COMCAJA
CAJA DE COMPENSACION FAMILIAR CAMPESINA

CAJA DE COMPEMSACION FAMILIAR CAMPESINA
COMCAJA

INFORME DE AUDITORIA

PROCESO O AREA AUDITADA:	**UNIDAD DE GESTIÓN DE TICS**
TRABAJADORES AUDITADOS:	**CARLO NARANJO** – Líder de Unidad **LUIS ANTONIO BERNAL** **FELIPE RODRIGUEZ**
.FECHA DE INFORME:	**FEBRERO DE 2019**
FECHA DE LA VISITA DE AUDITORIA:	**SEPTIEMBRE - DICIEMBRE DE 2018**
AUDITOR:	**JHON QUINTERO ALONSO**

Dando cumplimiento al Cronograma de Auditoría de rutina aprobado por la Dirección Administrativa para el año 2018, de manera atenta me permito comunicarle que el día 29 de Septiembre de 2018, se dio inicio a la Auditoria de esta Unidad, verificando el adecuado cumplimiento de los procesos y procedimientos establecidos, realizando las pruebas de auditoría necesarias para tener evidencia suficiente y poder emitir el informe de auditoría.
Las evaluaciones se realizaron de acuerdo con la regulación, las políticas definidas por el Agente Especial de Intervención y mejores prácticas de auditoría sobre el particular. Es importante mencionar que la responsabilidad del auditor interno es señalar los hallazgos y recomendaciones sobre los sistemas de control interno y de administración de riesgos

1. OBJETIVO

Verificar la aplicación de los procesos y procedimientos señalados en los instructivos, manuales, reglamentos, normatividad vigente, así como validar los controles existentes para mitigar y evitar los riesgos de la Unidad.

2. ALCANCE

El alcance de este trabajo se da por la evaluación de la gestión de la Unidad de Gestión de Tics para el año 2017 y lo corrido del año 2018.

3. RESULTADOS GENERALES DE LA AUDITORIA

A continuación me permito describir la metodología utilizada para describir los aspectos más relevantes encontrados en la auditoría:

Metodología - Calificación de Situaciones Observadas

Para propósitos de este informe, se clasificaron las situaciones observadas en:

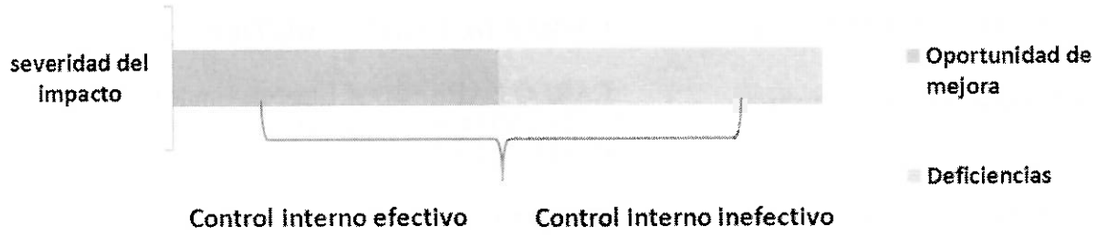
- Deficiencias de control interno.
- Oportunidades de mejora, entendidas así:

Oportunidad de Mejora: Corresponde a aquellos hallazgos que no siendo una deficiencia, presentan oportunidad para aprovechar en aspectos de eficiencia y/o eficacia en el logro del objetivo de control que se persigue.

Estas circunstancias están relacionadas con actividades de ajuste que buscan fortalecer los procesos y por tanto, conllevan acciones de adopción potestativa por parte de la Universidad.

Una deficiencia es una situación que afecta el cumplimiento de los objetivos sujetos al alcance de la auditoría.

Escala Cualitativa A continuación, se detalla la escala cualitativa de calificación asignada a los factores previamente descritos asociados a las situaciones observadas para el cumplimiento del alcance de esta auditoria:



Valoración de riesgos: Adicionalmente, se ha incorporado la metodología de valoración de riesgos, de la siguiente manera:

Tipo de Hallazgo	Impacto del riesgo	Requiere Plan de acción
Oportunidad de mejora	Insignificante - Bajo	Si. Nota: La oportunidad de mejora corresponde a una posible mejora al proceso sin que esto quera decir que este mal ejecutado el control.
Deficiencia	Significativo	Si. Nota: En este caso la observación se incluye en informe ya que la situación descrita en la misma podría convertirse en un riesgo que impida el alcance de los objetivos

3.1. ADMINISTRACIÓN DE BIENES Y SERVICIOS INFORMÁTICOS

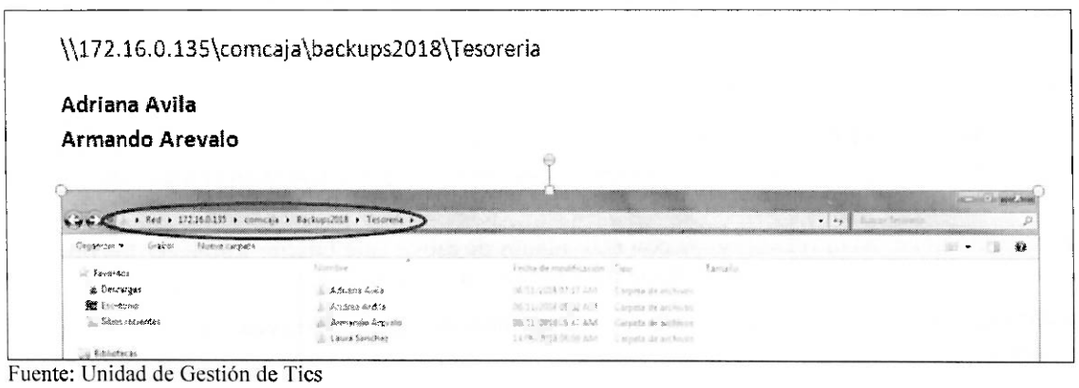
3.1.1. VERIFICACIÓN DE SISTEMAS DE BACK UP Y/O RESPALDO

A continuación se describen las acciones adelantadas por la Unidad de Gestión de Tics por motivo de la administración de los respaldos de información y evidenciadas en esta auditoria:

