	DEPARTAMENTO DE RISARALDA **Despacho del Gobernador** **EVALUACIÓN INDEPENDIENTE** **INFORME DE AUDITORÍA INTERNA**
Versión: **5**	Vigencia: **07-2021**

AUDITORIA INTERNA: Auditoría Interna Evaluación y Seguimiento al proceso de Gestión Informática Y Servicios Tecnológicos.	**FECHA ELABORACIÓN:** AGOSTO-SEPTIEMBRE 2022
DIRECTIVO RESPONSABLE: María Nancy Escobar Morales **AUDITOR(ES):** Sandra Milena Villa Motato	**DESTINATARIO** Proceso de Gestión Informática Y Servicios Tecnológicos.

ASPECTOS GENERALES

OBJETIVO(S):

Examinar la adecuada y eficaz aplicación y cumplimiento del proceso de **Gestión Informática Y Servicios Tecnológicos**, permitiendo adoptar las acciones correctivas pertinentes que surjan y que generen valor agregado y mejorar las operaciones de la Administración Departamental, y contribuir al cumplimiento de los objetivos y metas institucionales.

ALCANCE:

Verificar el cumplimiento del proceso de **Gestión Informática Y Servicios Tecnológicos** durante la vigencia junio 2021 a junio 2022, de acuerdo con las políticas y procedimientos establecidos por la entidad para la elaboración oportuna y aplicación del marco normativo en las diferentes etapas que tengan relación con este proceso.

CRITERIOS:

- Manual de la Política de Gobierno Digital. implementación de la política de Gobierno Digital – MinTIC.
- Resolución número 00500 de marzo 10 de 2021 Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
- Resolución número 00746 de marzo 11 de 2022 Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución número 500 de 2021.
- Ley 1915 de 2018 Por la cual se modifica la ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- Ley 1712 2014 Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

- Ley 1581 2012 Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1955 del 2019 Establece que las entidades del orden nacional deberán incluir en su plan de acción el componente de transformación digital, siguiendo los estándares que para tal efecto defina el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).
- Circular 7 de 2005 Departamento Administrativo de la Función Pública.
- Norma Técnica Colombiana ISO/IEC 27001 es una norma colombiana que hace posible que las organizaciones aseguren la confidencialidad y al mismo tiempo la integridad de toda la información que tengan.
- RESOLUCIÓN NÚMERO 01126 DE 2021 "Por la cual se modifica la Resolución 2710 de 2017" "Artículo 3. Plazo de adopción. Las entidades estatales del orden nacional que trata el artículo segundo de la presente resolución deberán culminar el proceso de transición al protocolo IPv6 en convivencia con el protocolo IPv4 a más tardar el 30 de junio de 2022. Por su parte, las entidades territoriales deberán finalizar dicho proceso a más tardar el 31 de diciembre del año 2022. En todo caso, dicha adopción deberá ser acorde al plan de diagnóstico formulado por cada entidad.
- Políticas, planes, procedimientos de Operación del proceso Gestión Informática Y Servicios Tecnológicos.

METODOLOGIA*:*

- ✓ Técnica de verificación oral o verbal. (Indagación, entrevistas)
- ✓ Técnica de verificación escrita. (Análisis tabulación, confirmación, certificación,)
- ✓ Técnica de verificación documental. (Comprobación, rastreo)

.

DESARROLLO DE LA AUDITORIA

De conformidad con el plan de auditorías establecido para el año 2022 por la Oficina Asesora de Control Interno, se procedió con la Auditoría Interna Evaluación y Seguimiento al proceso de Gestión Informática y Servicios Tecnológicos, se realizaron las respectivas visitas y entrevistas a la Dirección de Informática y Sistemas, con el fin de verificar el cumplimiento de las normas y procedimientos establecidos en materia de las políticas y procedimientos establecidos por, la entidad, la ley y sus decretos en las diferentes etapas que tengan relación con el proceso de Gestión Informática y Servicios Tecnológicos de la Administración Departamental.

Teniendo en cuenta lo anterior se procedió con la revisión de:

1. **Desarrollo de las Políticas de Operación planes y procedimientos.**
2. **Licenciamiento de Software**
3. **Riesgos de gestión.**

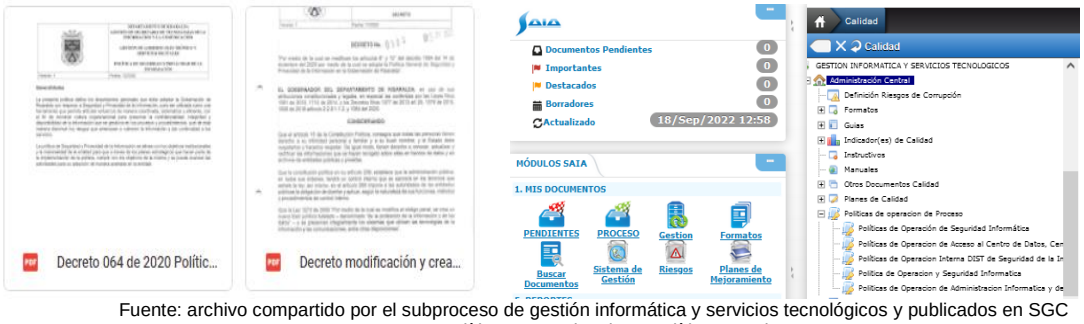
1. Desarrollo de las Políticas de Operación planes y procedimientos.

Teniendo en cuenta los lineamientos dados por el Ministerio de las Tecnologías de la Información y Comunicaciones, enmarcado dentro de la Política de Gobierno Digital y en concordancia por lo dispuesto en la norma Técnica de Colombia ISO 27001/2013 y las Políticas de Operación, establecidas por la Administración Departamental; se efectuó la evaluación respectiva, de los aspectos que se describen. La Administración Departamental a través del proceso Gestión Informática y Servicios Tecnológicos, liderado por la Dirección de Informática y Sistemas, tiene establecidas cinco (5) políticas de operación, dentro de lo que se realizó el desarrollo de la auditoria.

- Políticas de Operación Interna DIST de Seguridad de la Información
- Políticas de Operación de Seguridad Informática
- Políticas de Operación de Acceso al Centro de Datos, Centro de Cableado y Rack de Comunicaciones
- Políticas de Operación de Administración Informática y de Sistemas de Información.
- Políticas de operación de Gestión de Tecnologías de la Información

1.1. Políticas de Operación interna DIST de seguridad de la información.

Se evidenció que el proceso de Gestión Informática y Servicios Tecnológicos tiene definidas las políticas de operación y la política de seguridad y privacidad de la información la cual esta mediante decreto 1064 del 14 de diciembre de 2020, se pudo identificar que para la fecha de la auditoria se contaba con actualización, pero por no corresponder su publicación a la fecha del alcance de la auditoria no se relaciona dentro del desarrollo.



Fuente: archivo compartido por el subproceso de gestión informática y servicios tecnológicos y publicados en SGC
Imagen 1 Políticas operacionales y políticas por decretos

En cuanto a la comunicación y socialización de las políticas, se aportó por parte del proceso de gestión informática y servicios tecnológicos registro de capacitaciones y socializaciones por medio de correos memorando como de visitas a los municipios de Balbo, La Celia, Quinchía y Santa Rosa de Cabal

Fuente: archivo compartido por el subproceso de gestión informática y servicios tecnológicos
Imagen 2 capacitaciones y socializaciones

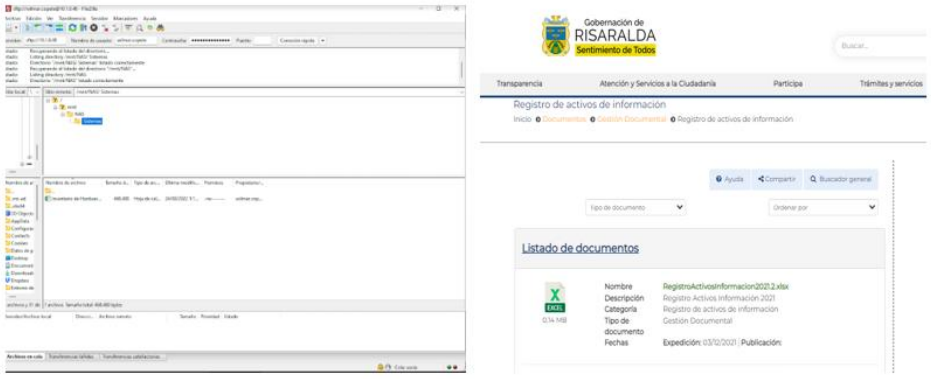
Teniendo en cuenta que la norma 27001/2013 indica que *"Las políticas de la Seguridad de la información deben adaptarse continuamente a las necesidades y cambios de la organización por lo que no pueden permanecer estáticas."*

se evidenció la revisión, y la actualización de las Políticas de seguridad de la información por parte de los responsables del proceso de Gestión Informática y Servicios Tecnológicos en el perdido auditado, pero existen actividades que al momento de la auditoria no se realizan como es el caso de la solicitud de servicios por el SAIA que se encuentra en la Política De Operación Gestión De Tecnologías De Información.

