. Ruta Onedriver: https://solidarias-my.sharepoint.com/:f:/g/personal/

	privacidad de la información 2022.	laura_malaver_uaeos_gov_co/EuB _gCMhIcZFjZBas7kI8pkBdWs8iGtnEtmb6CRCOFpgJA?e=QKia7N"
	0,35% de 1% 0,35 de Una (1) Actualización Plan de seguridad y privacidad de la información 2023	Se informa que, para la actualización del plan de seguridad y privacidad de la información, se tendrá en cuenta el desarrollo de la directiva presidencial 02-2022 reiteración de la política pública en materia de seguridad digital y la ejecución del plan de seguridad vigencia 2022, se evidenció que a 30 de abril se han desarrollado varias actividades del plan, alcanzando un avance del 35%
	0,2% de 1% 2 de 3 Reportes de Seguimiento al plan de tratamiento de Riesgos de seguridad Digital	Se evidenció el reporte mensual del plan de tratamiento de riesgos de seguridad digital para los meses de marzo y abril, por tanto se evidenció que la actividad del reporte se está realizando mensualmente desde el mes de marzo, se recomienda solicitar ajuste de la meta de 3 reportes a 10 reportes de Seguimiento al plan de tratamiento de Riesgos de seguridad Digital para la presente vigencia. 2 de 10
	0% de 2% 0 de 1 informe final de Seguimiento del plan de tratamiento de Riesgos de seguridad Digital	Se tienen planeado realizar el informe del plan de tratamiento de Riesgos de seguridad Digital para el mes de noviembre.
	0% de 1% 0 de 1 Actualización plan de tratamiento de Riesgos de seguridad Digital 2023	Se evidenció que, durante el seguimiento a los controles del plan de tratamiento de riesgos, se identificaron nuevos riesgos de seguridad asociados a los procesos con sus respectivos controles, los cuales definirán el plan de tratamiento de riesgos de seguridad digital 2023. Actividad programada para el mes de septiembre de 2022, sin embargo, se evidenció que, en cumplimiento de la política de administración de riesgos de la Unidad, se está realizando integración de los riesgos de seguridad digital, en el mapa institucional de riesgos de la Unidad.
	0% de 2% 0% de 100 % de ejecución de las actividades del plan de mantenimiento de servicios tecnológicos 2022	Se evidenció que para el proceso de contratación del servicio mantenimiento preventivo y correctivo se encuentra la proyección de Análisis del Sector y Análisis del mercado y actualización de Estudios previos. Adicionalmente se presentó un reproceso en la respuesta a la solicitud cotización por parte de los oferentes, razón por la cual la contratación de los servicios de mantenimiento de TICS pasó de febrero a junio en el Plan anual de adquisiciones. Las jornadas de mantenimiento preventivo se tienen programadas para los meses de julio y diciembre de 2022.
	0% de 1% 0 de 1 Actualización Plan de mantenimiento de servicios tecnológicos 2023	Se tiene planeado realizar la actualización en el mes de septiembre, las novedades que se encuentran el Plan de Mantenimiento se tendrán en cuenta para la actualización del Plan para la vigencia del 2023

	1% de 2% 51% de 100 % de ejecución de las actividades del plan de Transformación Digital	Se evidenció el seguimiento al plan de Transformación Digital y se evidencia un avance del 51%, del cual se encuentra el registro de la actividad en el link: Z:\ARCHIVO GTI_TRD_2022\124.03 PLANES\Plan de Transformación Digital"
	0% de 1% 0 de1 informe final de Seguimiento del plan de Transformación Digital	Actividad programada para el mes de noviembre de 2022.
1.3 Actualizar e implementar el plan de comunicación y sensibilización de la política de gobierno digital y seguridad de la información.	0.64% de 2% 32% de 100% de ejecución de las actividades del Plan de Comunicación y Sensibilización de la política de gobierno digital y seguridad de la información 2022.	Dentro del Plan de Sensibilización se evidenció la elaboración de tips sobre los siguientes temas: *Almacenamiento y respaldo de la información- el tip fue enviado por correo electrónico a todos los funcionarios de la entidad. *Teletrabajo Seguro * Como funciona el PHISHING * Conoces la Secretaría de Transparencia *Protección de datos personales en redes sociales * Consejos de seguridad para uso de WhatsApp Los TIPS fueron enviados por correo electrónico a todos los funcionarios de la entidad. Adicionalmente se ha avanzado en actividades como: - Capacitaciones a usuarios de sistemas de información - Capacitación de transformación digital - Capacitación de accesibilidad web
	0% de 1% 0 de 1 Actualización Plan de Comunicación y Sensibilización 2023	Se evidenció que las novedades que se encuentran el Plan comunicaciones y sensibilización se tendrán en cuenta para la actualización del Plan para la vigencia del 2023 donde se tiene planeado realizar la actualización en el mes de Octubre.
	0% de 1% 0 de 2 Informe general del resultado de la implementación del plan de comunicación y sensibilización.	El informe de la implementación del plan de comunicación y sensibilización, se tiene planeado realizar en el mes de mayo y diciembre de 2022
2. Transparencia y Acceso a la Información Pública		
2.1 Mantenimiento y actualización del menú de Transparencia y Acceso a la información pública de la página web	1.33% de 4% 1 de 3 Informes Trimestral de la gestión adelantada	Se evidenció seguimiento al menú de transparencia de acceso a la información publica y a la página web El reporte se encuentra en la siguiente ruta: Z:\ARCHIVO GTI_TRD_2022\124.03 PLANES\Plan Accion\4. Abril

	del menú de transparencia.	
3. Mantener en óptimas condiciones la plataforma tecnológica para garantizar la disponibilidad de la información y servicios tecnológicos		
3.1. Renovar y actualizar las licencias de software de seguridad de la UAEOS.	0% de 7% 0 de 154 licencias de software de seguridad instaladas.	Se evidenció que en el plan anual de adquisiciones esta programado para el mes de junio, sin embargo, se evidenció cronograma de contratación en el cual se prevé ajustar la contratación para el mes de agoto de 2022, teniendo en cuenta que el licenciamiento del software se vence en el mes de diciembre de 2022
3.2 Renovar y actualizar las licencias de office 365 para los funcionarios de la entidad	0% de 6% 0 de 213 renovación y adquisición de licencias de office 365, Windows 2019 Server y Suite Office 2019.	Esta Actividad está sujeta al vencimiento de las licencias Adquiridas en la vigencia del 2021, la cual vence en el mes de diciembre del 2022 y el proceso de la nueva contratación inicia en el mes de octubre. De acuerdo con las licencias adquiridas en la vigencia del 2021 se realiza la asignación a los funcionarios y contratistas que van ingresando a la entidad y según lo solicitado en la mesa de ayuda. Se evidenció que actualmente se encuentran asignadas las licencias así: Exchange Online (plan 1): 127 / 131 Office 365 E1: 40 / 40 Office 365 E3: 3 / 3"
3.3 Garantizar la disponibilidad y funcionamiento de las copias de seguridad de la información de la UAEOS	3% de 9% 4 de 12 informes de copias de seguridad realizadas.	Se evidenciaron 4 informes de copias de seguridad de: * Carpetas compartidas y aplicaciones a través de la herramienta Cobián – el cual es realizado diariamente en una hora específica por tarea y el soporte del desarrollo de la actividad se encuentra en la siguiente ruta: M:\ARCHIVO GTI_TRD_2022\124.02 INFORMES\Informes de Funcionarios \Katia Jimenez\Cobian\Abril 2022
	1.66% de 5% 1 de 3 informes trimestrales de pruebas de recuperación de acuerdo a las políticas de Backup.	Se evidenció la realización del primer informe en el mes de marzo y se tiene planeado realizar el 2 informe para el mes Junio. Se evidenció el primer informe de pruebas de recuperación de los sistemas de información en el mes de marzo, el cual se encuentra en la siguiente ruta: Z:\ARCHIVO GTI_TRD_2022\124.03 PLANES\Plan Accion\4. Abril
3.4. Realizar las actualizaciones de software (Parches de seguridad, firmware, Sistemas operativos, Servicios, Módulos) de la infraestructura tecnológica.	1.75% de 7% 1 de 4 reportes de actualizaciones de software	Se evidenció primer reporte de actualización de software, correspondiente al periodo enero a marzo de 2022, el cual se encuentra en la ruta: Z:\ARCHIVO GTI_TRD_2022\124.03 PLANES\Plan Accion\3. Marzo
3.5 Realizar reporte sobre la gestión del inventario de hardware Grupo de Tecnologías de Información.	1.5% de 3% 1 de 2 reportes de gestión de inventario de hardware a cargo	Se evidenció la actualización del inventario de acuerdo con los traslados o cambios de equipos que se realicen. Se tiene programado la segunda revisión y actualización del inventario para el mes noviembre de 2022.