Back -up equipos de cómputo

- Se realizan mensualmente desde (septiembre 2018) antes era semestral por capacidad en los servidores.
- XP (manualmente en el puesto de trabajo) última fecha de back up oct 26 de 2018.
- Windows 7 (se programa automáticamente)

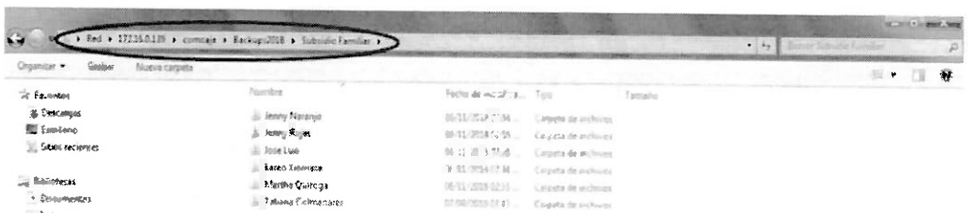
Evidencias: Back-up realizados a los equipos de cómputo de la sección de Presupuesto y Tesorería, Departamento de Subsidio Familiar con fecha de realización el **06 de noviembre de 2018**. Tal como se observa en las siguientes imágenes:



Fuente: Unidad de Gestión de Tics

\\172.16.0.135\comcaja\backups2018\Subsidio Familiar

Martha Quiroga

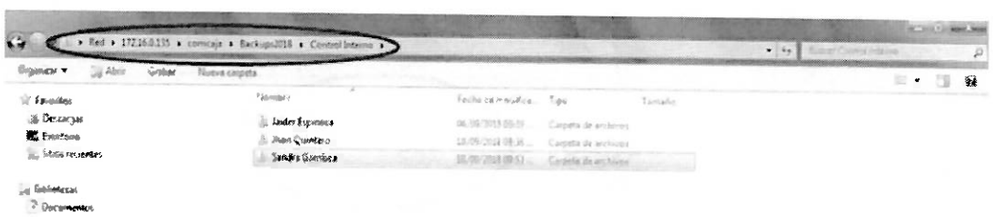


Fuente: Unidad de Gestión de Tics

Back-up realizado a los equipos de cómputo de la Unidad de Control Interno Corporativo, Sección de Contabilidad con fecha de realización el **18 de Septiembre de 2018**. Tal como se observa en las siguientes imágenes:

\\172.16.0.135\comcaja\backups2018\Control Interno

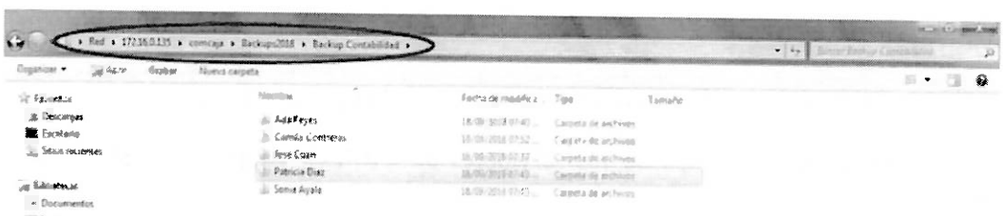
Sandra Gamboa



Fuente: Unidad de Gestión de Tics

\\172.16.0.135\comcaja\Backups2018\Backup Contabilidad

Patricia Díaz

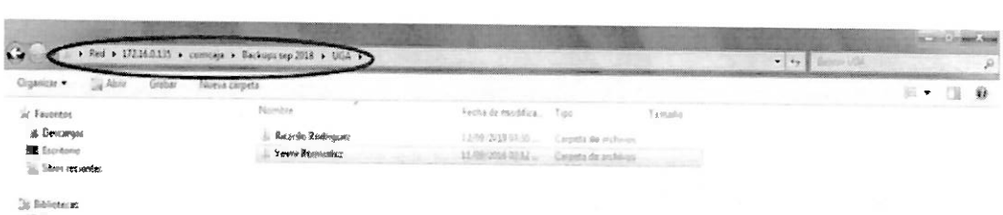


Fuente: Unidad de Gestión de Tics

Back-up realizado a los equipos de cómputo de la Unidad de Gestión Administrativa, Unidad Misional de Servicios Sociales con fecha de realización el **11 de Septiembre de 2018**. Tal como se observa en las siguientes imágenes:

\\172.16.0.135\comcaja\Backups sep 2018\UGA

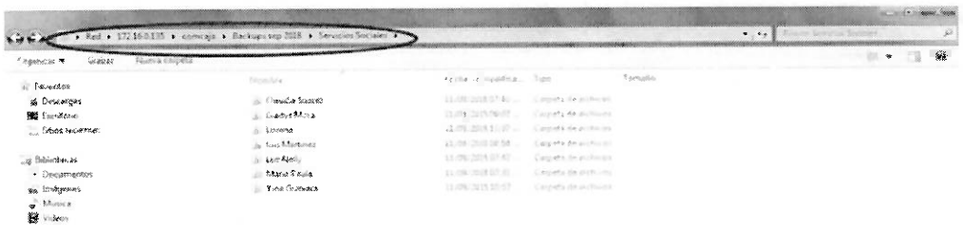
Yeimi Bermúdez



Fuente: Unidad de Gestión de Tics

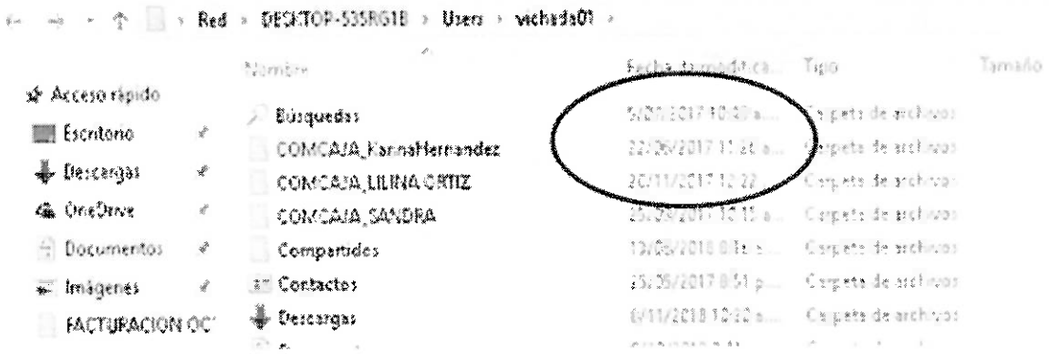
\\172.16.0.135\comcaja\Backups sep 2018\Servicios Sociales

Luis Carlos Martínez



Fuente: Unidad de Gestión de Tics

Según lo informado por la Unidad de Gestión Administrativa los Back-ups de los equipos de cómputo de las oficinas departamentales a la fecha de al auditoría se encuentran alojados en la carpeta compartida local de cada departamental, se está gestionando la compra de unidades externas y disponer de un trabajador para la capacitación para realizar los Back-ups.
Conforme a las evidencias suministradas por la Unidad de Tics el último Back-up realizado a los equipos de la departamental Vichada corresponden al año 2017, tal como se observa en la siguiente imagen:



Fuente: Unidad de Gestión de Tics

BACK UP SERVIDORES

Se evidenció que los back-up de los servidores se realizan de la siguiente forma:

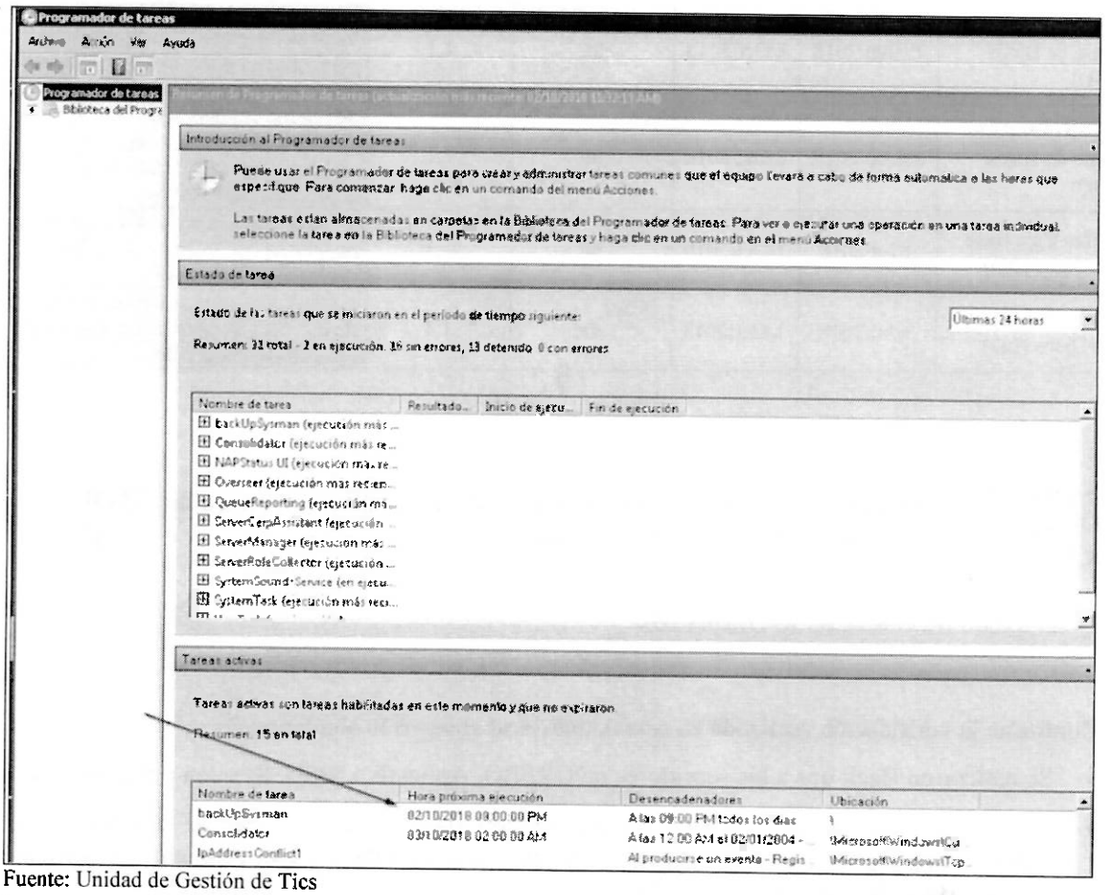
A diario: Se realizan los Back-ups de los servidores de ORFEO, Aplicativo SISU, Sysman y Servivienda.

- **Proceso de Orfeo:** Se ejecuta con una instrucción manual por parte del ingeniero encargado, se realiza en las tardes post jornada laboral.
  Está pendiente desarrollar esta actividad de manera automatizada.