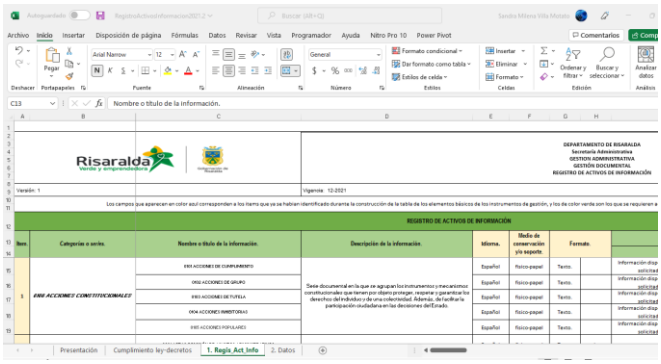
1.1.1 Inventario de los Activos

De acuerdo con los lineamientos dados por el Ministerio de Tecnologías de la Información y Comunicaciones- MinTIC a través de sus decretos y normativa reglamentaria, específicamente del componente del Modelo de Seguridad y

Privacidad de la Información - MSPI, se aporta avance de elaboración del procedimiento Gestión De Activos De Información Seguridad y Privacidad de La Información el cual tiene como fin garantizar la preservación de la integridad, confidencialidad y disponibilidad de la información, por tal razón se informa que el procedimiento fue elaborado tomando como base las buenas prácticas de la gestión de incidentes de seguridad de la información que dispone la norma ISO 27035 y en cumplimiento a las guías emitidas por MinTIC para la elaboración del mismo; considerando la criticidad de la información y la protección de los activos que la soportan, la respuesta a incidentes de seguridad se consolida como una herramienta estratégica que permite al Departamento, no solo estar en la capacidad de dar respuesta oportuna a incidentes de seguridad, si no también detectar, evaluar y gestionar las vulnerabilidades de la plataforma tecnológica que soporta la operación informática, de los sistemas de información misional, de gestión administrativa y de apoyo, principalmente de los medios que alojan los activos de información del Departamento. Se cuenta con un archivo en Excel donde se tiene custodia por parte de Gestión informática y Servicios tecnológicos frente a los activos críticos con toda su información; Se actualizo la política de seguridad y privacidad, y se creó el comité de privacidad, para garantizar la seguridad privacidad de la información y seguridad digital de los clientes internos y externos que hacen uso de los recursos informáticos del Departamento. se identificó la clasificación de los activos de información los cuales fueron publicados por gestión documental como indica la norma, se debe revisar la plantilla toda vez que fue publicada en un formato que no corresponde esto se evidenció una vez se realizó inspección en página de la Gobernación de Risaralda mediante enlace: https://www.risaralda.gov.co/documentos/150020/registro-de-activos-de-informacion/

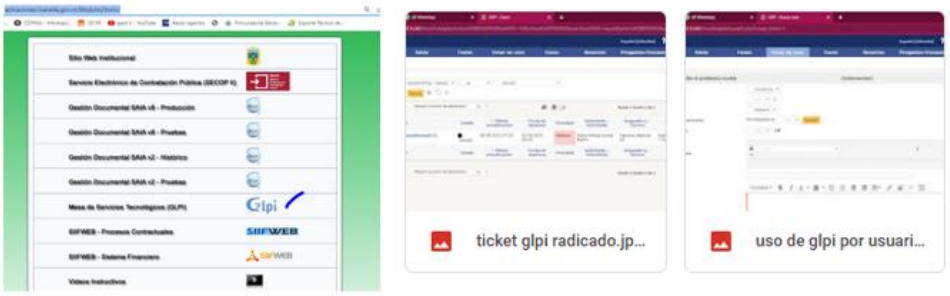


Fuente: archivo compartido por el subproceso de gestión informática y servicios tecnológicos
https://www.risaralda.gov.co/documentos/150020/registro-de-activos-de-informacion/
Imagen 3 ubicación de activos en NAS y web



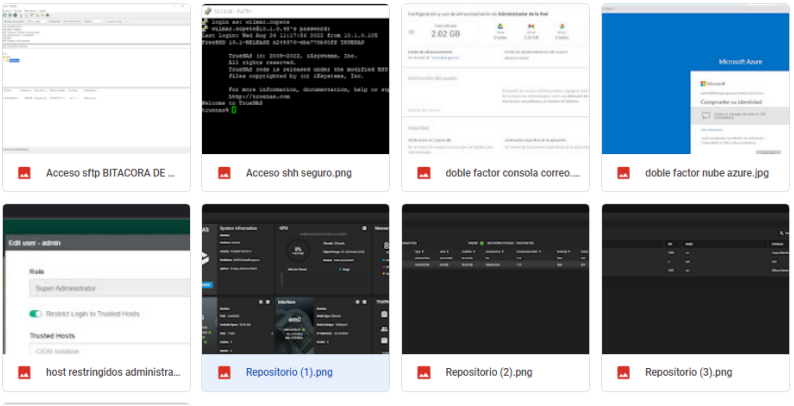
Fuente: https://www.risaralda.gov.co/documentos/150020/registro-de-activos-de-informacion/
Imagen 4 archivo descargado de la web

Teniendo como premisa que los activos se deben tener controlados en diciembre de 2021 se empezó con la ejecución de puesta en marcha en producción por parte del proceso de Gestión Informática y Servicios Tecnológicos la implementación de un procedimiento formal para el registro y cancelación de registro de usuarios. Este proceso de realiza de manera formal por medio de un ticket de gestión de solicitudes en GLPI mediante el enlace http://aplicaciones.risaralda.gov.co/Modulos/Inicio/ esto dio solución a lo que se realizaba de manera informal a través del aplicativo SAIA/solicitud de atención y que algunas ocasiones se perdía la trazabilidad



Fuente: http://aplicaciones.risaralda.gov.co/Modulos/Inicio/
archivo compartido por el subproceso de gestión informática y servicios tecnológicos
imagen 5 capturas de GLPI y captura de ingreso al modulo

así mismo se cuenta con gestión de derechos de acceso privilegiado donde se evidenció un control por parte de los responsables del proceso de Gestión Informática y Servicios Tecnológicos, para la asignación de privilegios a los usuarios por medio del directorio activo y según cláusulas de contratos. Se realizan revisiones periódicas por parte de la Dirección de Informática y sistemas, mediante las cuales se realiza configuración de “usuario estándar” en los equipos de cómputo de la administración. Las contraseñas de los usuarios administradores cuentan con técnicas de doble factor de autenticación a cargo del director y profesional especializado.



Fuente: archivo compartido por el subproceso de gestión informática y servicios tecnológicos
imagen 6 capturas de proceso de control de usuarios

1.1.2 Política de Ámbito Físico al Centro De Datos

1.1.2.1 **"***El acceso físico al centro de datos se debe realizar por el personal autorizado por la Dirección de Informática y Sistemas Tecnológicos-DIST, ya que la puerta permanece debidamente cerrada y asegurada, haciendo de la huella dactilar y combinación numérica de 4 dígitos como doble factor de autenticación"*

Se evidenció que en el momento de verificación de ingreso a centro de datos solo se puede realizar por el usuario autorizado y autentificado que tiene registrada la huella, así mismo se identificó que se lleva el soporte de las personas que ingresaron al centro de datos con la respectiva autorización, se identifica que no se diligencia en algunos casos todas las variables.

Fuente: archivo compartido por el subproceso de gestión informática y servicios tecnológicos y archivo de evidencias controles de riesgos
imagen 7 capturas de proceso de control de ingreso data center

Fuente: propia captura de ingreso al data center 25-08.2022
imagen 8 capturas de proceso de control de ingreso data center

1.1.2.2 *"Cada rack interno del centro de datos debe permanecer con llave y estas deben ser asignadas por oficio a las personas que la Dirección de Informática y Sistemas crea conveniente, en desarrollo de sus funciones."*

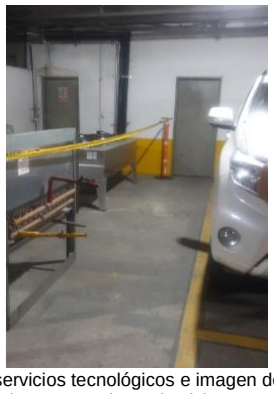
Se evidenció el cumplimiento de esta política por parte de los responsables del proceso de Gestión Informática y Servicios Tecnológicos. El centro de datos de la Administración Departamental cuenta con un dispositivo de seguridad biométrico y permanecen tanto centro de datos como racks debidamente cerrados y fue asignado por acta de reunión se tienen autenticadas para autorizar ingreso tres usuarios que fueron notificados, lo cual se soporta con acta N° 03 del 28 de febrero del 2022.