	del grupo de Tecnologías	
3.6 Realizar revisión y reporte de deterioro de los equipos tecnológicos	1% de 2% 1 de 2 reportes de deterioro de los equipos tecnológicos	Se evidenció reporte de ampliación de vidas útiles de los equipos Tecnológicos, se envía al Grupo de Administrativa a través de correo electrónico del día 30 del mes de marzo de 2022. Se tiene programado realizar el segundo reporte para el mes de junio de 2022
3.7. Adquirir y configurar el hardware necesario conforme a las necesidades de la Unidad.	0% de 2% 0 de 18 componentes de tipo hardware adquiridos y configurados.	Para el proceso de Contratación para la Adquisición de Hardware, se evidenció que a 30 de abril se adelantó el proceso precontractual para la adquisición de 18 equipos de cómputo, los cuales se planea instalar entre agosto y septiembre.
4. Gestionar los servicios y sistemas de información de la UAEOS		
4.1. Atender las solicitudes de soporte técnico realizadas por los usuarios de la Unidad.	1.66% de 5% 33% de 100% de las solicitudes de soporte técnico atendidas.	Con corte a 30 de abril de 2022 se evidenciaron un total de 320 solicitudes gestionadas por la mesa de ayuda El reporte se encuentra en la siguiente ruta: M:\ARCHIVO GTI_TRD_2022\124.02 INFORMES\Informes de Funcionarios\ Katia Jimenez\GLPI\Abril 2022
4.2 seguimiento a la estrategia de Uso y apropiación del Grupos Tics	0% de 2% 0 de 1 Evaluaciones Uso, apropiación y seguimiento a los sistemas de información y equipo tecnológico de la entidad.	Se identificaron las preguntas esenciales para la definición de la evaluación de uso y apropiación para aplicar a los funcionarios y medir de manera efectiva el conocimiento de TI que hay en la entidad, la cual se aplicará a partir del 1 de junio. Se evidenció que se tiene programado aplicar dos evaluaciones, la primera en el mes de junio, la segunda en el mes de noviembre, sin embargo, en la meta de la actividad se planteó 1 evaluación, se recomienda ajustar la meta del plan de acción a 2 evaluaciones de Uso, apropiación y seguimiento a los sistemas de información y equipo tecnológico de la entidad.
	0% de 1% 0 de 2 informe de seguimiento a las Evaluaciones de Uso, apropiación y seguimiento a los sistemas de información y equipo tecnológico de la entidad.	Se tiene planeado realizar el informe con base en los resultados de la evaluación realizada en junio de 2022.
4.3 Consultar los servicios tecnológicos productivos	2,47% de 8% 34.629 de 127.920 Consultas realizadas a los servicios web de la entidad.	De acuerdo a las consultas realizadas durante los meses de enero a abril de 2022 se realizaron un total de 34.629 consultas de usuarios nuevos en, centro documental, compras públicas locales, mapa de gestión, portal web, cursos virtuales, SIIA.
4.4 Realizar revisión y reporte de deterioro de los sistemas de información	1% de 2% 1 de 2 reportes de deterioro de los	Se realiza actualización y reporte de las vidas útiles de los intangibles, donde se envía el correo al grupo de Financiera el día 21 de abril de 2022.

	sistemas de información	
4.5. Realizar e implementar el Plan de gestión de servicios de TI.	0,3% de 1% 0,3 de 1 Plan de gestión de servicios de TI.	Se realizó verificación del inventario de Software y Hardware, correspondiente al grupo Tic's con el fin de evaluar su capacidad y vida útil, para identificar los cambios futuros de acuerdo a la demanda de servicios de TI de los funcionarios. A la fecha la actividad se inició con la revisión del inventario del grupo TIC´s que es el insumo para la elaboración del plan de gestión de servicios TI. Se evidenció que con corte a 30 de abril se reportó 30% de avance.
4.6. Implementar aplicaciones de software a la medida de las necesidades de la UAEOS.	1.33% de 4% 1 de 3 informes de implementación aplicaciones de software a la medida de las necesidades de la UAEOS.	Se realizó el informe de implementación aplicaciones de software a la medida de las necesidades de la UAEOS. El reporte se encuentra en la siguiente ruta: M:\ARCHIVO GTI_TRD_2022\124.02 INFORMES\Informes de Funcionarios\ Katia Jimenez\GLPI\Abril 2022" Los informes restantes se encuentran programados para los meses de agosto y diciembre
4,7 Apoyar técnicamente a las transmisiones de eventos virtuales o presenciales que realiza la entidad	1.25% de 4% 33.33% de 100% de las solicitudes allegas	Durante los meses de enero a abril de 2022 se solicitaron 22 apoyos técnicos a las transmisiones de eventos virtuales o presenciales que realiza la entidad.
5. Implementar las dimensiones y políticas que conforman el MIPG para lograr una mayor apropiación y cumplimiento adecuado de las funciones, garantizando la satisfacción y participación ciudadana		
5.1 Adelantar las actividades para la implementación de las políticas que conforman el MIPG de acuerdo al plan de trabajo dispuesto por la Entidad	1,25% de 4% 33, 3%100% del Cumplimiento de las actividades asignadas del MIPG	Se realizo el reporte correspondiente a: • Actualizar el directorio de sistemas de información de la UAEOS • Implementar lineamientos de accesibilidad web en la sede electrónica institucional • Capacitación a los funcionarios de la entidad sobre Accesibilidad • Realizar divulgación y comunicación interna de los proyectos de TI" • Actualizar el documento de Estrategia de uso y apropiación 2022 • Realizar evaluación del nivel de adopción de TI en la UAEOS • Revisar y actualizar el catálogo de servicios de TI • La entidad desarrolló durante el periodo evaluado capacidades de gestión de TI que generen mayor eficiencia en la prestación del servicio al usuario (interno o externo) • Seguimiento al plan de mejoramiento producto de la auditoría de tecnologías de la información • Continuar con el desarrollo de las actividades contempladas en el Plan Anticorrupción: componente 5 Transparencia y acceso a la información. • Reporte oportuno de plan de acción • Reporte oportuno de indicadores • Reporte oportuno de SPI Reporte oportuno de riesgos
CUMPLIMIENTO TOTAL A ABRIL 30 DE 2022		**24,4%**

DESARROLLO Y OPERACIÓN DE APLICACIONES DE LA UNIDAD

La oficina de control interno realizó seguimiento del estado de las aplicaciones de la Unidad de lo cual evidenció:

- ✓ **Página WEB** en operación, actualización y mejora. Se accede a través de https://www.uaeos.gov.co/
- ✓ **SIIA**, en operación y actualización y mejora. https://acreditacion.uaeos.gov.co/siia/
- ✓ **INTRANET**, en operación, actualización y mejora. http://institucional.uaeos.gov.co/intranet/en
- ✓ **SISTEMA DE INVENTARIO**, no se encuentra en operación pero se encuentra en actualización y mejora. http://institucional.uaeos.gov.co/inventario/
  Se tiene planeado incluir los nuevos campos de acuerdo al proceso actual.
- ✓ **CERTIFICADOS LABORALES**, se entregó en funcionamiento listo para operación en la vigencia 2021, sin embargo, no se realizó la divulgación debido a la falta de un requisito de cargas masivas, el cual se encuentra pendiente a nivel de contratistas. Se tiene programado iniciar su operación en el mes de julio de 2022 para todos los funcionarios de la unidad. https://institucional.uaeos.gov.co/certificados/public/
- ✓ **CURSOS VIRTUALES,** en operación, actualización y mejora. **http://virtuales.uaeos.gov.co/virtuales/**
- ✓ **MAPA DE GESTIÓN,** en operación, con soporte y mantenimiento. https://virtuales.uaeos.gov.co/mapagestion/mapas/
- ✓ **ENCUESTA ATENCIÓN AL CIUDADANO,** en operación con soporte y mantenimiento. http://virtuales.uaeos.gov.co/encuesta/public/preguntas
- ✓ **DIRECTORIO DE FUNCIONARIOS,** en operación, actualización y mejora. https://virtuales.uaeos.gov.co/funcionarios/public/
- ✓ **CENTRO DOCUMENTAL KOHA,** en operación con soporte y mantenimiento. https://virtuales.uaeos.gov.co:8081/
- ✓ **SGDEA,** en operación. http://sgd.uaeos.gov.co/SGDEA/
- ✓ **PQRDS,** en operación. Actualmente, se viene actualizando, encontrándose pendiente ajustes con el apoyo de soporte nivel 3, en lo referente al correo electrónico. https://sitios.uaeos.gov.co/portal/pqr/index.php?idcategoria=6
- ✓ **SISTEMA DE GESTIÓN DE CALIDAD,** se encuentra en desarrollo (reemplazo de Isolución).
- ✓ **COMPRAS PÚBLICAS LOCALES (SITIOS WEB DE CONSULTA),** en operación, actualización y mejora. https://virtuales.uaeos.gov.co/locales/
- ✓ **PLANFES (SITIOS WEB DE CONSULTA),** en operación, actualización y mejora. http://sitios.uaeos.gov.co/PAZ/
- ✓ **CADENA DE VALOR,** en operación, sin embargo, para su funcionamiento se requiere de una actualización y mejora. http://institucional.uaeos.gov.co/cadenaValor/
- ✓ **GESTIÓN CONTRACTUAL,** el aplicativo se encuentra en funcionamiento, sin embargo por la ley de garantías electorales de la presente vigencia no se pudo iniciar su operación. A la fecha se están adelantando las actualizaciones de formatos con

lo cual se planea dar inicio al aplicativo para la contratación 2023. https://institucional.uaeos.gov.co/contractual/public/

- ✓ **PORTAL PARA NIÑOS,** en operación con soporte y mantenimiento. https://virtuales.uaeos.gov.co/portalninos/public/
- ✓ **JUEGO AVENSOL,** en operación. https://virtuales.uaeos.gov.co/AvenSol/
- ✓ **PORTAL EDUCACIÓN SOLIDARIA,** en operación con soporte y mantenimiento. https://virtuales.uaeos.gov.co/educacionSolidaria/
- ✓ **REGISTRO HOJAS DE VIDA,** en operación, actualización y mejora. https://virtuales.uaeos.gov.co/registroHV/public/crearHoja
- ✓ **SISTEMA DE VIÁTICOS**, en desarrollo. https://institucional.uaeos.gov.co/viaticos/public/
- ✓ **EVALUACIÓN A PROVISIONALES,** en desarrollo. https://institucional.uaeos.gov.co/evaluacion/public

Cumplimiento de los parámetros expresados en la política de seguridad de la información haciendo énfasis en los backup de la información.