- **Proceso de Sysman, SISU:** se realiza a través del programador de tareas, internamente el aplicativo tienen programadas las actividades de back-up. Como se evidencia en las imágenes a continuación:

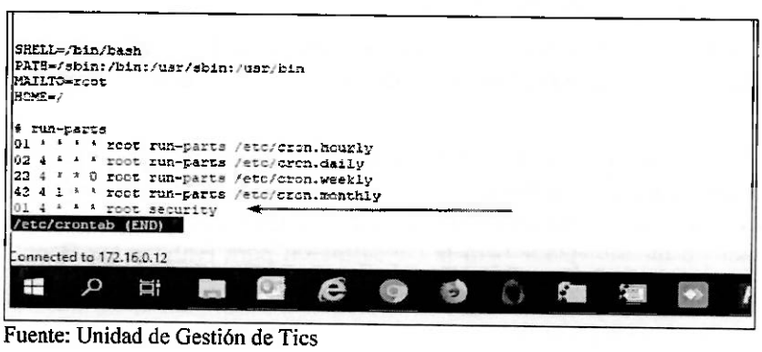
COMCAJA
CAJA DE COMPENSACION FAMILIAR CAMPESINA

Programador de tareas Sysman



Fuente: Unidad de Gestión de Tics

Programador de tareas SISU



Fuente: Unidad de Gestión de Tics

El resultado de los back ups el ingeniero encargado los mueve al servidor de back ups 172:15.0.25.
Bimensualmente: Según lo informado por el profesional de la Unidad de Tics se realizaron back ups cada dos meses a servidores de la página web, intranet, SIRECI, SIREVAC y Asopagos. La tarea de ejecuta de manera manual.
La tabla a continuación detalla lo evidenciado aplicando las pruebas de auditoría, para tal fin se analizó el periodo comprendido entre el 29 de junio y el 02 de octubre de 2018, la cantidad de Back-ups realizados y la frecuencia de realización:

APLICATIVO - TIPO	Periodo analizado en la auditoría		Cantidad Back up realizados	Frecuencia Back up (en días)	Observación de auditoría
SERVIVIENDA	17/Jul/2018	1/Oct/2018	44	1,3	Se realiza diariamente (días laborales) Se ejecuta con instrucción manual
SISU Base de Datos (BD)	3/Jul/2018	2/Oct/2018	80	1,1	Se realizó diariamente Se evidencia que los back ups se realizaron a las 5:54 horas de acuerdo al programador de tareas
SISU Programas	30/Jun/2018	2/10/2018	84	1,1	Se realizó diariamente

(PRG)					Se evidencia que los back ups se realizaron a las 6:11 horas de acuerdo al programador de tareas
Sysman Nomina Base de Datos (BD)	29/Jun/2018	2/Oct/2018	**85**	1,1	Se realizó diariamente Se evidencia que los back ups se realizaron a las 21:02 horas de acuerdo al programador de tareas
SYSMAN-ERP-Base de Datos (BD)	29/Jun/2018	2/Oct/2018	**90**	1,1	Se realizó diariamente Se evidencia que los back ups se realizaron a las 21:31 horas de acuerdo al programador de tareas
Orfeo Caja Base de Datos (BD)	3/Jul/2018	1/Oct/2018	**50**	1,3	Se realiza diariamente (días laborales) Se ejecuta con instrucción manual de profesional encargado
Orfeo Prod Base de Datos (BD)	3/Jul/2018	1/Oct/2018	**49**	1,4	Se realiza diariamente (días laborales) Se ejecuta con instrucción manual de profesional encargado

Situación Observada No. 1	Actualizar la Política de respaldo y restauración de los sistemas de información, datos y configuraciones	**OM**	**X**
		D	**X**

Descripción de la Situación Observada

Conforme la verificación realizada en esta auditoría se observó lo siguiente:

- Se realizaron Back ups a los servidores de ORFEO, Aplicativo SISU, Sysman y Servivienda.
- El back-up del aplicativo Orfeo se ejecuta con una instrucción manual por parte del ingeniero encargado, se realiza en las tardes post jornada laboral, está pendiente desarrollar esta actividad de manera automatizada.
- Los back-ups de los aplicativos Sysman, SISU: Programador de tareas, internamente el aplicativo tienen programadas las actividades de back up
- Según lo informado por el profesional de la Unidad de Tics se realizaron back ups cada dos meses a servidores de la página web, intranet, SIRECI, SIREVAC y Asopagos. La tarea de ejecuta de manera manual.
- Según lo informado por la Unidad de Gestión Administrativa los Back-ups de los equipos de cómputo de las oficinas departamentales a la fecha de la auditoría se encuentran alojados en la carpeta compartida local de cada departamental, se está gestionando la compra de unidades externas y disponer de un trabajador para la capacitación para realizar los Back-ups.
- Conforme a las evidencias suministradas por la Unidad de Tics el último Back-up realizado a los equipos de la departamental Vichada corresponden al año 2017
- Se evidenció que no se viene realizando la preparación y entrega de los medios de respaldo correspondientes a un mes de back-up a firma responsable de custodia externa tal como lo indica la Circular 13/2013 de la caja. "Procedimientos de respaldo y restauración de los sistemas de información, datos y Configuraciones.
- .La Unidad de Gestión de Tics manifestó que no existe un plan de afinamiento a las bases de datos de Comcaja, ya que la información almacenada en estas bases de datos se modifica constantemente, permitiendo operaciones como actualización, borrado, edición de datos y consulta, se tratan los log de transacciones únicamente cuando un dato o consulta fue errado.

Es importante definir e implementar procedimientos de respaldo y restauración de los sistemas, datos y configuraciones que estén alineados con los requerimientos y el plan de continuidad de negocio.