Fuente: archivo compartido por el subproceso de gestión informática y servicios tecnológicos
imagen 9 acta n 03 del 28-02-2022 autorización y asignación

1.1.2.3 *"Los dispositivos de monitoreo ambiental del centro de datos deben ser revisados a través del software de APC NetBotzAdvanced View"*

Se identifica que se realizó el respectivo monitoreo en el periodo auditado donde se observa que la infraestructura del aire acondicionado fue actualizada se explica por parte de gestión informática que este cambio género que los niveles de calor que se venían presentando se estabilizaran no queriendo indicar que aún no existan dificultades con los medidores de temperatura por su obsolescencia, al revisar evidencias se identifica fallas reportadas en el software

APC en la infraestructura, se identifica que donde quedo ubicada la centrifugadora presenta un riesgo toda vez que aunque se tiene una cinta de seguridad esto no garantiza que por un error humano al parquear se cause un accidente



Fuente: archivo compartido por el subproceso de gestión informática y servicios tecnológicos e imagen de captura de visita imagen 10 estado de reporte de las APC e imagen producto de visita

1.1.3 Ámbito De Administración De Las Bases De Datos De Los Sistemas De Información.

1.1.3.1 *"Los accesos remotos a las bases de datos por parte de terceros deben ser monitoreadas por el administrador de la base de datos y llevar registro en la bitácora de cada base de datos, previamente mediará la solicitud de acceso y será debidamente autorizada."*

Se evidencia control en cuanto a la aplicación de la Bitácora general de inventarios de SW y HW. Para el tema de proveedores: HUMANO, envían scripts a ser instalados como liberación de actualización. SAIA, cuenta con su usuario y clave debidamente documentado en la bitácora, y hace parte de su contrato de mantenimiento del sistema de información; el control está dado por el seguimiento de tickets El mismo se encuentra en el data center de la Gobernación. SIIFWEB se encuentra en su infraestructura TI, y el control está dado por el seguimiento de tickets. Desde la Dirección de Informática y Sistemas, se realiza la labor de monitoreo por parte del administrador de las Bases de Datos a través de los logs, donde se registran secuencialmente todos los acontecimientos, eventos o acciones que puedan ocurrir. Además de esto, en el momento que un tercero requiera realizar un ajuste a su aplicación a nivel de BD, este envía el Script para ejecutar la respectiva actualización.

1.1.3.2 *"Los proveedores de software que brindan soporte, no podrán realizar cambios en la base de datos de producción, estos cambios siempre se*

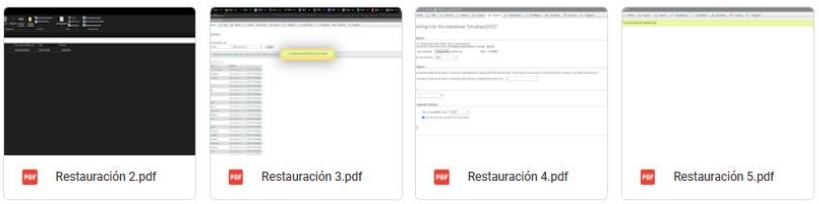
deben realizar en un ambiente de prueba y verificar las afectaciones de los datos; para ser valorados por el personal de soporte de la gobernación y así ser instaladas en el ambiente de producción.".

Se evidenció que la Administración Departamental cuenta con Ambiente de pruebas para el aplicativo SAIA versión 8 y versión 2, no se identificó que exista para el resto de las aplicaciones o que se tenga implementado, ya que no se cuenta con la infraestructura tecnológica (Licencias adicionales de Oracle + infraestructura) para su implementación.

Fuente: archivo compartido por el subproceso de gestión informática y servicios tecnológicos
imagen 11 evidencia de ambiente pruebas SAIA

1.1.3.3 *"Los administradores de base de datos deberán verificar la realización de las copias de seguridad y comprobar su correcta restauración al menos una vez cada cuatrimestre haciendo uso de una máquina virtual.".*

Se evidenció que las Bases de Datos son verificadas y se realiza copias de seguridad, pero por falta de infraestructura tecnológica, no se pueden realizar las pruebas de restauración a las mismas cada cuatro meses, se realizó prueba de restauración de la base de datos del módulo de contratación de Ijuriidca donde se generó con buenos resultados.



Fuente: archivo compartido por el subproceso de gestión informática y servicios tecnológicos
imagen 12 evidencia de ambiente de rasuración base IJURIDACA modulo contratos

1.1.4 Ámbito De Administración De Los Dispositivos Activos De Red.

1.1.4.1 *"La Dirección de Informática y Sistemas asignará por escrito la administración de los dispositivos de red.".*

se evidenció a través del memorando 24635 del 21 de diciembre del año 2021 la asignación formal para la administración de dispositivos de red.

1020- 24635 Dirección de Informática y Sistemas Tecnológicos

MEMORANDO

Pereira, 21 de diciembre de 2021

PARA: Andres Del Rio Restrepo, Contratista
Argemiro Gomez Calderon, Tecnico Administrativo
Grado 06
ASUNTO: Designación y autorización la administración de los dispositivos de red y bases de datos

Cordial Saludo.

En Atención al Plan de Mejoramiento 1049 de 2021 en cuanto al Item 7, se ha designado al funcionario Argemiro Gómez Calderón técnico administrativo Gr-6 con el apoyo del Ingeniero Contratista Andrés del Río para la administración de los dispositivos de red, y bases de datos, del Departamento, para las labores propias en el mismo, aplicando el formato respectivo y con la autorización desde esta Dirección.

Atentamente,

JORGE ALEJANDRO GAITÁN CONTRERAS
Director Tecnico Grado 05
Dirección de Informática y Sistemas Tecnologicos

Revisó : WILMAR LIBERTO [redacted] 68 ✓

Fuente: archivo compartido por el subproceso de gestión informática y servicios tecnológicos
imagen 13 evidencia de asignación dispositivos de red

1.1.4.2 *"La Dirección de Informática y Sistemas asignará por escrito la administración de servidores en sus sistemas operativos y configuraciones.".*

Se aportó evidencia de cumplimiento de funciones de uno de los funcionarios dentro de lo que esta la administración de Servidores.

1.1.4.3 "*Todas las redes inalámbricas existentes en la entidad deberán cumplir con los Estándares de Seguridad definidos por la Dirección de Informática y Sistemas"*

Se evidencia, mediante el establecimiento de reglas en el UTM de una zona LAN- DMZ y una zona WAN –DMZ, existe el levantamiento de requerimientos por parte de los Ingenieros infraestructura y soporte (incluidos en sus alcances contractuales). Para este proceso se implemento dejar documentado los procesos realizados mensualmente para no perder la transferencia del conocimiento estos documentos son parte de la dirección como medio de consulta.

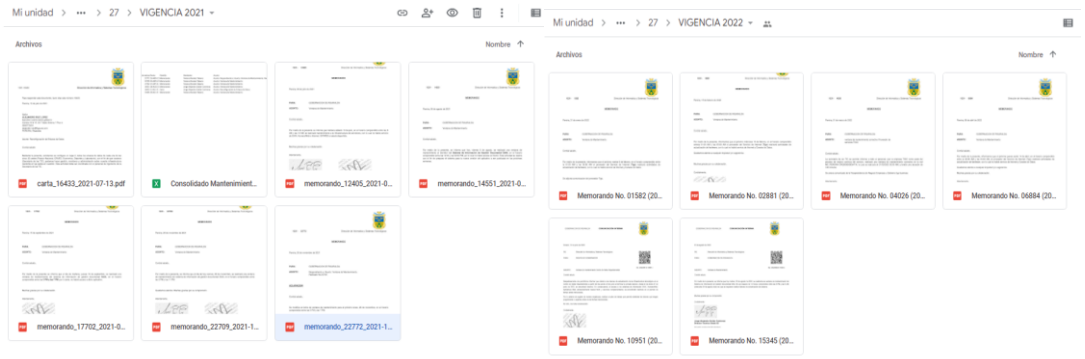
1.2 POLITICAS DE OPERACIÓN DE SEGURIDAD INFORMATICA.

1.2.1 "Las *claves o contraseñas de acceso a los recursos informáticos son responsabilidad exclusiva y confidencial de cada uno de los funcionarios o contratistas de la Administración Departamental. La información generada y/o procesada será responsabilidad del usuario a nombre de quien quede registrada".*

Se realizó pruebas en la mesa de ayuda y se pudo identificar que mediante el controlador de dominio para el uso de los equipos por parte de los usuarios internos se tiene la política de cambio de contraseña y bloqueo en caso de intentos no efectivos al ingreso por vencimiento del contrato u olvido de contraseña, esto frente a la autentificación en el dominio, se identificó que existe el riego que una vez se retire el cable de red y se realice el ingreso por parte de un usuario que no está activo en el dominio este puede ingresar

1.2.2 "*Cualquier suspensión programada de servicios de la Infraestructura tecnológica, tales como mantenimiento de Servidores, Bases de Datos, Servicio de navegación, entre otros; serán informados con anterioridad a través de SAIA, correo electrónico institucional y Spark.".*

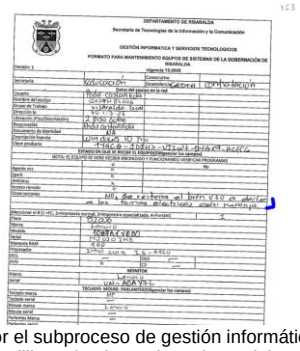
Se identifico que se cumplió con lo determinado en la política donde la suspensión de cualquiera de los servicios es notificada con anterioridad mediante los canales de comunicación habilitados al interior de la Administración Departamental se aportó evidencia de acuerdo con el alcance de la auditoria.