Se evidenció que los backup a los sistemas de información, aplicativos e información que se encuentra alojada en la carpeta compartida y solicitudes especiales, se vienen realizando diariamente y en diferentes horarios entre las 6:00pm hasta las 10:30pm que se realiza la última tarea, con el fin de evitar la congestión de la red. Así mismo se evidenció que de conformidad con las políticas de seguridad de la información no se realiza backup a la información alojada en los equipos personales, equipos de trabajo en casa, información alojada en la nube por cada funcionario individualmente. Estos Backups se realizan en disco duros propios que están custodiados por el profesional del grupo TICS Katia Jiménez, y se guarda en una oficina bajo llave. El profesional mencionado es la única persona con acceso a estos discos duros, los cuales son almacenados en un área separada y con control de acceso. También se evidenció que se encuentra información de respaldo en la NUBE, sin embargo, el espacio no es suficiente y este no permite el almacenamiento de información con caracteres específicos o nombres de archivo muy largos. Por lo anterior, se evidenció que los backup se encuentran almacenados en la nube y en unidades de disco duro internas, cumpliendo con el numeral 5.7 de la política de seguridad y privacidad de la información.

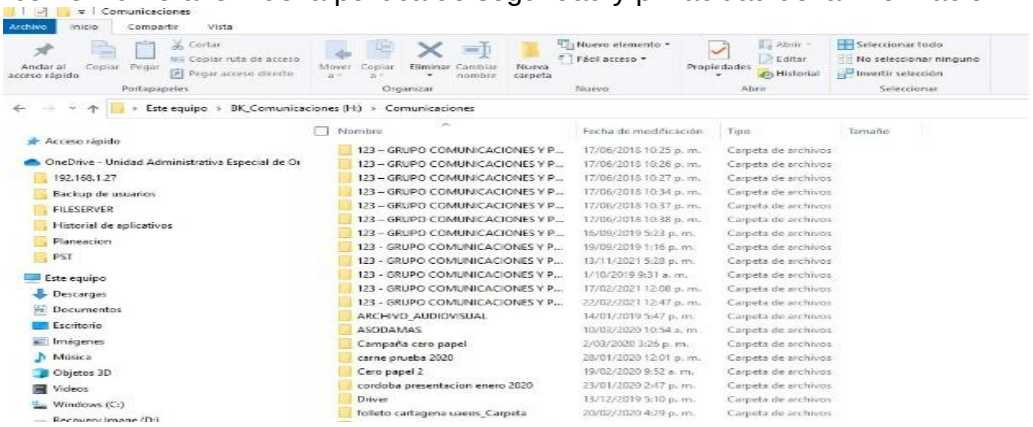
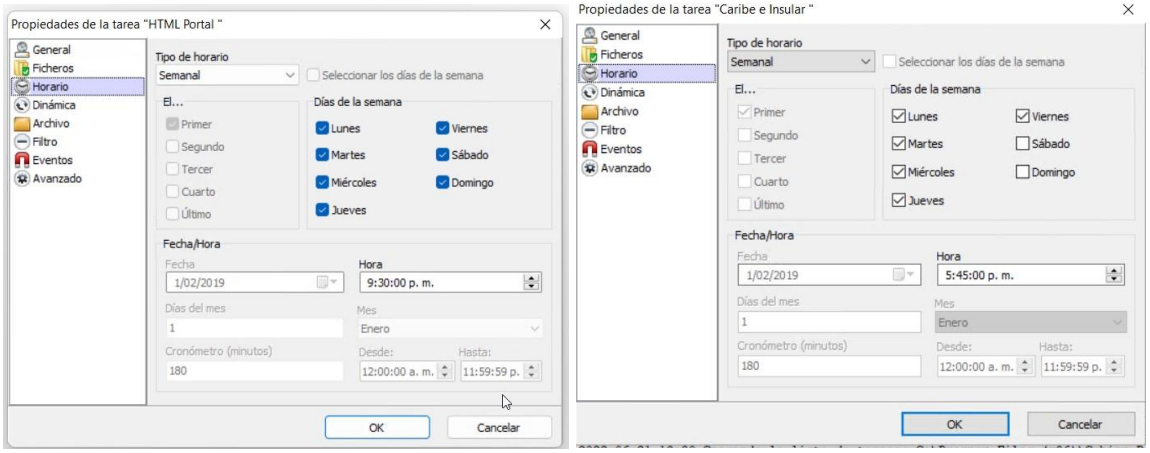


Imagen disco externo de Comunicaciones – fuente equipo de copias



Imágenes configuración de hora de la herramienta Cobiam,- Fuente COBIAN

Se evidenció que los backup del aplicativo Isolución se están realizando de lunes a viernes a las 7:00 pm

INDICADORES DE GESTIÓN

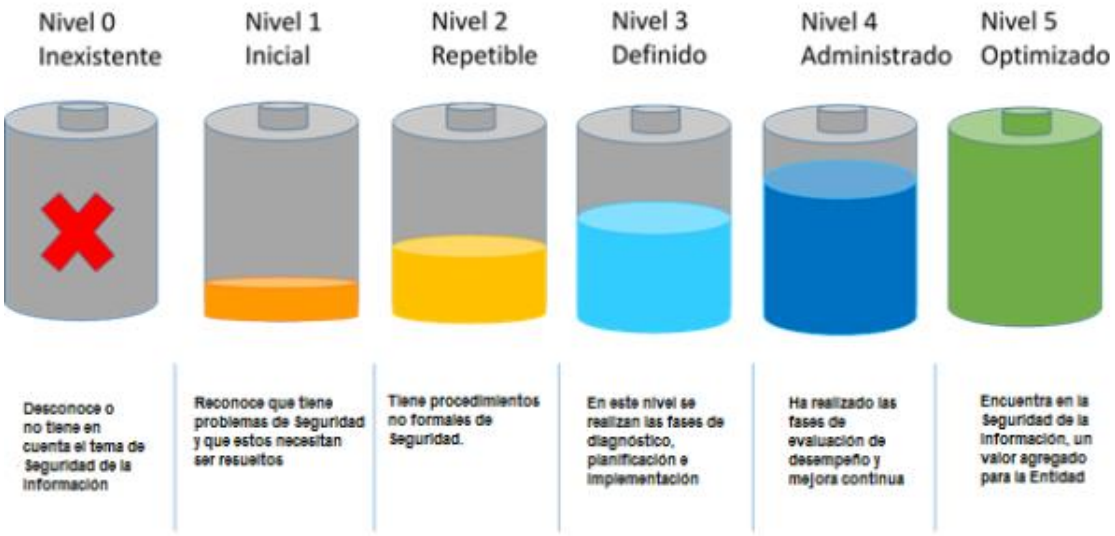
Se evidenció que el nombre de los indicadores identificados en la caracterización del proceso Gestión informática en Isolución, se encuentran desactualizados toda vez que esta muestra índice del año 2020, sin embargo, se evidencia que estos han sido reportados en el formato excel remitido a planeación. En la auditoria de la vigencia anterior se recomendó solicitar al grupo de planeación y estadística habilitar el módulo de indicadores en el aplicativo para su posterior reporte, sin embargo, para la presente vigencia aún continúa sin actualizar. Adicionalmente se evidenció que la Unidad ha tomado como acción de mejora, para solucionar los problemas generados por la plataforma Isolución, desarrollar un sistema de información propio para gestionar el sistema Integrado de gestión de organizaciones solidarias SIGOS.

CUMPLIMIENTO DE LOS REQUISITOS DEL MSPI (MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN).

Se evidenció documento en formato excel en donde se puede verificar el cumplimiento de los 14 dominios de la Norma técnica Colombiana ISO 27001:2013. En este documento se evidencian los niveles de madurez del MSPI. En la vigencia 2021 se evidenció cumplimiento del nivel 4 que hace referencia a un nivel administrado por tanto se han realizado las fases de evaluación de desempeño y mejora continua.

Se evidenció en el informe de implementación del MSPI que el nivel de madurez del sistema incluye los controles técnicos y administrativos, los procesos de gestión, las buenas prácticas de seguridad de la información, y demás procesos que intervienen en la entidad. El nivel de

madurez mide la brecha entre el nivel actual de la entidad y el nivel optimizado y de acuerdo a la calificación obtenida en cada uno de los dominios para la calificación de los controles, La Unidad Administrativa Especial de Organizaciones Solidarias se encuentra en un nivel de madurez **ADMINISTRADO,** el cual expresa que en este nivel se encuentran las entidades que cuentan con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.