Oportunidad de Mejora

Actualizar por parte del área la Política de respaldo y restauración de los sistemas de

información, datos y configuraciones. La política debe incluir:

- Diagrama del proceso de back-up actualizado.
- Diagrama del proceso de restauración de copias de respaldo actualizado.
- Componentes y Programación Copias de Respaldo (Back-ups) actualizado.
- Formatos de control de back- up actualizado.
- Definir la metodología para la custodia de documentación digital (custodia de los archivos online, custodia de los archivos offline y/o Empresa especialista en la custodia de documentación esencial entre otros) y diversificar los riesgos como estrategia de back- up.

3.1.2. GESTIÓN DEL INVENTARIO UNIDAD DE TICS

3.1.3. Verificación de Inventario (Equipos de Cómputo, Tecnológicos, Software)

Para efectos de la auditoría se realizó la verificación del inventario a cargo de la Unidad de Gestión de Tics haciendo énfasis en los elemento tipo: Servidores, UPS, Switches, Computadores portátiles, Rack, Video beam, Router, Impresora, Multifuncional. A continuación se relaciona lo observado en esta verificación, describiendo la ubicación y estado de cada elemento:

No.	AREA	No de placa	DESCRIPCION	observación de auditoria
1	TIC	007880	UPS	Ubicación: Sexto (6) piso. Estado: en Uso UPS del rack.
2	TIC	007881	SWITCH	Ubicación: Sexto (6) Piso - Oficina de Tics Estado: En uso
3	TIC	007879	COMPUTADOR PORTATIL	Ubicación: Sexto (6) piso - Oficina Tics Estado: en Buen Estado - no está en Uso.
4	TIC	007715	RACK	Ubicación: Centro de Computo Estado: en Uso
5	TIC	007721	SWITCH	Ubicación: Sexto (6) Piso - Oficina de Tics Estado: Bueno en Desuso
6	TIC	007785	SWITCH	Ubicación: Sexto (6) piso - Bodega Tics **Estado: en Mal Estado - para dar de baja.**
7	TIC	007718	SWITCH	Ubicación: Sexto (6) Piso - Oficina de Tics Estado: En uso
8	TIC	007579	VIDEOBEAM	Ubicación: Sexto (6) piso - Bodega Tics **Estado: en Mal Estado - para dar de baja.**
9	TIC	007639	COMPUTADOR PORTATIL	Ubicación: Sexto (6) piso - Bodega Tics **Estado: en Mal Estado - Pendiente dar de baja.**
10	TIC	008102	SWITCH	Ubicación: Sexto (6) Piso Estado: en Uso Red del sexto (6) Piso y telefonía IP.
11	TIC	008103	RACK	Ubicación: Sexto (6) piso. Estado: en Uso
12	TIC	008104	SWITCH	Ubicación: Cuarto (4) Piso Estado: en Uso Red del cuarto (4) Piso se actualizó la red el 26 de septiembre de 2018.
13	TIC	008105	RACK	Ubicación: Cuarto (4) piso. Estado: en Uso telefonía e Internet)
14	TIC	008106	SWITCH	1. Entregado a departamental Guaviare memorando 20172400001393 fecha: 20 de enero de 2017 2. Ubicación: Sexto (6) Piso - Oficina de Tics Estado: Bueno en desuso Actualmente
15	TIC	008107	RACK	entregado a departamental Guaviare memorando 20172400001393 fecha: 20 de enero de 2017 **Documento con sello de recibido**
16	TIC	007293	ROUTER	Ubicación: Sexto (6) piso - Bodega Tics **Estado: en Mal Estado - para dar de baja.**
17	TIC	007498	RACK	Ubicación: Sexto (6) piso - Bodega Tics **Estado: en Mal Estado - para dar de baja.**
18	TIC	007529	IMPRESORA	Ubicación: Sexto (6) piso - Bodega Tics **Estado: en Mal Estado - para dar de baja.**
19	TIC	007560	ROUTER	Ubicación: Sexto (6) Piso - Oficina de Tics