Fuente: archivo compartido por el subproceso de gestión informática y servicios tecnológicos
imagen 14 evidencia de notificaciones de suspensión de servicio por mantenimientos

1.2.3 *"No emplear el tomacorriente regulado (color naranja), para conectar impresoras, neveras, cafeteras, ventiladores, etc. Estos son para uso exclusivo de los equipos de cómputo."*

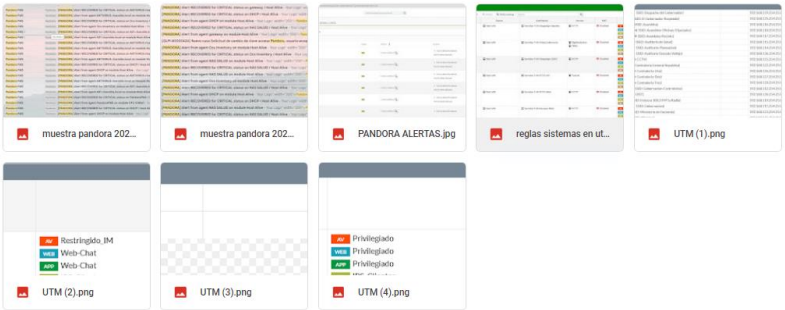
En los mantenimientos se reitera el buen uso de las tomas naranjas, pero se tiene identificado que esta política no se puede controlar una vez que solo se hace revisión por parte los técnicos una vez se hace mantenimiento o es reportado un daño. Así mismo se deja una nota en el formato de soporte, pero no se ha realizado o no se identifico que se realicen campañas del buen uso de este medio de conexión a la red eléctrica.



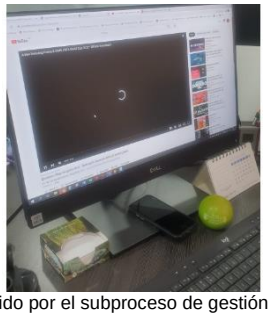
Fuente: archivo compartido por el subproceso de gestión informática y servicios tecnológicos
imagen 15 evidencia de diligenciamiento de mal uso del toma de conexión naranja

1.2.4 *"No se permite el acceso a redes Sociales y contenido multimedia a excepción de las solicitudes especificas realizadas por el secretario de Despacho o director de Dependencia, justificando la necesidad del servicio para el cumplimiento de las funciones del área o dependencia.".*

Se realizaron pruebas en campo con el objetivo de revisar el funcionamiento de las políticas de acceso en la secretaria de haciendo donde se tomaron al azar tres equipos tesorería contabilidad y practicante Sena, se verifica el funcionamiento de los controles realizados en la bitácora de perímetro en cuanto a la habilitación de funcionamiento YouTube, AnyDesk y Facebook esto se realizó con el objetivo de poder verificar la funcionalidad de políticas de restricción y bloqueo para páginas web con contenido sexual y redes sociales, mediante firewall Fortinet, por parte de la Dirección de Informática y Sistemas así mismo se realiza monitoreo continuo.



Fuente: archivo compartido por el subproceso de gestión informática y servicios tecnológicos
imagen 16 evidencia de políticas de restricciones y monitoreo UTM PANDORA Y FORTNET



Fuente: archivo compartido por el subproceso de gestión informática y servicios tecnológicos
imagen 17 evidencia de visita a hacienda

*1.2.5 **"**Restricción de uso a los dispositivos de almacenamiento masivo USB, discos externos, SSD, NAS, DAS, SAN".*

Durante el desarrollo de la auditoria se identificó que se realiza uso de dispositivos USB donde de informo por parte de Gestión Informática y Servicios Tecnológicos. que en un periodo fueron bloqueados y restringidos los puertos de USB, pero ocasiono traumatismos para el funcionamiento de las diferentes dependencias, por lo cual se decidió que se debían tener habilitados, incumpliendo esto con la política de seguridad de la información toda vez que aun esta vigente

1.3 POLÍTICAS DE OPERACIÓN ACCESO AL CENTRO DE DATOS DEPARTAMENTAL.

Para esta política se identifica que está contenida dentro de las políticas de Operación interna DIST de seguridad de la información en la Política de Ámbito Físico al Centro De Datos y ámbito De Administración De Los Dispositivos Activos De Red, por tal motivo no se realiza documentación de proceso

1.4 POLÍTICAS DE OPERACIÓN DE ADMINISTRACIÓN INFORMÁTICA Y DE SISTEMAS DE INFORMACIÓN

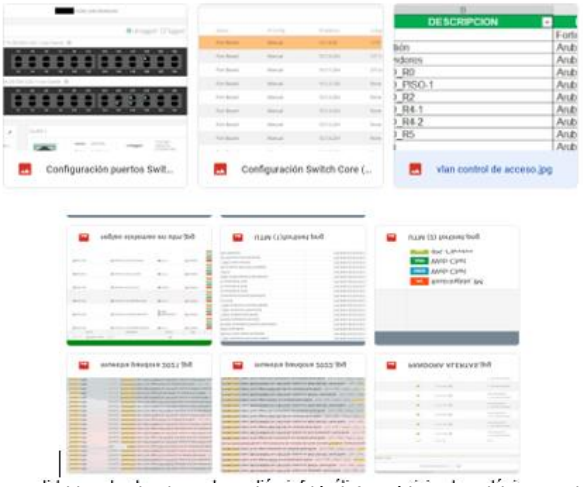
*1.4.1 **"**La creación de cuentas de usuario para acceso remoto a la red interna de la Gobernación a través de VPN, sólo será autorizada por el director de Informática y Sistemas Tecnológicos."*

Se informó que existen ingresos por acceso remoto a la red interna de la gobernación a través de VPN; que son controladas por el director del proceso a través de la bitácora central y a través de esta se realiza el control de quienes tienen acceso, se aportó control de bitácora como las solicitudes de acceso y su respectiva autorización.

Fuente: archivo compartido por el subproceso de gestión informática y servicios tecnológicos
imagen 18 evidencia de autorizaciones y bitácora de control por ingresos VPN

1.4.2 *"La red interna deberá estar protegida de amenazas externas, a través de sistemas que permitan implementar reglas de control de tráfico desde y hacia la red de la Administración Departamental".*

El procesos de gestión informática y servidos tecnológicos cuenta con protección en diferentes capas de la red que son transparentes en algunos casos para el usuario como es el caso de reglas de control de tráfico que se tienen implementadas utilizando, Fortinet, Reglas en sistemas en UTM, y como complemento se hace seguimiento en pandora a las alertas que se presentan en tiempo real, se ha implementado una tecnología de filtros de seguridad conforme a las políticas, se aportó contratos de permanencia de protección de antivirus a través de resoluciones 00012 del 20 de noviembre de 2020 y 016 del 21 de junio de 2022 en estas resoluciones no se puede observar a que fechas van las renovaciones de las licencias, al realizar pruebas se identifica que las diferentes conexiones o redes identificadas se tienen segmentadas y controladas a través de Vlan.

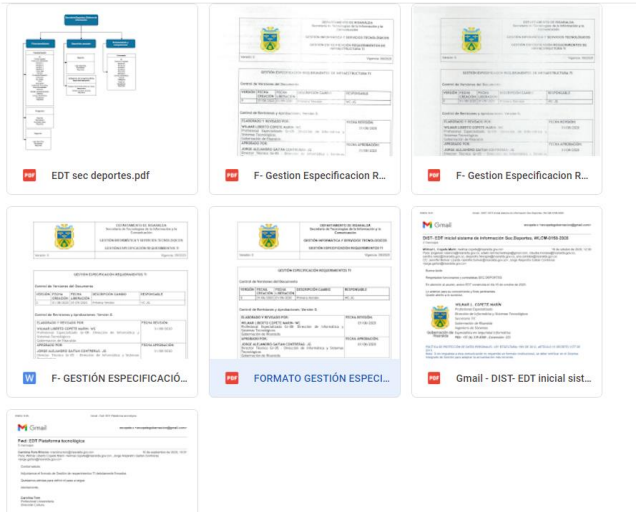


Fuente: archivo compartido por el subproceso de gestión informática y servicios tecnológicos
imagen 19 evidencia de controles de protección interno y externa de perímetro

1.4.3 *"La Administración de Sistemas de Información, en su adquisición, desarrollo y mantenimiento por parte de la Administración Departamental, deberá contar*

con la participación de la Secretaría Tic, Dirección de Informática y Sistemas Tecnológicos, donde se tenga en cuenta la EDT (estructura de desglose de trabajo). Para lo anterior se utilizan los formatos de Especificación de Requerimiento TI y Formato de Especificación de Requerimiento de Infraestructura cuando el proyecto sea nuevo interno, externo o con base Outsourcing".