Niveles de madurez Fuente Guía modelo de seguridad y privacidad

Acorde con el sistema de Gestión de Seguridad de la Información SGSI es la base para el desarrollo de la NTC ISO 27001 con respecto a la Seguridad de la Información y con la cual se pretende minimizar los riesgos de pérdida o daño en la información, datos, registros y en general de todo tipo de información o sistema informático, se adelantó la verificación de las siguientes categorías:

CATEGORÍA: BACKUPS
PROCESO: GESTIÓN INFORMÁTICA
OBJETIVO: GARANTIZAR EL RESPALDO DE INFORMACIÓN Y PROTEGER CONTRA LA PÉRDIDA DE INFORMACIÓN

Lograr garantizar una total protección de la información es una tarea imposible de cumplir, ya que los riesgos a los que se está expuesta son de diferente índole y muchos provienen de ataques informáticos o virus que son impredecibles y que se aprovechan de las falencias de los programas, firewalls y en general de todos los dispositivos informáticos. Es por esto que es de vital importancia la elaboración y

gestión de las copias de seguridad, teniendo como objetivo mantener la integridad y disponibilidad de la información.

Las copias de seguridad son parte critica para el funcionamiento de cualquier sistema de información, de acuerdo con la definición incorporada en la NTC ISO 27001. Se debe proteger la Información importante frente a cualquier situación que suponga un riesgo o amenaza. Esta información que resulta fundamental para la organización es lo que se denomina activo. Los archivos digitales que se guardan en las bases de datos de los sistemas de información, en las carpetas compartidas que tiene cada área y que usan los funcionarios de la UAEOS para el cumplimiento de sus funciones misionales debe ser protegida por su carácter teniendo en cuenta su criticidad, confidencialidad y guardando su trazabilidad.

En el desarrollo de la auditoría se pudo evidenciar que se realizan copias diarias de seguridad mediante el aplicativo COBIAN, donde se configura la tarea, el horario y los días y en que se realiza la copia de seguridad, el cual es guardado diariamente en discos duros externos cumpliendo con el literal T.4.1.1 del MSPI. Así mismo, la entidad almacena las copias de seguridad en discos propios custodiados por el Grupo Tics y se evidencia que se cuenta en el SIGOS con el procedimiento denominado "Respaldo de información de equipos de cómputo y servidores" Cumpliendo con el literal T.4.1.1 del MSPI.

Se evidenció que se aplica el formato establecido para diligenciar la información de los Backups. La funcionaria encargada de la realización de los Backups somete a consideración cada uno de los aplicativos determinando el grado de criticidad de cada uno de ellos. Se evidenció que el procedimiento “RESPALDO DE INFORMACIÓN DE EQUIPOS DE CÓMPUTO Y SERVIDORES" No determina el ciclo de vida de la información incumpliendo el literal T.4.1.1 del MSPI. Se recomienda incluir dentro del procedimiento "RESPALDO DE INFORMACIÓN DE EQUIPOS DE CÓMPUTO Y SERVIDORES" la determinación de los ciclos de vida de la información de acuerdo a la normatividad vigente.

La entidad a la fecha NO cuenta con copias de seguridad externas, debido a que no se cuenta con la disponibilidad de apropiación presupuestal incumpliendo el literal T.7.1.5 del MSPI, sin embargo, la entidad se encuentra realizando copias de seguridad en la nube que es un aplicativo que no cuenta las especificaciones técnicas requeridas que garanticen que no se presente riesgo en la perdida de la información. Por tanto se recomienda otorgar el recursos necesario y suficiente para contratar el servicio de copias de seguridad que permitan a la Unidad garantizar la continuidad del negocio en términos de información.

CATEGORÍA: BASES DE DATOS
PROCESO: GESTIÓN INFORMÁTICA
OBJETIVO: GARANTIZAR LA SEGURIDAD DE LA INFORMACIÓN EN LAS BASES DE DATOS

En términos generales, la seguridad de las bases de datos se refiere a medidas de protección para garantizar el acceso no autorizado de los datos, estos datos se pueden encontrar en archivos, programas y están almacenados en servidores, en la nube, portales web o dispositivos en los cuales se almacenan o ingresan por medio de un programa.

La entidad cuenta con medidas de seguridad de la información como Ingeniería de la seguridad de datos, Encriptación, Detección de intrusión y respuesta ante una brecha de seguridad, Firewall, Análisis de vulnerabilidades, Pruebas de intrusión, Información de seguridad y gestión de eventos, Ciberseguridad: HTTPS, SSL y TLS, y Detección de amenazas en punto final.

En el desarrollo del proceso de auditoría se evidenció que cada uno de los aplicativos guarda la información de las operaciones que realiza la base de datos. La información se encuentra dentro del mismo aplicativo en la carpeta log. Por lo anterior se cumple con el numeral 6.2.5 de la norma ISO 27001. Mediante el aplicativo COBIAN se realizan las copias de seguridad de acuerdo a las prioridades de cada uno de los aplicativos. Por lo anterior, se cumple con el numeral 6.2.6 de la norma ISO 27001. Se cuenta con formato interno sin estandarizar donde se identifica el administrador de cada sistema con su clave. Igualmente se evidenció que a este archivo solo tienen acceso las personas autorizadas. Por lo anterior se cumple con el numeral 6.2.8 de la norma ISO 27001.

El formato de gestión de perfiles de usuarios al cual se sugiere adicionar campos con el fin de complementar y especificar la información. Por lo anterior se cumple con el numeral 4.1.4 de la norma ISO 27001. Se recomienda adelantar la acción de mejora adicionando los campos requeridos y estandarizando el formato al SIGOS.

Se evidenció que se renueva por lo menos una vez al año las claves de los usuarios de las bases de datos. Por lo anterior se cumple con el numeral 1.4.3 de la norma ISO 27001. La configuración del sistema de usuarios obliga el cambio cada 3 meses de la contraseña, cumpliendo con el numeral 4.1.4 de la norma ISO 27001.

Se evidencia que en el momento la entidad no tiene archivos de carácter confidencial que requieran encriptación.

Se identificó que se ha realizado la restauración de las copias de seguridad de la información, lo cual se puede evidenciar en los informes de supervisión y en los informes de actividad de los contratistas. Cumpliendo con el numeral T4.3.1 de la norma ISO 27001. Así mismo, se sincroniza información por medio de office 365 en la nube, para la presente se garantizará las copias externas de la información de la entidad mediante acuerdo marco de precios de Colombia Compra Eficiente. Cumpliendo con el numeral T4.3.1 de la norma ISO 27001.

Se evidenció que en el momento se cuenta con equipos de escritorio para respaldo en caso de avería, sin embargo, no se cuenta con respaldo para servidores y sistemas de almacenamiento. Se recomienda asignar los recursos necesarios para contar con respaldo de servidores y sistemas de almacenamiento, con el fin de evitar inactividad de los aplicativos.

Se evidenció que las bases de datos en SQL Server y MYsql soportan herramientas de auditoría, cumpliendo el numeral T.4.5.1 del MSPI.

En el plan de continuidad del negocio se encuentra definido el plan de contingencia y se refiere al respaldo de copias de seguridad en caso de situaciones no deseadas. Cumpliendo con el numeral T6.2.3 de la norma ISO 27001.

Existen LOGS en los servidores para almacenar las transacciones realizadas en las bases de datos.

CATEGORÍA: COMPRA Y GARANTÍA DE HARDWARE
PROCESO: GESTIÓN INFORMÁTICA
OBJETIVO: EVALUAR EL PROCEDIMIENTO Y GARANTIZAR EL CORRECTO FUNCIONAMIENTO DE LOS EQUIPOS ADQUIRIDOS

Ante la enorme oferta de aparatos tecnológicos la adquisición es un proceso que requiere tener en cuenta diferentes variables importantes dependiendo del caso específico, como por ejemplo:

- ✓ PRESUPUESTO: Es necesario optimizar el producto a adquirir, utilizando el recurso económico necesario, que nos garantice un elemento de alta calidad sin costos elevados, con eficiencia comparativa con otros productos.
- ✓ NECESIDAD: Es indispensable adelantar un estudio de las necesidades que el producto a adquirir me va a solucionar, se debe tomar información de la WEB, de varios fabricantes y realizar análisis comparativos de rendimiento vs. costo, lo cual nos permite establecer una buena relación costo – beneficio.

- ✓ GARANTIA Y RESPALDO: Se debe contar con garantía y soporte post venta, esto nos proporciona la seguridad que el producto que se va a adquirir funcionará de acuerdo a lo planeado.
- ✓ ULTIMAS VERSIONES: Dependiendo de los recursos disponibles, siempre es preferible adquirir las últimas versiones del mercado, muy importante en tecnología ya que los tiempos en los cuales pasa un producto a obsolescencia cada vez son más cortos.

En la verificación se pudo evidenciar que se maneja como control de equipos en garantía, la revisión nivel uno y en caso de que el equipo afectado esté en garantía se abre caso con el proveedor para revisión del equipo, ya sea en las instalaciones de la Unidad, o en las instalaciones del proveedor, en caso dado, se solicita reposición. El supervisor del contrato custodia los documentos de garantía almacenándolos en la carpeta compartida de TICS.