COMCAJA
CAJA DE COMPENSACION FAMILIAR CAMPESINA

				Estado: En uso
20	TIC	007566	ROUTER	Ubicación: Sexto (6) piso - Bodega Tics **Estado: en Mal Estado - para dar de baja.**
21	TIC	006893	UPS	Ubicación: Sexto (6) piso - Bodega Tics **Estado: en Mal Estado - para dar de baja.**
22	TIC	006558	RACK	Ubicación: Tercer (3) Piso - oficina de correspondencia. Estado: en Uso Red del tercer (3) Piso.
23	TIC	005209	MONITOR	Ubicación: Centro de Computo Estado: en Uso
24	TIC	005218	CPU	Ubicación: centro de cómputo Según lo informado por el profesional Felipe Rodriguez equipo destinado x pruebas.
25	TIC	005240	IMPRESORA	Pendiente Ubicación
26	TIC	005244	MULTIFUNCIONAL	Ubicación: Sexto (6) piso - Bodega Tics **Estado: en Mal Estado - para dar de baja.**
27	TIC	005500	MONITOR	Ubicación: Centro de Computo Estado: en Uso Equipos de pruebas.
28	TIC	005509	SERVIDOR	Ubicación: Sexto (6) piso - Oficina Tics **Estado: en Mal Estado - para dar de baja.**
29	TIC	005512	VIDEOBEAM	Ubicación: Sexto (6) piso - Bodega Tics **Estado: en Mal Estado - para dar de baja.**
30	TIC	005516	VIDEOBEAM	Ubicación; Sexto (6) piso - Bodega Tics **Estado: en Mal Estado - para dar de baja.**
31	TIC	005518	COMPUTADOR PORTATIL	Ubicación: Sexto (6) piso - Oficina Tics **Estado: en Mal Estado - para dar de baja.**
32	TIC	005519	ROUTER	Ubicación: Quinto (5) piso - oficina UGA Estado: en Uso.
33	TIC	005527	SWITCH	Ubicación: Sexto (6) Piso - Oficina de Tics Estado: En uso
34	TIC	005538	ROUTER	pendiente ubicación
35	TIC	005540	ROUTER	Ubicación: Sexto (6) Piso - Oficina de Tics Estado: En uso
36	TIC	004908	MULTIFUNCIONAL	Ubicación: Sexto (6) Piso - Oficina de Tics Estado: En uso
37	TIC	004909	COMPUTADOR PORTATIL	Ubicación: Sexto (6) piso - Bodega Tics **Estado: en Mal Estado - Pendiente dar de baja.**
38	TIC	004931	VIDEOBEAM	Ubicación: Sexto (6) piso - Bodega Tics **Estado: en Mal Estado - para dar de baja.**
39	TIC	004966	COMPUTADOR PORTATIL	Ubicación: Sexto (6) piso - Bodega Tics **Estado: en Mal Estado - Pendiente dar de baja.**
40	TIC	005065	COMPUTADOR PORTATIL	1. Se retira equipo a líder Andres Molina 02 de febrero de 2018. 2. Ubicación: Sexto (6) piso - Oficina Tics Estado: en Buen Estado - no está en Uso. Actualmente
41	TIC	005096	IMPRESORA DE PUNTO	Ubicación: Sexto (6) Piso - Oficina de Tics Estado: En uso
42	TIC	005145	CPU	Ubicación: Centro de Computo Estado: en Uso como Servidor de Intranet
43	TIC	004701	CPU	Ubicación: Centro de Computo Estado: en Uso Equipos de pruebas.
44	TIC	004770	CPU	Ubicación: Centro de Computo Estado: en Uso Equipos de pruebas.
45	TIC	004774	COMPUTADOR PORTATIL	Ubicación: Sexto (6) piso - Oficina Tics **Estado: en Mal Estado - Pendiente dar de baja.**
46	TIC	004776	COMPUTADOR PORTATIL	Ubicación: Sexto (6) piso - Oficina Tics Estado: en Buen Estado - no está en Uso.
47	TIC	003814	MONITOR	Se retira equipo a Profesional Martha Quiroga 08 de Junio de 2018.
48	TIC	003884	RACK	Ubicación: Centro de Computo Estado: en Uso
49	TIC	003888	RACK	Ubicación: Centro de Computo Estado: en Uso telefonía e Internet Conmutador, Router de los proveedores.
50	TIC	003889	RACK	Ubicación: Centro de Computo Estado: en Uso Principal Servidores y Switches administradores
51	TIC	003890	SWITCH	Ubicación: Centro de Computo Estado: en Uso

COMCAJA
CAJA DE COMPENSACION FAMILIAR CAMPESINA

				Administrador de todos los Switches
52	TIC	003891	SWITCH	Ubicación: Sexto (6) Piso - Oficina de Tics Estado: Bueno en uso para pruebas
53	TIC	003893	SERVIDOR	Ubicación: Centro de Computo **Estado: en Desuso** **pendiente baja**
54	TIC	003894	SERVIDOR	Ubicación: Centro de Computo Estado: en Uso
55	TIC	003895	SERVIDOR	Ubicación: Sexto (6) piso - Oficina Tics **Estado: en Mal Estado - para dar de baja.**
56	TIC	003896	SERVIDOR	Ubicación: Centro de Computo Estado: en Uso Aplicativo SISU.
57	TIC	003897	COMPARTIDOR DE DISPOSITIVOS	ubicado en el centro de cómputo se conectan cuatro (4) equipos
58	TIC	003898	UPS	Ubicación: Centro de Computo Estado: en Uso
59	TIC	003971	CPU	Ubicación: Centro de Computo Estado: en Desuso equipo funciona
60	TIC	004544	SERVIDOR	Ubicación: Sexto (6) piso - Oficina Tics **Estado: en Mal Estado - para dar de baja.**
61	TIC	004585	SERVIDOR	Ubicación: Centro de Computo Estado: en Uso La carpeta compartida Servidor Back ups
62	TIC	004586	SERVIDOR	Ubicación: Sexto (6) piso - Oficina Tics **Estado: en Mal Estado - para dar de baja.**
63	TIC	004587	SERVIDOR	Ubicación: Sexto (6) piso - Oficina Tics **Estado: en Mal Estado - para dar de baja.**
64	TIC	004588	SERVIDOR	Ubicación: Sexto (6) piso - Oficina Tics **Estado: en Mal Estado - para dar de baja.**
65	TIC	004589	SERVIDOR	Ubicación: Sexto (6) piso - Oficina Tics **Estado: en Mal Estado - para dar de baja.**
66	TIC	004590	COMPARTIDOR DE DISPOSITIVOS	ubicado en el centro de cómputo se conectan cuatro (4) equipos
67	TIC	003623	COMPUTADOR PORTATIL	Ubicación: Quinto (5) piso - Oficina UGA Estado: en Buen Estado - en préstamo a auxiliar Lucia de la Unidad de Gestión Administrativa. **No se evidenció soporte del préstamo de equipo a la trabajadora.**
68	TIC	003635	MONITOR	Se retira a Lizeth Hernández Formato - Entrega de elementos devolutivos de inventario responsable fecha: 08 de Junio de 2018.
69	TIC	003392	CPU	Ubicación: Centro de Computo Estado: en Uso Equipos de pruebas.
70	TIC	003394	MONITOR	Se retira equipo a Jose Luis Díaz 29 de Enero de 2018.
71	TIC	003397	MULTIFUNCIONAL	Ubicación: Sexto (6) piso - Bodega Tics **Estado: pendiente confirmar dar de baja.**
72	TIC	003428	COMPUTADOR PORTATIL	Ubicación: Sexto (6) piso - Bodega Tics **Estado: en Mal Estado - Pendiente dar de baja.**
73	TIC	003437	COMPUTADOR PORTATIL	Ubicación: Sexto (6) piso - Oficina Tics Estado: en Buen Estado - no está en Uso.
74	TIC	003652	COMPUTADOR PORTATIL	Ubicación: Sexto (6) piso - Oficina Tics Estado: en Buen Estado - no está en Uso.
75	TIC	004745	COMPUTADOR PORTATIL	Ubicación: Sexto (6) piso - Oficina Tics Estado: en Buen Estado - no está en Uso.
76	TIC	007839	DISCO DURO EXTERNO	Ubicación: Sexto (6) piso - Bodega Tics **Estado: en Mal Estado - para dar de baja.**
77	TIC	001703	CPU	Ubicación: Centro de Computo Estado: en Uso Equipos de pruebas.
78	TIC	001754	COMPUTADOR PORTATIL	Ubicación: Sexto (6) piso - Bodega Tics **Estado: en Mal Estado - Pendiente dar de baja.**
79	TIC	000232	COMPUTADOR PORTATIL	Ubicación: Sexto (6) piso - Oficina Tics Estado: en Buen Estado - no está en Uso.
80	TIC	000020	SCANNER	Ubicación: Sexto (6) piso - Bodega Tics **Estado: en Mal Estado - Pendiente dar de baja.**
81	TIC	003943	MONITOR	Se retira a ingeniero Luis Antonio Bernal Formato - Entrega de elementos devolutivos de inventario responsable