Se identifica que se realizó la parametrización de los registros en los formatos de Especificación de Requerimiento TI y Formato de Especificación de Requerimiento de Infraestructura cuando el proyecto sea nuevo interno, externo o con base Outsourcing, cuenta con documentos controlados para SAIA donde no se identifican riegos y se cuenta con la documentación de procesos realizados a sistemas de información de deportes, cultura y adulto mayor son procesos que se encuentran en transición pero que están en cambio permanente como es el caso de SAIA donde se indica por parte del proceso de gestión informática que se realizaron diferentes pruebas antes de sacarlo a producción pero por la misma dinámica para poder ajustar se requiere realizar procesos en producción para identificar falencias en tiempo real, se informa que se han presentado fallas que a la fecha se están documentado y ajustando, el aplicativo se encuentra en la DMZ, para evitar el escaneo de puertos y la posibilidad de inyección de código. Se aportó formatos diligenciados en cada uno de los sistemas mencionados con la observación que al revisar las evidencias corresponden al año 2020 y no fueron actualizados.



Fuente: archivo compartido por el subproceso de gestión informática y servicios tecnológicos imagen 20 evidencia de diligenciamiento de formatos de requerimiento

1.5 POLÍTICAS DE OPERACIÓN DE GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

1.5.1 "*Todo requerimiento de servicio y solicitud de atención a la Dirección de Informática y Sistemas Tecnológicos- DIST-, se debe realizar a través de sistema SAIA solicitud de atención Sistemas TIC, sistema para la gestión de soporte técnico de la DIST; administrado por la mesa de servicios TI en la extensión 538, ubicación física piso 0 del Palacio Gris de la Gobernación de Risaralda".*

Teniendo en cuenta que el SAIA es el sistema de gestión documental y que las solicitudes de servicio se realizaban en la versión dos pero no se tenía un control de indicadores de servicios, se implementó el funcionamiento del software de gestión de servicios GLPI desde finales del año 2021 donde empezó a operar el módulo este software fue configurado para que cada usuario pueda realizar la solicitud por medio de un ticket y le pueda realizar trazabilidad tiene clasificación de prioridades y en un futuro se pretende tener documentado el inventario y llevar el histórico de cada maquina con el animo de poder dar soporte y no perder la transferencia del conocimiento del estado del hardware.

1.6 PLANES Y PROCEDIMIENTOS

En el sistema de gestión se encuentran publicados dos procedimientos que hacen referencia a la administración del centro de datos y el soporte técnico a usuarios publicados en agosto 2022, un plan de contingencia y recuperación de los sistemas de información y las comunicaciones el cual fue publicado en el año 2017, el proceso de gestión informática y sistemas tecnológicos aportó evidencia de desarrollo de propuesta del plan actualizado pendiente de aprobación en comité está en revisión, se indica que con este documento se busca asegurar que las Tecnologías de la Información y las Comunicaciones (TIC) trasversal a los procesos de gestión de la Gobernación de Risaralda, cuente con el debido plan de contingencia, recuperación y continuidad del negocio al servicio del cliente interno y externo; donde se busca maximizar la protección de la información y recuperar su espacio tecnológico ante cualquier eventualidad, haciendo uso de buenas prácticas para cubrir su información, hardware, software. Se debe tener presente que las entidades deben definir y aplicar un proceso de valoración de riesgos de la seguridad y privacidad de la información, que permita Identificar los riesgos que causen la perdida de confidencialidad, integridad, disponibilidad, privacidad de la información, así como la continuidad de la operación de la Entidad dentro del alcance del MSPI por ello La entidad debe verifica que los lineamientos, normas y/o

estándares orientados a la continuidad en la prestación de los servicios se cumplan para ello se requiere contar con este plan

Fuente: archivo compartido por el subproceso de gestión informática y servicios tecnológicos y archivo descargado del SG imagen 21 evidencia plan de contingencia publicado 2017 y archivos de propuesta

No se identifica el desarrollo completo de Un Sistema de Gestión de la Seguridad de la Información (SGSI) en funcionamiento como lo indica la política de seguridad y privacidad de la información en su capítulo I artículo 3 objetivo 1 según decreto 1064 del 14 de diciembre del 2020 se identifica que se ha realizado un avance en publicaciones de documentos que hacen parte del SGSI dado que un sistema de gestión de la seguridad de la información tiene componentes a nivel estratégico que definen los requerimientos a considerar en el desarrollo del sistema, como son la alineación estratégica con los objetivos de la organización y las expectativas de las partes interesadas; a nivel táctico definen, la gestión de cumplimiento proporcionan soporte legal y normativo, a nivel operativo definen las actividades que deben desarrollarse en forma continua para mantener el sistema operativo proporcionando información relevante; y a nivel de revisión y mejora, definen las actividades para identificar oportunidades de mejora del sistema.

Teniendo esto como premisa se solicitó avance de transición de protocolo IPV4 a IPV 6 como lo plantea el Ministerio de Tecnología de la información y las comunicaciones donde inicialmente se había dado un plazo para este proceso pero por efectos de pandemia se reglamentó mediante Resolución Número 01126 De 2021 que "*Las entidades estatales del orden nacional que trata el artículo segundo de la presente resolución, deberán culminar el proceso de transición al protocolo IPv6 en convivencia con el protocolo IPv4 a más tardar el 30 de junio de 2022. Por su parte, las entidades territoriales deberán finalizar dicho proceso a más tardar el 31 de diciembre del año 2022. En todo caso, dicha adopción deberá ser acorde al plan de diagnóstico formulado por cada entidad*"

Una vez revisadas las evidencias aportadas no se identifica que el plan de diagnóstico del plan de transición de IPV 4 a IPV 6 aportado cumpla con lo requerido por la resolución toda vez que tiene dos partes una vigencia de 2022 otra de 2020 lo cual no es claro a la ora de revisar el cronograma y los respectivos avances que se tienen a la fecha, se aportó borrador de estudio previo como reuniones realizadas con el ministerio frente a este tema pero no se vislumbra el desarrollo.

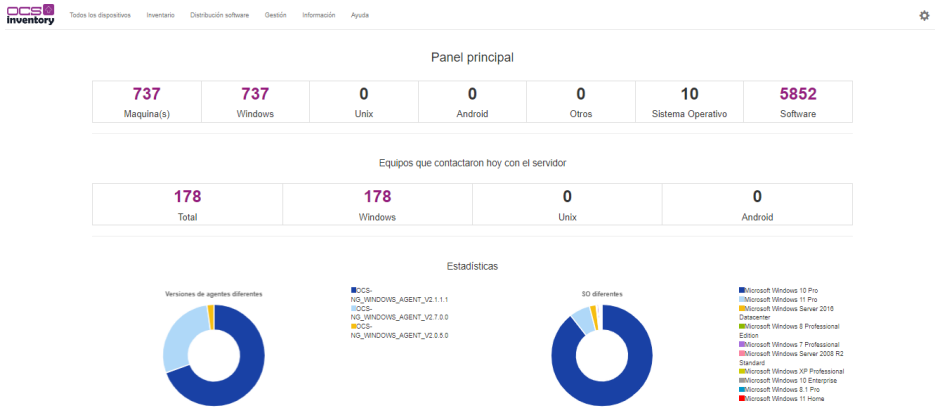
Fuente: archivo compartido por el subproceso de gestión informática y servicios tecnológicos
imagen 22 evidencia acciones realizadas para IPV 4 a IPV6

2. LICENCIAMIENTO DE SOFTWARE

En el momento la administración Departamental cuenta con un total de 678 equipos de cómputo, según la información entregada por el software de inventario de activos **OCS INVENTORY**, el cual se encuentra instalado en cada uno de los equipos de cómputo, y que fue suministrado por la Dirección de Informática y Sistemas del Departamento. De acuerdo con lo anterior y en con el fin de verificar que la Administración cumpla con lo ordenado en la Ley 23 de 1982, Circular 7 de 2005 Departamento Administrativo de la Función Pública se realizó consulta en OCS INVENTORY por nombre de software o aplicaciones ofimáticas no licenciados. Donde se pudo identificar que en algunas maquinas existen instalados programas que permiten atenciones remotas como anydesk y TeamViewer, así mismo se identificó el uso de WinRAR software que requiere tener licencia para estar instalado en las maquinas.

Con el propósito de realizar una revisión eficiente de los equipos de cómputo, la Dirección de Informática y Sistemas suministró acceso al aplicativo **OCS INVENTORY.**

"Open Computer and Software Inventory Next Generation (OCS) es un software libre que permite a los Administradores de TI gestionar el inventario de sus activos de TI. OCS-NG recopila información sobre el hardware y software de equipos que hay en la red que ejecutan el programa de cliente OCS ("agente OCS de inventario"). OCS se puede utilizarse para visualizar el inventario a través de una interfaz web".