Se pudo determinar que se establecen los criterios de evaluación para la adquisición de equipos, los cuales se definen en los estudios cuando se va a realizar la compra de equipos. Por su parte, el grupo de TIC´S apoyados en el contrato de mantenimiento y la mesa de ayuda diagnostican los equipos y se hacen recomendaciones de cambio o reposición. Sin embargo, se evidenció que la Unidad no cuenta con un procedimiento definido para la adquisición de equipos tecnológicos incumpliendo el literal A14 de la NTC ISO 27001. Se recomienda documental el procedimiento para la adquisición de equipos tecnológicos de conformidad con el literal A14 de la NTC ISO 27001

Todos los equipos adquiridos por la UAEOS cuentan con licencia de software desde las condiciones iniciales de adquisición en los estudios. En el contrato de mantenimiento preventivo se establece el mantenimiento para toda la infraestructura de hardware de la UAEOS

CATEGORÍA: CONTROL IMPACTO AMBIENTAL
PROCESO: GESTIÓN INFORMÁTICA
OBJETIVO: EVALUAR LOS SISTEMAS DE GESTIÓN DE DESEMPEÑO DE LOS EQUIPOS INSTALADOS EN LA ENTIDAD PARA LIMITAR EL IMPACTO DE SUS ACTIVIDADES SOBRE EL MEDIO AMBIENTE.

El control ambiental como parte fundamental en la preservación del medio de subsistencia no solo del hombre sino de la naturaleza en general, requieren de medidas de mitigación ambiental las cuales son un conjunto de acciones de prevención, control, atenuación, restauración y compensación de impactos

ambientales negativos que se dan por el desarrollo de un proyecto, con el fin de asegurar un uso sostenible de los recursos naturales y de la protección del medio ambiente.

Para minimizar los impactos ambientales, se debe realizar un adecuado manejo y disposición de los materiales obsoletos, desgastados, inservibles o dañados, los reutilizables y los residuos. Estas son medidas de prevención encaminadas a evitar los impactos, efectos y riesgos ambientales que pueden causar impactos negativos o daño a las personas o al medio ambiente.

Es necesario establecer medidas de control destinadas a enfrentar los riesgos que se identifiquen en cada una de las áreas de la organización implementando estrategias, políticas o acciones que permitan mejorar la calidad ambiental aprovechando las oportunidades existentes.

Una vez verificado los numerales se evidenció que el centro de cómputo cuenta con un sistema de ventilación, aire acondicionado de precisión y contra incendio Nova Systems, los cuales cumplen con los requerimientos para el centro de cómputo. En el marco del contrato anual de mantenimiento correctivo y preventivo se realizan como mínimo 2 mantenimientos en el año, cumpliendo con el literal T.3.1.1 del MSPI. Se cuenta con un plan de mantenimiento preventivo y correctivo, servicios tecnológicos y se encuentran publicados en la página web https://www.uaeos.gov.co/Planeaci%C3%B3n-gesti%C3%B3n-y-control/Planeaci%C3%B3n/Planes/Planes-integrados-2021/Plan-de-Mantenimiento-de-Servicios-Tecnol%C3%B3gicos cumpliendo con el literal T3.2.4

Se tienen instalados y se limpian los filtros de los aires acondicionados de precisión y de ambiente.

En el marco del contrato anual de mantenimiento correctivo y preventivo se realizan como mínimo dos (2) mantenimientos en el año a los filtros de los aires acondicionados de precisión y de ambiente, cumpliendo con el literal T 3.2.4 del MSPI. Se cuenta con un aire acondicionado principal precisión marca Stulz y como contingencia se cuenta con dos (2) aires acondicionados MINI SPLIT marca Samsung, cumpliendo con el literal T 3.1.4 del MSPI. La UAEOS en el SIGOS en el proceso de gestión administrativa se cuenta con el procedimiento denominado " baja de bienes" identificado con el código UAEOS-PR-GAD-002.

En la entidad No se cuenta con una política clara y definida para determinar la vida útil de los dispositivos informáticos a dar de baja, incumpliendo con el numeral AD.4.3.2 del MSPI. Se recomienda diseñar una guía clara y definida de la vida útil

de los dispositivos informáticos, con el fin de incluirla en el procedimiento de baja de bienes.

CATEGORÍA: GESTIÓN MESA DE AYUDA
PROCESO: GESTIÓN INFORMÁTICA
OBJETIVO: GARANTIZAR LA GESTIÓN DE ATENCIÓN A LAS SOLICITUDES ALLEGADAS, EL TIEMPO EN RESPUESTA Y LA SOLUCIÓN REALIZADA.

La gestión de mesa de ayuda es un sistema de tecnología que recibe, administra, organiza, automatiza, responde e informa acerca de los requerimientos o incidencias que se presentan en cualquier ámbito informático.

Después de que la mesa de ayuda ha sido notificada de un problema, el cual presenta cualquier usuario a través de un ticket, en el que se detalla la solicitud, la mesa de ayuda gestiona para que los agentes que dan solución realicen los procesos correspondientes en el menor tiempo posible y minimizando la posibilidad de error.

Los indicadores, variables o parámetros estadísticos que genere esta herramienta permiten realizar planeación por fallas frecuentes, obsolescencia de hardware y/o software o por malos manejos de los usuarios finales.

Con esta herramienta se puede dar solución a los requerimientos o incidencias en corto tiempo, así mismo se pueden establecer prioridades y posibles soluciones para problemas comunes, los cual redunda en la satisfacción de los usuarios finales y aumento de la productividad ya que se reducen los tiempos fuera de servicio de los dispositivos o sistemas.

En el desarrollo del proceso de auditoría se evidenció que la frecuencia de capacitación es 2 veces al año, y que por medio del plan de sensibilización se plantean consejos informáticos con el fin de implementar mejoras continuas para los usuarios. Dentro la política de seguridad de la información se establece tiempos de respuesta dependiendo de la urgencia de la solicitud y diariamente se realizan solicitudes de fallas en los servicios, fallas en los aplicativos y fallas en la infraestructura. Se evidenció que dentro del aplicativo de mesa de ayuda se genera el reporte de tiempos de atención de las solicitudes y en el plan de mantenimiento existen dos jornadas de mantenimiento correctivo y preventivo. Se evidencia que dentro del SIGOS se encuentra el procedimiento documentado y aprobado de mesa de ayuda dentro del proceso de Gestión Informática y dentro del contrato de gobierno digital se tiene la actividad de actualización del inventario de activos.

Se tiene el procedimiento “IMPLEMENTACIÓN DE REQUERIMIENTOS A LOS SISTEMAS DE INFORMACIÓN” donde se reciben o se idéntica los requerimientos de actualizaciones y mejoras a los aplicativos de la entidad

CATEGORÍA: POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
PROCESO: GESTIÓN INFORMÁTICA
OBJETIVO: EVALUAR EL PROCEDIMIENTO Y GARANTIZAR EL CORRECTO FUNCIONAMIENTO DE LOS EQUIPOS

Contiene los procedimientos, prácticas y estructuras organizativas que, alineadas con la misionalidad de la Entidad, permiten minimizar los riesgos en la seguridad y privacidad de la información, garantizando la disponibilidad, integridad y confidencialidad de la información.

Dentro de la privacidad se entiende también la confidencialidad, la cual se refiere a que los datos personales no pueden divulgarse sin consentimiento expreso del titular, el carácter de información confidencial es permanente, no está limitado o condicionado a un plazo o termino fijo.

La privacidad es el derecho de los usuarios a proteger sus datos en la red y a decidir qué información puede ser visible para los demás, por lo tanto, una persona está en su derecho de evitar que otros accedan a sus datos personales sin su consentimiento

En el desarrollo del proceso de auditoría se evidenció que la política de Seguridad y privacidad de la información se actualizó y aprobó en esta vigencia. Dentro de las revisiones de equipos se revisa cumplimiento a la política de seguridad de la información como también dentro del plan de sensibilización y el contrato de Gobierno digital se encuentran las actividades de evaluación del conocimiento de la política.

CATEGORÍA: REDES Y COMUNICACIONES
PROCESO: GESTIÓN INFORMÁTICA
OBJETIVO: CONOCER Y EVALUAR LOS MECANISMOS DE PROTECCIÓN DEL HARDWARE Y CABLEADO Y LAS MEDIDAS DE PROTECCIÓN SOBRE LA INFORMACIÓN

La infraestructura de redes y comunicaciones son todos aquellos elementos básicos e imprescindibles para el funcionamiento adecuado de cualquier sistema. Esta

infraestructura está en cambio constante, debido a la implementación de nuevos dispositivos, obsolescencia de lo que se tienen, creación de nuevas reglas de seguridad etc.

El desarrollo de la infraestructura de TIC, las tecnologías digitales y la convergencia de la radiodifusión, las telecomunicaciones y la informática, ofrecen considerables oportunidades para la implementación de las nuevas tecnologías.

Cada cambio implementado significa mayor complejidad de la red, por ello también es necesario simplificar y estandarizar los cambios con el fin de evitar que la complejidad de la red la vuelva de difícil manejo, hay que saber aprovechar al máximo la infraestructura ya desplegada e implementar las soluciones adecuadas en cada caso.

Para optimizar el funcionamiento de la red y las comunicaciones es muy importante tener en cuenta:

- Sanear y optimizar el cableado, y eliminar switches intermedios, con lo que se conseguiría reducir los costos generales de instalación, mantenimiento y aumentar la velocidad de la red.
- Utilizar dispositivos de red gestionados que permitan aumentar el rendimiento y funcionalidad de la red, así como el diagnóstico avanzado.
- Aumentar el rendimiento y la fiabilidad de la infraestructura de redes y comunicaciones. Con dispositivos gestionados que ofrezcan flexibilidad para aplicar el control de forma centralizada o distribuida.
- Realizar un buen trabajo de segmentación de red con las políticas de seguridad adecuadas, separando roles de usuarios y tipos de máquinas.