				fecha: 18 de Junio de 2018.
82	TIC	003885	PLANTA TELEFONICA	Ubicación: Centro de Computo Estado: en Uso
83	CARLOS ALIRIO NARANJO	008113	CPU	Ubicación: Centro de cómputo **Según lo informado por el analista Felipe Rodriguez de la Unidad de Tics corresponde al servidor del FIREWALL de la Caja.** **Según el inventario de elementos de la Caja suministrado por la Unidad de gestión administrativa el elemento se encuentra pendiente de dar de baja.**

3.1.4. Verificación compra de equipos de cómputo y tecnológicos

Para efectos de auditoria se evidenció contablemente la compra de equipos de cómputo y de tecnología los cuales fueron utilizados para cambiar dichos equipo en las (4) Departamentales y parte del Nivel central, en la siguiente tabla y en la casilla "observación de auditoria" se describe a quien fue entregado el elemento, con qué documento o formato y si se observó alguna novedad:

No.	No de placa	DESCRIPCION	observación de auditoria
1	009433	COMPUTADOR AIO	entregado a departamental Guaviare a través de memorando sin número de radicado fecha: 05 de Junio de 2017 **Documento con firma de recibido**
2	009434	COMPUTADOR AIO	entregado a departamental Guaviare a través de memorando sin número de radicado fecha: 05 de Junio de 2017 **Documento con firma de recibido**
3	009435	COMPUTADOR AIO	entregado a departamental Guaviare a través de memorando sin número de radicado fecha: 05 de Junio de 2017 **Documento con firma de recibido**
4	009436	COMPUTADOR AIO	entregado a departamental Guaviare a través de memorando sin número de radicado fecha: 05 de Junio de 2017 **Documento con firma de recibido**
5	009437	COMPUTADOR AIO	entregado a departamental Guaviare a través de memorando sin número de radicado fecha: 05 de Junio de 2017 **Documento con firma de recibido**
6	009438	COMPUTADOR AIO	entregado a departamental Guaviare a través de memorando sin número de radicado fecha: 05 de Junio de 2017 **Documento con firma de recibido**
7	009439	COMPUTADOR AIO	Entregado a departamental Guainía a través de memorando sin número de radicado fecha: 31 de Mayo de 2017 **Se observa certificación de recibo a satisfacción del jefe departamental con fecha del 06 de junio de 2017.**
8	009440	COMPUTADOR AIO	Entregado a departamental Guainía a través de memorando sin número de radicado fecha: 31 de Mayo de 2017 **Se observa certificación de recibo a satisfacción del jefe departamental con fecha del 06 de junio de 2017.**
9	009441	COMPUTADOR AIO	Entregado a departamental Guainía a través de memorando sin número de radicado fecha: 31 de Mayo de 2017 **Se observa certificación de recibo a satisfacción del jefe departamental con fecha del 06 de junio de 2017.**
10	009442	COMPUTADOR AIO	No se evidenció soporte de entrega de computador AIO a la departamental. **Según lo informado por la Unidad de Tics está en trámite el envío del mencionado soporte por parte de la Jefe de departamental.**
11	009443	COMPUTADOR AIO	No se evidenció soporte de entrega de computador AIO a la departamental. **Según lo informado por la Unidad de Tics está en trámite el envío del mencionado soporte por parte de la Jefe de departamental.**