Fuente: imagen extraída de OCS INVENTORY
imagen 23 evidencia de reporte OCS INVENTORY general

El proceso de gestión de Informática y Sistemas tecnológicos indica que *"Con OCS no sólo se puede capturar información de equipos, sino que se pueden crear configuraciones que luego se podrán desplegar en la configuración de GLPI. Además, OCS puede integrarse con GLPI para automatizar la sección de inventario que es lo que se pretende en un futuro".*

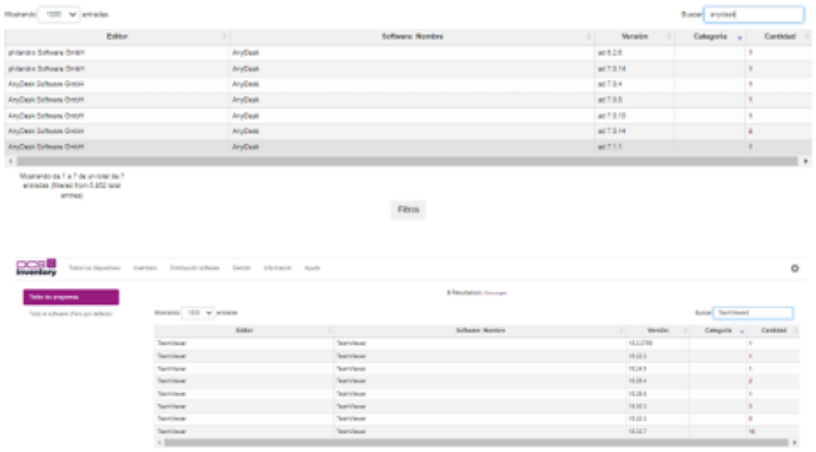
2.1 SOFTWARE INSTALADO

En las consultas realizadas en los diferentes escenarios por maquinas, se pudo establecer que en un 95% el software encontrado es el preinstalado por el fabricante. Así mismo se evidenció la existencia de Software instalado por los usuarios finales, de los cuales, tras el análisis y la validación realizada, son considerados software libre, versiones de prueba, aplicaciones para acceder al contenido de equipos móviles (celulares). Para la explicación del uso de las licencias, se debe diferenciar entre el software preinstalado y el software instalado posteriormente, donde en lo preinstalado se considera todos los programas que están cargados en el disco duro por el fabricante, y en programas instalados posteriormente, todo software instalado por usuarios finales o diferentes al fabricante.

Teniendo en cuenta lo anterior, a continuación, se presentan algunas de las aplicaciones encontradas en los equipos de cómputo, de acuerdo con las consultas arrojado por la herramienta **OCS INVENTORY**:

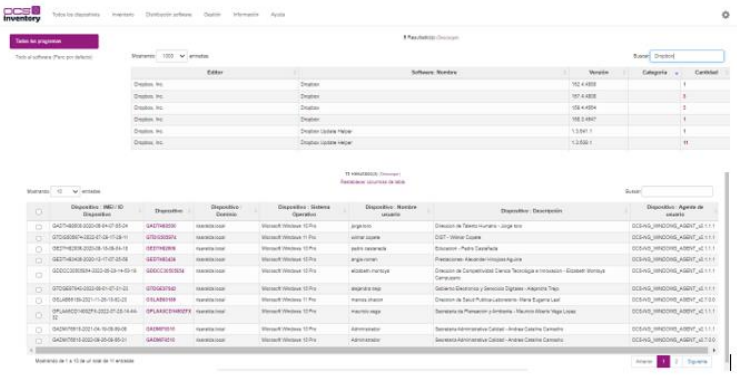
- Software: **AnyDesk**, **TeamViewer**: son softwares informáticos privado de fácil acceso, que permite conectarse remotamente a otro equipo. Entre sus funciones están: compartir y controlar escritorios, reuniones en línea, videoconferencias y transferencia

de archivos entre ordenadores, estas aplicaciones se encuentran en 10 equipos anydesk y 27 equipos TeamViewer, como se observa en las siguientes imágenes.



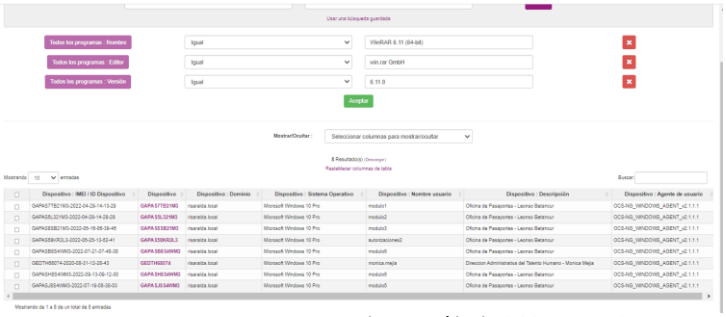
Fuente: reporte generado y extraída de OCS INVENTORY
imagen 24 evidencia de reporte OCS INVENTORY software instalo team wiever y anydesk

- Software: **Dropbox** es un servicio de alojamiento de archivos multiplataforma en la nube, operado por la compañía **Dropbox**. El servicio permite a los usuarios almacenar y sincronizar archivos en línea y entre ordenadores y compartir archivos y carpetas con otros usuarios y con tabletas y móviles. Además del equipo referenciado, esta aplicación se encuentra instalada en varios equipos, como se observa en la siguiente imagen.



Fuente: reporte generado y extraída de OCS INVENTORY
imagen 25 evidencia de reporte OCS INVENTORY software instalo Dropbox

- Software **WinRAR**: es un software de compresión de datos distribuido por Ron Dwight. Aunque es un producto comercial, existe una versión de prueba gratuita de 40 días, después del periodo de prueba transcurrido, cada vez al abrir WinRAR se le mostrará un aviso para que compre una licencia. esta aplicación se encuentra instalada en varios equipos como se observa en la siguiente imagen.



Fuente: reporte generado y extraída de OCS INVENTORY
imagen 26 evidencia de reporte OCS INVENTORY software instalo Winrar

2.2 Sistemas Operativos Instalados

De acuerdo con los registros encontrados en OCS INVENTORY de Microsoft, La Administración Departamental posee las siguientes licencias. Esta cantidad corresponde a las existentes a la fecha de la generación del reporte en auditoria.

Sistema Operativo	TOTAL
Microsoft Windows 10 Enterprise	2
Microsoft Windows 10 Pro	614
Microsoft Windows 11 Home	1
Microsoft Windows 11 Pro	37
Microsoft Windows 7 Professional	3
Microsoft Windows 8 Professional Edition	2
Microsoft Windows 8.1 Pro	1
Microsoft Windows Server 2008 R2 Standard	2
Microsoft Windows Server 2016 Datacenter	15
Microsoft Windows XP Professional	1
TOTAL	678

INVENTARIO DE EQUIPOS	
Sistema Operativo	Cantidad
Microsoft Windows 10	855
Microsoft Windows 11 Pro	41
Microsoft Windows 7	8
Microsoft Windows 8	4
Microsoft Windows 8.1	4
Microsoft Windows XP	6
Windows Vista	1
Total	919

INVENTARIO OBSOLESCENCIA	
Sistema Operativo	Cantidad
Microsoft Windows 7	8
Microsoft Windows 8	4
Microsoft Windows 8.1	4
Microsoft Windows XP	6
Windows Vista	1
Total	23

Fuente: reporte generado y extraída de OCS INVENTORY y reporte evidencias de los riegos
imagen 27 evidencia de reporte de sistemas operativos instalados

Revisados los soportes de los riesgos de gestión se reporta un total de 919 licencias como evidencia a uno de los controles con una diferencia de 219 máquinas que no reporto el software OCS INVENTORY. Teniendo en cuenta que el 9 de abril de 2019 fue la fecha límite de soporte para Windows XP, que para Windows 7 no se dispone de soporte al público en general desde 2015, y que el soporte extendido expiro en el año 2020, el soporte técnico para Windows 8 finalizo el 12 de enero de 2016 y el soporte técnico para Windows 8.1 finalizará el 10 de enero de 2023 como para Windows Server 2008 R2 ya no se recibe soporte técnico solo actualizaciones hasta

enero 2023, se informa que con respecto a esto que ha realizado al trazabilidad de informar a cada una de las dependencias para proceder a sacar del inventario pero no se puede obligar a que no se utilicen quedan bajo al repsonsabildiad de cada dependencia esto aplicaba para el año 2021, pero se informa que teniendo en cuenta que existe un plan de mejoramiento con la Contraloria, donde se debe revisar el tema de licensias tanto de sistemas opertivos como de offce y tomar decisones para dar de baja se esta realizando plan para realizar este proceso lo cual esta pendiente de definir.