En el desarrollo de la auditoría se pudo evidenciar que la infraestructura de la red inalámbrica es gestionada de acuerdo a las necesidades de los usuarios, para lo cual se estableció VLAN diferente para este tipo de accesos, cumpliendo con el numeral T1.1.2 de la norma ISO 27001. Dentro del contrato de mantenimiento preventivo de infraestructura tecnológica se realizan testeos de red evaluando su correcto funcionamiento y se tienen colores definidos para el cableado de voz, datos y cámaras. También se cuenta con dispositivo SOPHOS, el cual brinda la protección perimetral y defensa de la red de la entidad. Cumpliendo con el numeral T1.1.2 de la norma ISO 27001.

La entidad cuenta con un polo a tierra ubicado en el sótano, el cual brinda la protección de los equipos en posibles descargas eléctricas, cumpliendo con el numeral T1.1.2 de la norma ISO 27001. Se evidencia que se cuenta con 2 UPS de

20 KVA, las cuales nos brindan la regulación de voltaje en toda la entidad, cumpliendo con los numerales T1.1.2 y T3.1.4 de la norma ISO 27001.

Se cuenta con sistema de aire acondicionado de precisión el cual garantiza la temperatura idónea para el funcionamiento de los equipos del centro de cómputo, cumpliendo con los numerales T1.1.2 y T3.1.4 de la norma ISO 27001.

Dentro del Firewall Sophos se configuran y actualizan las políticas de protección que brindan seguridad ante un ataque externo de hackers, dentro del plan de continuidad del negocio establecen las contingencias que garanticen buen funcionamiento de la red, cumpliendo con el numeral T1.1.2 de la norma ISO 27001.

Se evidenció que no se cuenta con los suficientes nodos para conexión en la red, ya que se han realizado ampliaciones en los puestos de trabajo por medio de switchs. Se recomienda la correspondiente ampliación de la red cableada de la entidad.

Por medio del certificado de seguridad HTTPS de la entidad se garantiza el cifrado de datos.

Se evidencia que en la configuración de la red se establecieron VLAN´s para los diferentes tipos de equipo y acceso. Se cuenta con el firewall Sophos, el cual permite la creación de usuarios remotos estableciendo VPN seguras.

CATEGORÍA: SEGURIDAD LOGICA E INFORMÁTICA
PROCESO: GESTIÓN INFORMÁTICA
OBJETIVO: MANTENER LA INTEGRIDAD, DISPONIBILIDAD, PRIVACIDAD, CONTROL Y AUTENTICACIÓN DE LA INFORMACIÓN

La seguridad lógica se refiere a la manera de aplicar procedimientos para asegurar el acceso a los datos o sistemas solo de las personas autorizadas dependiendo de los roles que cumplan dentro de la organización.

Es el conjunto de medidas destinadas a la protección de los datos y aplicaciones informáticas, garantizando accesos por roles, permisos o funciones.

El licenciamiento del software, la instalación de software de seguridad como antivirus y dispositivos de protección perimetral como los firewalls son elementos básicos que brindan seguridad lógica y minimizan los daños que se pueda ocasionar a la información por hackers, virus, etc.

La implementación de roles, logs de transacciones, claves de acceso, seguridad perimetral y sistemas de video vigilancia, permiten optimizar la seguridad y garantizar en un alto porcentaje la disponibilidad y mantener la privacidad de la información.

En el desarrollo del proceso auditor se evidenció que se utilizan las siguientes metodologías: Discos duros externos, sistemas de almacenamiento, copias de respaldo en la nube y utilización del Software de backup Cobian, adicionalmente existe un administrador por el COBIAN y por el controlador de Dominio. Por políticas del controlador de dominio y Buenas Prácticas se establece la contraseña con los parámetros estándar (mínimo 8 caracteres, que sea alfanumérica, tener un caracter especial y por lo menos utilizar una mayúscula y una minúscula. Así mismo, por el controlador de dominio para los usuarios y por la licencia de office 365 para los correos, se tiene establecido el cambio periódico de contraseña. En esta vigencia se elaboró documento del proceso de mantenimiento preventivo y correctivo donde falta ser aprobado por el comité institucional. Todos los equipos de cómputo de la entidad cuentan con Software de antivirus instalados y actualizados. El software de antivirus tiene implementado la detección de malware y se encuentra totalmente licenciado.

Dentro de la compra de las licencias de software se adquieren las actualizaciones automáticas para la vigencia, dentro del plan de adquisiciones se determina las necesidades de licenciamiento para la vigencia, programando de esta manera la compra. Así mismo, dentro del contrato de mantenimiento preventivo y correctivo se establece la revisión periódica del software no licenciado en cada uno de los equipos, se realiza el mantenimiento preventivo periódico de los computadores y también cuando se realizan servicios de mesa de ayuda se realiza la revisión de software no licenciado.

La memoria RAM de los computadores se ajusta a las necesidades de cada funcionario. Se evidencia que el procesador de los computadores se ajusta a las necesidades de cada funcionario.

AUDITORÍA AL CUMPLIMIENTO DE LA NORMA NTC 5854:2011 ACCESIBILIDAD A PÁGINAS WEB

La oficina de control interno verificó el cumplimiento de los numerales 3 (requisitos de nivel de conformidad) y 4 (conformidad) de la norma técnica Colombiana NTC 5854 de 2011, de lo cual identificó que la unidad viene implementando los requisitos de nivel de conformidad y conformidad de la NTC 5854:2011 por medio de la implementación de los requisitos de accesibilidad de las pautas WCGA2.0. Se evidenció que la unidad realizó una autoevaluación de su nivel de accesibilidad con respecto a dichas pautas, lo cual daría como

resultado un nivel de accesibilidad AA, que implica que la página web de la unidad en las características de perceptible, operable, comprensible y robusto cumple con la calificación mínima requerida en el FURAG.

Lo anterior se puede evidenciar en el documento publicado en la página web de la unidad en el siguiente link: https://www.uaeos.gov.co/sites/default/files/archivos/Informe%20accesibilidad%20p%C3%A1gina%20web_0.pdf

Se evidenció que el grupo de TI cuenta con una OPS mediante la cual se adelantan las actividades de actualización y desarrollo de la página web a sede electrónica de acuerdo a los lineamientos establecidos por MINTICS en el decreto 2106 de 2019.

CONTROLES DE SEGURIDAD, ACCESO Y GESTIÓN EN LA ADMINISTRACIÓN DE USUARIOS DE LOS SISTEMAS DE INFORMACIÓN QUE UTILIZA LA UNIDAD.

Los usuarios son administrados por el controlador de dominio, el cual restringe por nombre de usuario y clave el ingreso a la red y por políticas de seguridad el acceso a la información. Los controles de seguridad están basados en el control de acceso por grupos de trabajo el cual cada uno de ellos tiene su información de manera independiente. Los parámetros de acceso se encuentran administrados por el rol de Windows Server denominado Active Directory, con el cual se crean los usuarios, se asignan password iniciales, y se da permiso de acceso a la información.

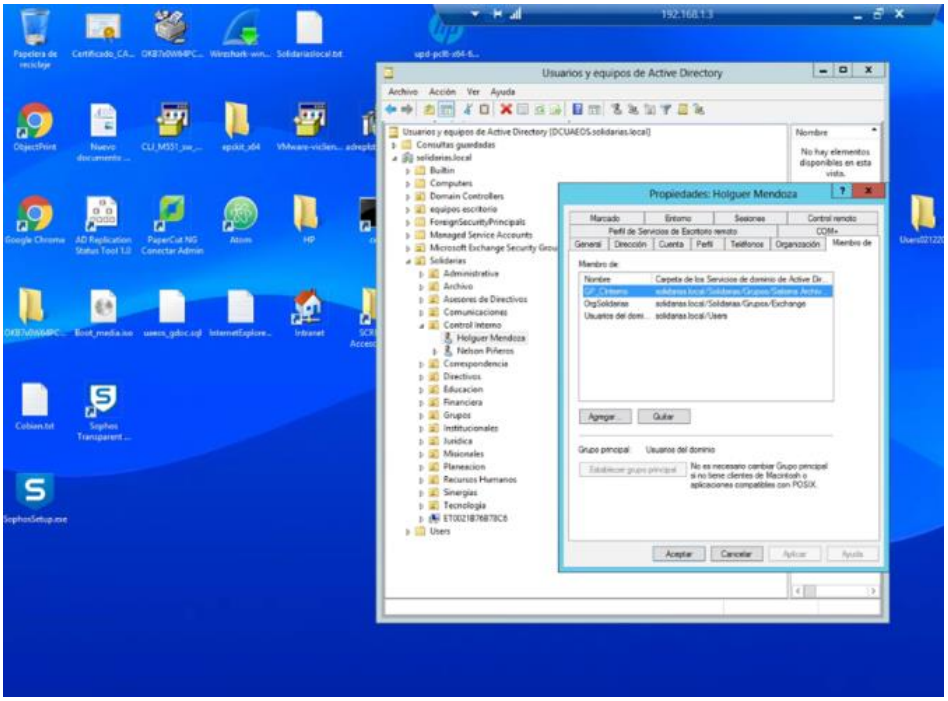


Imagen configuración de usuario en controladora de dominio

CUMPLIMIENTO ACTIVIDADES DE PRÉSTAMO Y RETIRO DE EQUIPOS TECNOLÓGICOS

A partir del inicio de la declaratoria de emergencia sanitaria por COVID19 en la vigencia 2020 y la vigencia 2021 no se ha adelantado el préstamo de equipos mediante formato estándar "**PRÉSTAMO DE EQUIPO O ELEMENTOS TECNOLÓGICOS**" Código No. UAEOS-GIN-FO-06. Sin embargo, a partir de esta fecha se continua con el préstamo de equipos mediante el formato denominado "**ACTA DE ENTREGA EQUIPO TECNOLÓGICO**" código UAEOS-GIN-FO-07 el cual ha sido utilizado para otorgar los equipos que fueron requeridos para apoyar las actividades de los funcionarios que actualmente desarrollan la modalidad de trabajo en casa o para realizar el cambio de equipos que se requirieron. A la fecha se cuenta con 27 equipos asignados para trabajo en casa.