2.3 OFFICE

La Administración Departamental posee las siguientes licencias de Office según reporte aportado para informe de derechos de autor. Se realizó solicitud a cada dependencia para compra de equipos Se instala certificado desde UTM con Fortinet para restringir lo que entre y salga. Se informa que se realizó una reunión con la oficina de contabilidad en la tercera semana de agosto por que se suscribió plan de mejora con la contraloría por el tema de licencias se va a determinar el tema útil de las licencias para poder dar de baja no se documenta toda vez que no corresponde al alcance de la auditoria y el proceso esta en este momento revisando con las secretarias que tiene que ver con el tema por ser una decisión trasversal al proceso

PRODUCTO	Total
Microsoft Office Standard 2013	151
Microsoft Office Standard 2016	610
OpenOffice 4.1.2	1
OpenOffice 4.1.6	4
OpenOffice.org 3.0	1
OpenOffice.org 3.1	1
OpenOffice.org 3.2	2
TOTAL	**770**

Fuente: reporte generado y extraída de soporte informe derechos de autor
imagen 28 evidencia existencia de office por versión

2.4 ANTIVIRUS

Por parte del director de Sistemas, fue suministrado los contratos No. 1617 del 29 de junio de 2022. Una vez revisado dicho contrato, encontramos que uno de las obligaciones es la de suministrar 1 licencia de Software Antivirus para 1000 estaciones que va hasta el 31 de diciembre de 2022, ya instalado en los equipos de cómputo de la Administración Departamental, de lo anterior y teniendo en cuenta que el inventario de equipos de cómputo de la Administración Departamental es de 638 según reporte generado del OCS, y el reporte en los riegos de gestión es de 919 se puede establecer

que hay cobertura para el total de equipos de cómputo a la fecha no se pudo identificar que en el periodo de junio 2021 a junio 2022 se contara con este seguridad de perímetro.

2.5 CONTROLES PARA EVITAR LA UTILIZACIÓN E INSTALACIÓN DE SOFTWARE NO LICENCIADOS.

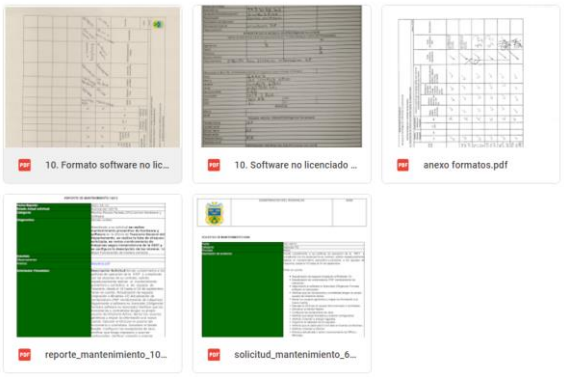
Para mitigar la utilización de software no licenciado, la Dirección de Informática y Sistemas, quien es el área responsable de los recursos tecnológicos de la Administración Departamental, tiene implementado lo siguiente:

2.5.1 Vigilancia y Monitoreo.

Para la ejecución de esta actividad es utilizado el aplicativo Web OCS INVENTORY. Para este proceso desde la mesa de ayuda se hace revisión integral desde la mesa de servicios, de cada equipo, donde se registra solicitud del servicio, para revisión integral de cada equipo, la misma es asignada a un técnico, quien debe atender el caso y documentar la solicitud con los respectivos formatos de registro

2.5.2 Revisión y Barrido.

Esta actividad se realiza periódicamente con el apoyo del personal adscrito a la Dirección de Informática y Sistemas.



Fuente: archivo compartido por el subproceso de gestión informática y servicios tecnológicos
imagen 29 evidencia de actividades de barrido de software instalado

2.5.3 Mantenimiento de Directorio Activo.

"Active Directory (AD) o Directorio Activo son los términos que utiliza Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Utiliza distintos protocolos, principalmente LDAP, DNS, DHCP y Kerberos.

De forma sencilla se puede decir que es un servicio establecido en uno o varios servidores en donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red, así como también la administración de políticas en toda la red.

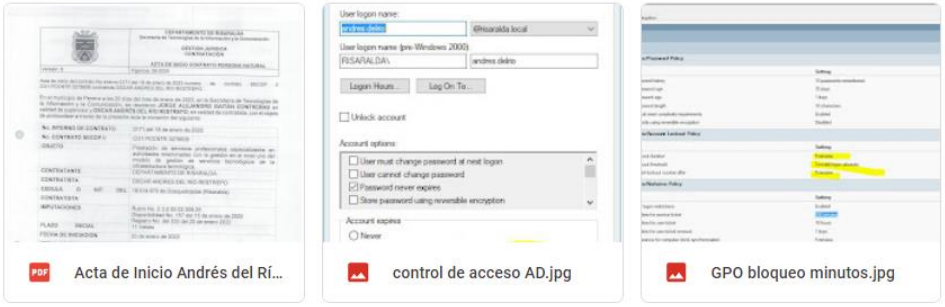
Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso.1

Active Directory permite a los administradores establecer políticas a nivel de empresa, desplegar programas en muchos ordenadores y aplicar actualizaciones críticas a una organización entera."

Desde la Dirección de Informática y Sistemas se cuenta con directorio activo, el cual tiene beneficios a nivel informático para la Administración Departamental, tales como:

- Organización: permite crear grupos para facilitar la administración.
- Permisos: control desde un sólo punto de los permisos a los recursos de la red.
- Autenticación: cualquier usuario puede entrar en otro equipo de la red con su usuario y clave, y tendrá los permisos que le hayan asignado.
- Políticas: Se puede controlar el comportamiento de los equipos y permisos de los usuarios de forma muy concreta.
- Autenticación externa: permite que otras aplicaciones lean los datos. Ejemplo: una aplicación de contabilidad no requiere otra clave para entrar, lee la del usuario en el directorio activo.
- Replicación: implementa características para la replicación de todos los datos entre servidores del directorio activo.

Esto se pudo identificar por medio de realización de pruebas de campo donde se solcito el acta de inicio de ingeniero de soporte de infraestructura y se revisó política de bloque de usuario, así mismo se identificó la política de hibernación y bloqueo de los equipos una ves no tengan funcionamiento.



Fuente: archivo compartido por el subproceso de gestión informática y servicios tecnológicos
imagen 30 evidencia de parametrización de políticas en directorio activo

2.6 DESTINO FINAL DEL SOFTWARE.

Todo equipo de cómputo reportado por el funcionario como inservible, es llevado al taller de Sistemas con el fin de certificar que la maquina no es funcional, y así llevar a cabo el procedimiento de baja ante la Dirección de Recursos Físicos. El software preinstalado en estas máquinas automáticamente pasa a ser dado de baja, teniendo en cuenta que hacen parte de las licencias OEM, las cuales están ligadas al equipo donde vienen instaladas.

3. Riesgos de Gestión del proceso Gestión Informática y Servicios Tecnológicos.

El proceso de Gestión Informática y Servicios Tecnológicos tiene identificados cuatro riesgos de gestión dentro de su proceso:

1. Interrupción del servicio de red de datos.
2. Inoperatividad de elementos de hardware y software en estaciones de trabajo y servidores de la Entidad.
3. Pérdida de la Información digital contenida en los correos institucional, servicios cloud, data center y demás información necesaria para continuar con los procesos y procedimientos de la administración departamental.
4. Uso de software no licenciado en los equipos de cómputo propiedad de la Gobernación de Risaralda.

Una vez validados estos riesgos, se evidenció lo siguiente:

Se realizan los Backus y el monitoreo de la tipología de la redLan de la administración central programados en el segundo, cuatrimestre de la vigencia 2022. De igual manera, la verificación del nivel de obsolescencia tecnológica de los equipos activos de red. Se aplica de forma efectiva la herramienta de control de acceso al centro de datos, centros de cableado y rack de comunicaciones de la administración central. De

las evidencias se identifica que los Backups del primer seguimiento corresponden al año 2022 pero los del segundo son de vigencias que no corresponden porque, aunque son incrementales como se explico por parte del proceso en las evidencias se identifica fechas que no corresponden. Se aportó acta de la contratación de seguridad perimetral y licencias antivirus vigencia de junio a diciembre, pero no se identificó que En el periodo de junio 2021 a junio 2022 se contara con la seguridad perimetral.

Fuente: archivos descargados del sistema de gestión en el módulo de riesgos del proceso de gestión informática y servicios tecnológicos seguimientos imagen 31 evidencia subidas para seguimiento de los riesgos

DERECHO DE RÉPLICA-MESA DE TRABAJO

Mediante memorando N° 19125-I de octubre 7 de 2022, la Oficina Asesora de Control Interno de Gestión, presentó informe preliminar, a fin de que el Proceso de Gestión Informática y Servicios Tecnológicos, procedieran a responder los respectivos posibles hallazgos negativos y observaciones.

el Proceso de Gestión Informática y Servicios Tecnológicos ejercicio su derecho de réplica mediante memorando No. 19717-I del 14 de octubre de 2022, frente a:

Hallazgo No. 1 incumplimiento de la Resolución Número 00500 De marzo 10 De 2021 Artículo 17 comprendido en La Políticas De Seguridad Y Privacidad De La información Artículo Tercero Desarrollar Un Sistemas De gestión De Seguridad De La información (SGSI). Durante la auditoria y teniendo en cuenta las evidencias compartidas en driver No se evidenció el desarrollo de un Sistemas De gestión De Seguridad De La información (SGSI) que contenga un plan de continuidad del negocio según lineamiento de MINITIC mediante la implementación en el modelo de seguridad de la información “MSPI” y resolución número 00500 que indica en su artículo 17 Etapas generales de la gestión de incidentes de seguridad digital. Los sujetos obligados deben incluir en su estrategia de seguridad digital las actividades a realizar

en las etapas de prevención; protección y detección; respuesta y comunicación; recuperación y aprendizaje. Incurriendo en el incumplimiento de la resolución 00500 artículo 17 y en la adopción de la política mediante el decreto 1064 de diciembre de 2020.