Ley 1712 de 2014 ley de transparencia y acceso a la información pública y Resolución 1519 de 2020 del Ministerio de la información y las comunicaciones

Dentro del proceso auditor se observó que la estructura del botón de transparencia está conforme a la resolución 1519 de 2020, la cual se presenta en el siguiente cuadro:

CATEGORÍA	SUBCATEGORÍA
1. Información de la entidad	1.1 Misión, visión, funciones y deberes
	1.2 Estructura orgánica - Organigrama
	1.3 Mapas y Cartas descriptivas de los procesos
	1.4 Directorio Institucional incluyendo sedes, oficinas, sucursales, o regionales y dependencias.
	1.5 Directorio de servidores públicos, empleados o contratistas.
	1.6 Directorio de entidades
	1.7 Directorio de agremiaciones o asociaciones en las que participe.
	1.8 Servicio al público, normas, formularios y protocolos de atención
	1.9 Procedimientos que se siguen para tomar decisiones en las diferentes áreas.
	1.10 Mecanismo de prestación directa de solicitudes, quejas y reclamos a disposición del público en relación con acciones u omisiones del sujeto obligado.
	1.11 Calendario de actividades y eventos
	1.12 Información sobre decisiones que puede afectar al público
	1.13 Entes y autoridades que lo vigilan
	1.14 Publicación de hojas de vida
2. Normativa	2.1 Normativa de la entidad
	2.1.1 Leyes
	2.1.2 Decreto Único Reglamentario
	2.1.3 Normativa aplicable
	2.1.4 Vinculo al diario o gaceta oficial
	2.1.5 Políticas, lineamientos y manuales
	2.1.6 Agenda Regulatoria
	2.2 Búsqueda de normas
	2.2.1 Sistema único de Información Normativa - SUIN
	2.2.2 Sistema de búsquedas de normas, propio de la entidad
	2.3 Proyectos de normas para comentarios
	2.3.1 Proyectos normativos
	2.3.2 Comentarios y documento de respuesta a comentarios
	2.3.3 Participación ciudadana en la expedición de normas a través del SUCOP
3. Contratación	3.1 Plan Anual de Adquisiciones
	3.2 Publicación de la información contractual
	3.3 Publicación de la ejecución de los contratos
	3.4 Manual de contratación, adquisición y/o compras
	3.5 Formatos o modelos de contratos o pliegos tipo

4. Planeación, presupuesto e informes	4.1 Presupuesto general de ingresos, gastos e inversión
	4.2 Ejecución presupuestal
	4.3 Plan de Acción
	4.4 Proyectos de Inversión
	4.5 Informes de empalme
	4.6 Información pública y/o relevante
	4.7 Informes de gestión, evaluación y auditoría
	* Informe de rendición de cuentas a la ciudadanía
	* Informes a organismos de inspección, vigilancia y control
	* Planes de mejoramiento
	4.8 Informes de la oficina de control interno
	* Informe pormenorizado
	* Otros informes y/o consultas a bases de datos o sistemas de información conforme aplique
	4.9 Informe sobre defensa pública y prevención del daño antijurídico
	4.10 Informes trimestrales sobre acceso a la información, quejas y reclamos
5. Trámites	5.1 Trámites (normativa, proceso, costos y formatos o formularios)
6. Participa	Mecanismo o procedimiento mediante el cual el público pueda participar en el ejercicio de facultades de la entidad
	Información que le corresponda conforme a los lineamientos del DAFP
7. Datos Abiertos	7.1 Instrumentos de gestión de la información (registro de activos de información, índice de información clasificada o reservada, esquema de publicación de la información, programa de gestión documental, tablas de retención documental.) Acto administrativo sobre costos de reproducción.
	7.2 Sección de datos abiertos
8. Información específica para Grupos de interés	Identificar la información específica para grupos de interés conforme su caracterización. Información para niños, niñas y adolescentes Información para Mujeres
9. Información relevante de la entidad	La entidad debe publicar la información, datos, reportes que esté obligado por normativa

A la fecha el botón de Transparencia presenta la siguiente estructura:

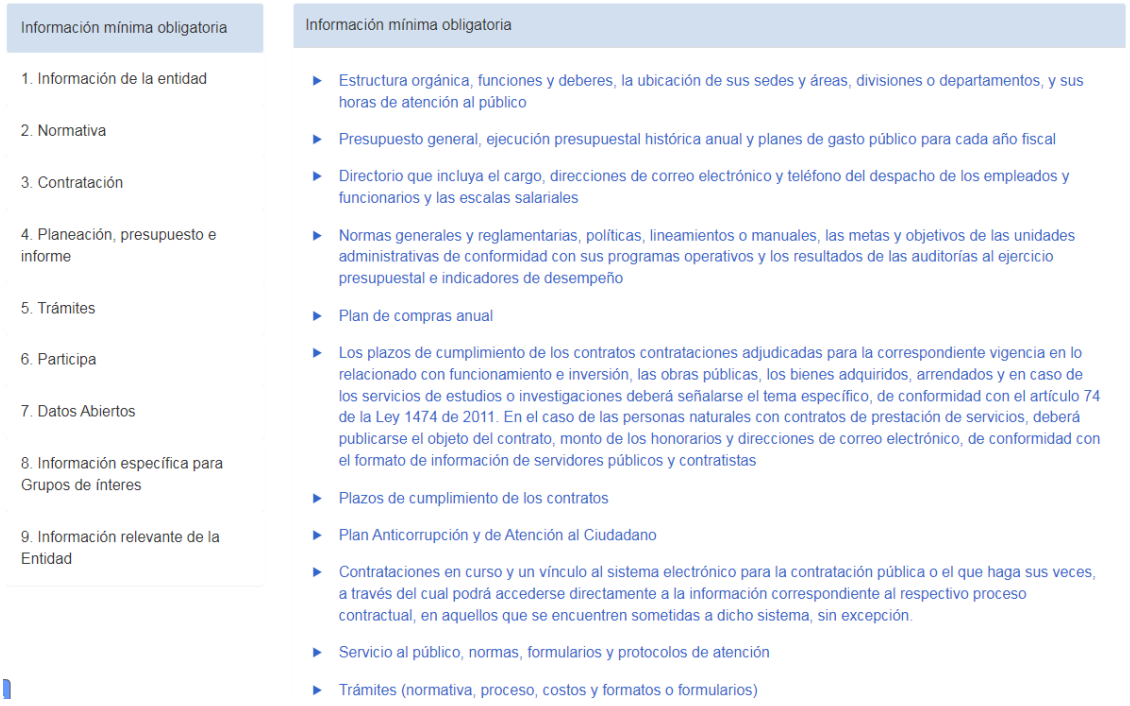


Imagen estructura menú de transparencia en página web UAEOS

Se evidenció que en la vigencia 2022 la estructura del menú de transparencia cumple con los requisitos mínimos establecidos a los lineamientos de sede electrónica definidos en el Decreto 2106 de 2019. A la fecha la UAEOS cuenta con Sede Electrónica mediante el cual se puede interactuar con la ciudadanía promoviendo la participación ciudadana.

PROYECTO DE INVERSIÓN

FORTALECIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIDAD ADMINISTRATIVA ESPECIAL ORGANIZACIONES SOLIDARIAS A NIVEL NACIONAL

Se evidenció con los pagos a la fecha que del total de la apropiación se ha ejecutado un 4.71%, correspondientes a OPS de ingenieros y desarrolladores por valor de $19.800.000. Así mismo, se evidenció que a la fecha se cuenta con prepliegos aprobado por comité de contratación para la contratación del servicios de mantenimiento preventivo y correctivo de hardware y software de la infraestructura tecnológica de la entidad por un valor de $149.361.958. También se evidenció la publicación de prepliegos dentro del cual está contemplado la sustitución y renovación de hardware en obsolescencia por valor de $84.015.721, y a la fecha se encuentra en espera de las respuestas a las observaciones. Esto con corte a 30 de abril de 2022.