Se realiza derecho de réplica en los siguientes términos: En el desarrollo del Sistema de Gestión de Seguridad de la Información SGSI, en lo referente a los aspectos considerados en el artículo 17 de la Resolución N°. 00500 de marzo 10 de 2021 expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones, en adelante, MinTIC:

La Dirección de Informática y Sistemas Tecnológicos, viene implementando el Sistema de Gestión de Seguridad y Privacidad de la Información SGSPI adoptado mediante el Decreto 1078 de 2018 en el capítulo de Política de Gobierno Digital, el cual incorpora en sus etapas de planificación, implementación y mejora continua, los aspectos referidos en el artículo 17 de la Resolución N°. 00500 de marzo 10 de 2021, por lo que no es preciso afirmar que se incumple la resolución 00500 artículo 17 y en la adopción de la política mediante el decreto 1064 de diciembre de 2020. Estos avances se pueden validar con los resultados del Furag de las vigencias anteriores.

De manera seguida, consignar que la Resolución inicialmente mencionada, fue ajustada por MinTIC, con la Resolución N°.000746 de marzo 11 de 2022, y su anexo técnico Relación con Proveedores, donde incluye la Gestión de la Seguridad con los proveedores, con base en la adquisición de productos y servicios, donde la Dirección de Informática y Sistemas Tecnológicos ha incorporado las pruebas de funcionalidad en los productos de software que han sido adquiridos, tal y como consta en las evidencias de la presente auditoría. Y sumado a lo anterior, al interior del proceso técnico de supervisiones contractuales donde los funcionarios de la misma Dependencia han sido asignados.

Con estas precisiones, se procederá de conformidad a realizar las acciones necesarias, para alcanzar el 100% de cumplimiento del artículo 17 de la Resolución N°. 00500 de marzo 10 de 2021, apoyados en las tareas realizadas para la implementación del MSPI.

Con lo anterior, se hace uso del derecho a réplica a que el Hallazgo N°1 no corresponde a una omisión por parte de los sujetos obligados, sino, a una Observación que debe ser atendida por parte de la Dependencia, con el suministro de la evidencia que sea solicitada por la Oficina de Control Interno.

RESPUESTA DE LA OFICINA ASESORA DE CONTROL INTERNO

En mesa de trabajo realizada el día 14 de octubre de 2022 se realiza socialización del Hallazgo con respecto a lo planteado en la réplica donde se acuerda que el hallazgo no se mantiene y se convierte en observación, de acuerdo con la justificación realizada en la réplica; por los responsables del proceso auditado Gestión Informática y servicios tecnológicos.

OBSERVACIONES

1. Es necesario que el proceso de gestión informática y servicios tecnológicos cuente con el Plan de Continuidad de Negocio (BCP) y el Plan de Recuperación de Desastres (DRP) teniendo en cuenta que estos hacen parte del desarrollo del Sistemas De gestión De Seguridad De La información (SGSI) según lineamiento de MINITIC mediante la implementación en el modelo de seguridad de la información “MSPI” y resolución número 00500 que indica en su artículo 17 Etapas generales de la gestión de incidentes de seguridad digital. Los sujetos obligados deben incluir en su estrategia de seguridad digital las actividades a realizar en las etapas de prevención; protección y detección; respuesta y comunicación; recuperación y aprendizaje.

2. Es conveniente que se inicie con el proceso de transición de IPV 4 a IPV 6 teniendo en cuenta la Resolución Número 01126 De 2021 donde se indica que los tiempos para las entidades territoriales deberán finalizar dicho proceso a más tardar el 31 de diciembre del año 2022 lo cual el no iniciar la transición puede generar sanciones a la entidad en un momento determinado.

3. Es importante que se cuente con ambiente de prueba para todos los sistemas de información que tiene la gobernación de Risaralda y que son supervisados por la dirección informática, como poder tener ambientes de restauración con los Backups que se realizan pero que por no contar con la infraestructura no se pueden realizar lo cual puede generar perdidas o caídas de servicio en un momento determinado.

4. Es necesario que se realice un adecuado control a la hora de realizar actualizaciones a las políticas que se tienen publicadas en el sistema de gestión toda vez que se identificaron acciones planteadas que a la fecha no son objetos de ejecución como fue el caso de las solicitudes de atenciones por el SAIA, uso de dispositivos USB; así mismo revisar la posibilidad de poder converger las políticas sin repetir acciones en

las que se tienen iguales acciones, esto trae consigo un mejor entendimiento y claridad para el usuario final.

5. Es importante que se incluya en el plan de sensibilización o capacitación el buen uso de las tomas naranjas de acuerdo con la política toda vez que es importante que se mantenga y se vele por el cumplimiento de esta para evitar el mal uso y posible daño de los elementos tecnológicos

6. es necesario que se revise el ítem de la política operación De Seguridad Informática que establece que: "*Todo los funcionarios o contratistas que utilicen los Recursos Informáticos, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica"* muestra que no es posible el cumplimiento dado que no se tiene el control directo ni responsabilidad directa toda vez que es trasversal a la entidad por consiguiente, se requiere de ajuste que integre una política de conservación electrónica para dar cumplimiento de los lineamientos MINITC, a LA NORMA TÉCNICA CALIDAD NTC ISO 27001 V2013 donde establece que: "*La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada*".

7. Es conveniente que se realice seguimiento y control a los formatos, documentos que se publican en el sistema de gestión y en la página para no incurrir en utilización de versiones y formatos obsoletos que permiten hallazgos de otro tipo.

RECOMENDACIONES

1. Establecer mecanismos de control para el servicio de GLPI que se implemento frente a la solución del ticket de solicitud realizada por los usuarios, garantizando que no se den por terminados sin dar una solución real a la solicitud.

2. Se sugiere implementar barrera de seguridad frente al perímetro donde se encuentra ubicada la centrifugadora toda vez que está expuesta a un error humano que puede ocasionar pérdidas económicas y daños en la infraestructura tecnológica

3. Para dar cumplimiento al cronograma de mantenimiento físico y teniendo en cuenta que no se tiene la responsabilidad de la adquisición de los insumos se recomienda implementar un mecanismo de control para tener a tiempo y dar cumplimiento al cronograma, como realizar revisión de los formatos implementados donde se identifique las fechas de realización sea en físico o digital.

4. Es pertinente poder contar con la transferencia del conocimiento con relación a indicadores de servicio realizados y que se tengan de forma oportuna a la hora de realizar consultas de posibles soluciones a la infraestructura.

5. Sería útil para la gestión de informática y servicios tecnológicos que se estudie la posibilidad personal de carrera administrativa en futuros procesos de organización de planta de personal o modernizaciones que se vayan a efectuar, toda vez, que la dirección cuenta con personal de apoyo por medio de la modalidad de contratación, el cual es necesario para dar continuidad al programa de gestión, y debe garantizar la continuidad para que el proceso se mantenga, pero existen cargos que son críticos para su adecuado desarrollo.

6. Se sugiere tener presente el cumplimiento de las metas del plan de desarrollo frente a la misión y visión que se enmarco frente a tecnología y que para ello se requiere de renovación de la infraestructura tecnológica “hardware y software”

7. El proceso de Gestión Informática y Servicios Tecnológicos anexo evidencias de avance frente a la construcción de los riegos de seguridad digital del proceso, pero teniendo en cuenta que a la fecha no se cuenta con el consolidado de los riegos de seguridad digital se recomienda revisar por parte de la secretaria toda vez que están enmarcados en la política de administración del riego adoptada por la Gobernación de Risaralda.

8. Es pertinente que se tenga presente el cumplimiento del plan de acción suscrito con el FURAG resultado de las recomendaciones realizadas vigencia 2021.

CONCLUSIONES

1. La dirección de gestión informática y servidos tecnológicos ha realizado esfuerzos en cumplimiento de la normatividad, pero por ser una dirección trasversal a la entidad depende de los esfuerzos que se realicen en algunos casos desde la alta gerencia para poder dar cumplimiento al modelo MSPI direccionado desde el Ministerio de Tecnologías de la Información y Comunicaciones.

2. La auditoría se ejecutó de acuerdo con lo previsto en el Plan de Auditoria y se cumplió con el objetivo y alcance; es importante resaltar el compromiso con el que se contó durante la auditoria por parte de del proceso de Gestión informática y servicios Tecnológicos, frente a la cordialidad, disponibilidad y atención prestada.

Sandra Milena Villa Motato
Auditor