SEGUIMIENTO A RECOMENDACIONES ANTERIORES

HALLAZGOS VIGENCIA 2021	SEGUIMIENTO OCI
Para la vigencia 2021 no se tiene disponibilidad presupuestal para la contratación de copias de seguridad externas, lo cual afecta la implementación de los controles de seguridad de la información de la Unidad. Actualmente, se están realizando copias de seguridad en la Nube. Se recomienda asignar los recursos necesarios para la contratación de las copias de seguridad externas y permitan mantener las medidas de seguridad de la información.	Para la vigencia 2022 se tiene asignado un rubro por valor de $30.955.881 para las copias de seguridad. A la fecha se está proyectando estudios previos.
Se evidenció que la redacción de los riesgos, así como de los controles, no se encuentran ajustados de conformidad con la política de administración de riesgos versión 2 del 25 de febrero de 2021 y su correspondiente metodología de identificación, valoración y control. Se recomienda solicitar acompañamiento al funcionario Jorge Muñoz, Profesional especializado del grupo de planeación y realizar análisis y ajuste de los riesgos y controles del proceso.	Se evidenció la actualización de la redacción de mapas de riesgos de acuerdo a la normatividad vigente. Tambien se encuentran en actualización los riesgos de seguridad digital que no se encontraban contemplados en la mapa de riesgos de la vigencia 2021.
Se evidenció que debido a los frecuentes sobrevoltajes de energía eléctrica la tarjeta de red de la planta telefónica sufrió daño en sus componentes electrónicos, para lo cual fue necesario enviarlo a reparación, reinstalándose y quedando en funcionamiento. Igualmente, se evidenció que una de las UPS no estaba cumpliendo su función cuando se producían cortes de energía, por lo cual fue necesario reubicar el suministro de energía en otra UPS, a la fecha se encuentra en funcionamiento y se está en el proceso de adquisición para el reemplazo de la UPS dañada. Se evidencia que el riesgo “Interrupción de los servicios	Se evidenció actualización del riesgo mencionado ajustándolo a nueva política de administración de riesgos versión 2 del 25 de febrero de 2021.

Tecnológicos" se materializó aun con los controles existentes. Se recomienda revisar controles y actividades de control con el fin de mitigar la materialización de este riesgo en vigencias futuras.	
Se evidenció que el botón de transparencia y acceso a la información pública de la página web de la unidad no guarda la estructura establecida en la resolución 1519 de 2020, por la cual se recomienda ajustar el link de transparencia y acceso a la información.	Se evidenció la actualización del link de transparencia y acceso a la información de la página web de la unidad de conformidad con la resolución 1519 de 2020 del Min Tic 
Se evidenció que los indicadores de gestión identificados en la caracterización del proceso de Gestión Informática miden la gestión de la vigencia 2020, por lo cual se encuentran desactualizados. Se recomienda que los indicadores de gestión sean actualizados y diligenciados, con fin de realizar trazabilidad a los indicadores y al mismo tiempo permitan a la alta dirección la toma de decisiones de manera oportuna.	Se evidenció medición y reporte de los indicadores de gestión del proceso. A la fecha la entidad no es propietaria de los códigos fuentes del aplicativo isolución, el cual no permite ajustarlo a los cambios normativos que impiden que este cumpla con su función. Por tal razón, la unidad se encuentra desarrollando su propio aplicativo, programado para la vigencia 2022 el desarrollo de tres de sus módulos incluyendo parametrización y estructura lógica del sistema.
Se evidenció que el grupo de TI cuenta con una OPS mediante la cual se adelantan las actividades de actualización y desarrollo de la página web a sede electrónica de acuerdo a los lineamientos establecidos por MINTICS en el decreto 2106 de 2019, sin embargo la carga operativa del profesional contratado no permite que se dedique el tiempo necesario para el desarrollo de la actualización, por tanto se recomienda asignar los recursos requeridos para el cumplimiento de lo exigido por el decreto 2106 de 2019.	Se evidenció que la carga operativa del profesional a cargo de la actualización y desarrollo de la página web a sede electrónica se compensó asignando recursos de talento humano que permitió apoyar las actividades de la página web de la unidad, convirtiéndola en sede electrónica.
Se evidenció que la Procuraduría General de la Nación - PGN a través del índice de transparencia y acceso a información pública ITA, evaluó el nivel de cumplimiento de la publicación de la información en la página web de conformidad con la ley 1712 de 2014, para lo cual la unidad obtuvo como resultado un cumplimiento del 97%, quedando pendiente el ítem referente a: "Publicación de la ejecución de contratos a. Aprobaciones, autorizaciones, requerimientos o informes del supervisor o del interventor, que prueben la ejecución de los contratos". Por lo tanto se solicita requerir a la Oficina Asesora Jurídica, dar lineamiento a los supervisores de contratos y convenios para que remitan los correspondientes informes de supervisión para la publicación en la página web.	En articulación con la oficina asesora jurídica, se vienen desarrollando campañas para la actualización permanente del ítem "PUBLICACIÓN DE LA EJECUCIÓN DE CONTRATOS".

CONCLUSIONES Y RECOMENDACIONES DE MEJORAMIENTO POR PARTE DE LA OFICINA DE CONTROL INTERNO

- La Oficina de control interno obtuvo evidencia razonable del cumplimiento del objetivo de proceso referente a "estrategias, planes y procedimientos definidos por el proceso, en pro de garantizar la disponibilidad y confiabilidad de los servicios y productos TIC, así como las actividades adelantadas para asegurar la infraestructura tecnológica, en el marco de la normatividad vigente garantizando la seguridad de los activos de información de cada uno de los procesos de la Unidad Administrativa Especial de Organizaciones Solidarias."

- Se materializó el riesgo con el aplicativo NOVASOFT el cual entró en conflicto al generar la liquidación del retroactivo y el mes de mayo, por lo cual fue necesario regenerar la nómina en Excel y concertar mesa de trabajo con Novasoft para el soporte técnico, cargue de la información y revisión de ajustes, de lo cual se evidenció que actualmente la Unidad no cuenta con contrato de actualización y soporte técnico. Dicha materialización no se vio reflejada en mapa de riesgos de Gestión Informática. Se recomienda identificar, valorar y dar tratamiento a los riesgos que se generen con las aplicaciones ya sea de desarrollo interno o externo de la Unidad.

- Se evidenció el reporte mensual del plan de tratamiento de riesgos de seguridad digital para los meses de marzo y abril, por tanto se evidenció que la actividad del reporte se está realizando mensualmente desde el mes de marzo, se recomienda solicitar ajuste de la meta de 3 reportes a 10 reportes de Seguimiento al plan de tratamiento de Riesgos de seguridad Digital para la presente vigencia. 2 de 10

- Se evidenció que el procedimiento “RESPALDO DE INFORMACIÓN DE EQUIPOS DE CÓMPUTO Y SERVIDORES" No determina el ciclo de vida de la información incumpliendo el literal T.4.1.1 del MSPI. Se recomienda incluir dentro del procedimiento "RESPALDO DE INFORMACIÓN DE EQUIPOS DE CÓMPUTO Y SERVIDORES" la determinación de los ciclos de vida de la información de acuerdo a la normatividad vigente

- La entidad a la fecha no cuenta con copias de seguridad externas, debido a que no se cuenta con la disponibilidad de apropiación presupuestal incumpliendo el literal T.7.1.5 del MSPI, sin embargo, la entidad se encuentra realizando copias de seguridad en la nube que es un aplicativo que no cuenta las especificaciones técnicas requeridas que garanticen que no se presente riesgo en la perdida de la información. Por tanto se recomienda otorgar el recursos necesario y suficiente para contratar el servicio de copias de seguridad que permitan a la Unidad garantizar la continuidad del negocio en términos de información.

- El formato de gestión de perfiles de usuarios al cual se sugiere adicionar campos con el fin de complementar y especificar la información. Por lo anterior se cumple con el numeral 4.1.4 de la norma ISO 27001. Se recomienda adelantar la acción de mejora adicionando los campos requeridos y estandarizando el formato al SIGOS.

- Se evidenció que en el momento se cuenta con equipos de escritorio para respaldo en caso de avería, sin embargo, no se cuenta con respaldo para servidores y sistemas de almacenamiento. Se recomienda asignar los recursos necesarios para contar con respaldo de servidores y sistemas de almacenamiento, con el fin de evitar inactividad de los aplicativos.

- Se pudo determinar que se establecen los criterios de evaluación para la adquisición de equipos, los cuales se definen en los estudios cuando se va a realizar la compra de equipos. Por su parte, el grupo de TIC´S apoyados en el contrato de mantenimiento y la mesa de ayuda diagnostican los equipos y se hacen recomendaciones de cambio o reposición. Sin embargo, se evidenció que la Unidad no cuenta con un procedimiento definido para la adquisición de equipos tecnológicos incumpliendo el literal A14 de la NTC ISO 27001. Se recomienda documental el procedimiento para la adquisición de equipos tecnológicos de conformidad con el literal A14 de la NTC ISO 27001

- En la entidad No se cuenta con una política clara y definida para determinar la vida útil de los dispositivos informáticos a dar de baja, incumpliendo con el numeral AD.4.3.2 del MSPI. Se recomienda diseñar una guía clara y definida de la vida útil de los dispositivos informáticos, con el fin de incluirla en el procedimiento de baja de bienes.

- Se evidenció que no se cuenta con los suficientes nodos para conexión en la red, ya que se han realizado ampliaciones en los puestos de trabajo por medio de switchs. Se recomienda la correspondiente ampliación de la red cableada de la entidad.
-

Cordialmente

Nelson Enrique Piñeros Moreno
Jefe de control interno

Proyectó: Holger Alberto Mendoza