COMCAJA
CAJA DE COMPENSACION FAMILIAR CAMPESINA

12	009444	COMPUTADOR AIO	No se evidenció soporte de entrega de computador AIO a la departamental. **Según lo informado por la Unidad de Tics está en trámite el envío del mencionado soporte por parte de la Jefe de departamental.**
13	009445	COMPUTADOR AIO	No se evidenció soporte de entrega de computador AIO a la departamental. **Según lo informado por la Unidad de Tics está en trámite el envío del mencionado soporte por parte de la Jefe de departamental.**
14	009446	COMPUTADOR AIO	entregado a departamental vichada a través de memorando sin número de radicado fecha: 06 de Junio de 2017 **Documento con sello de recibido**
15	009447	COMPUTADOR AIO	entregado a departamental vichada a través de memorando sin número de radicado fecha: 06 de Junio de 2017 **Documento con sello de recibido**
16	009448	COMPUTADOR AIO	entregado a departamental vichada a través de memorando sin número de radicado fecha: 06 de Junio de 2017 **Documento con sello de recibido**
17	009449	COMPUTADOR AIO	entregado a departamental vichada a través de memorando sin número de radicado fecha: 06 de Junio de 2017 **Documento con sello de recibido**
18	009450	COMPUTADOR AIO	1. Entregado a departamental vichada (La Primavera) memorando con número de radicado 20172400020523 fecha: 08 de Septiembre de 2017 2. Posteriormente entregado a Martha Gacha Formato - Entrega de elementos devolutivos de inventario responsable fecha: 03 de Agosto de 2018.
19	009452	COMPUTADOR AIO	Entregado a Jose Luis Díaz Formato - Entrega de elementos devolutivos de inventario responsable fecha: 29 de Enero de 2018.
20	009453	COMPUTADOR AIO	Entregado a Martha Quiroga Formato - Entrega de elementos devolutivos de inventario responsable fecha: 08 de Junio de 2018.
21	009454	COMPUTADOR AIO	Entregado a Lizeth Hernández Formato - Entrega de elementos devolutivos de inventario responsable fecha: 08 de Junio de 2018. Se retira monitor placa 3635 y CPU placa 3634.
22	009451	COMPUTADOR AIO	Entregado a departamental Guaviare memorando con número de radicado 20172400019753 fecha: 29 de Agosto de 2017 **Documento sin firma de recibido**
23	009185	Computador HP Pro 400G1 AIO	Entregado a Alba Adriana Avila en el año 2016, no hay registro y/o soporte de entrega de esta fecha en la Unidad de Tics y en la Unidad de Gestión Administrativa. **En el transcurso de la auditoría, la Unidad de las Tics diligencia el Formato "Entrega de elementos devolutivos de inventario responsable" tomando la firma de quien entrega y quien recibe.** **Fecha: 03 de Octubre de 2018.**
24	009186	Computador HP Pro 400G1 AIO	Entregado a Luz Andrea Ardila Labrador en el año 2016, no hay registro y/o soporte de entrega de esta fecha en la Unidad de Tics y en la Unidad de Gestión Administrativa. **En el transcurso de la auditoría, la Unidad de las Tics diligencia el Formato "Entrega de elementos devolutivos de inventario responsable" tomando la firma de quien entrega y quien recibe.** **Fecha: 17 de Octubre de 2018.**
25	009187	Computador HP Pro 400G1 AIO	Entregado a Armando Arévalo Linares en el año 2016, no hay registro y/o soporte de entrega de esta fecha en la Unidad de Tics y en la Unidad de Gestión Administrativa. **En el transcurso de la auditoría, la Unidad de las Tics diligencia el Formato "Entrega de elementos devolutivos de inventario responsable" tomando la firma de quien entrega y quien recibe.** **Fecha: 17 de Octubre de 2018.**
26	009489	COMPUTADOR PORTATIL	entregado a departamental Vichada memorando con número de radicado 2018240000023 fecha: 03 de Enero de 2018 **Documento sin firma de recibido**
27	009490	COMPUTADOR PORTATIL	entregado a departamental Vaupés memorando con número de radicado 2018240000043 fecha: 03 de Enero de 2018 **Documento sin firma de recibido**
28	009491	COMPUTADOR	entregado a departamental Guainía memorando con número de

COMCAJA
CAJA DE COMPENSACION FAMILIAR CAMPESINA

		PORTATIL	radicado 2018240000053 fecha: 03 de Enero de 2018 **Documento sin firma de recibido**
29	009492	COMPUTADOR PORTATIL	entregado a departamental Guaviare memorando con número de radicado 2018240000063 fecha: 03 de Enero de 2018 **Documento sin firma de recibido**
30	009496	COMPUTADOR PORTATIL	Entregado a Líder Andres Molina Formato - Entrega de elementos devolutivos de inventario responsable fecha: 02 de Febrero de 2018.
31	009457	MULTIFUNCIONAL	Entregado a departamental Guaviare memorando con número de radicado 20172400019753 fecha: 29 de Agosto de 2017 **Documento con sello de recibido y recibo a satisfacción de la Jefe departamental 21 de Septiembre de 2018.**
32	009455	COMPUTADOR AIO	Entregado a ingeniero Luis Antonio Bernal Formato - Entrega de elementos devolutivos de inventario responsable fecha: 18 de Junio de 2018. Se retira monitor placa 3943 y CPU placa 4676.
33	009493	COMPUTADOR PORTATIL	Ubicación: Sexto (6) piso Oficina del Ingeniero Carlos Naranjo Estado: Sin estrenar, Bueno
34	009494	COMPUTADOR PORTATIL	entregado a la Vanessa Soto Bejarano a través de memorando sin número de radicado fecha: 17 de Agosto de 2018 **Documento sin firma de recibido**
35	009495	COMPUTADOR PORTATIL	entregado a Jefe departamental vichada memorando con numero de radicado 20182400013023 fecha: 07 de Junio de 2017 **Documento sin firma de recibido**
36	009497	COMPUTADOR PORTATIL	Ubicación: Sexto (6) piso Oficina del Ingeniero Carlos Naranjo Estado: Sin estrenar. Bueno **No tiene placa física.**
37	009498	COMPUTADOR PORTATIL	Ubicación: Sexto (6) piso Oficina del Ingeniero Carlos Naranjo Estado: En Uso **No tiene placa física.**
38	009499	SERVIDOR DL380	Ubicación: Centro de Computo Estado: en Uso - Bueno Virtualización- Servidor Aplicativos Sysman, SISU, Orfeo.
39	009500	SERVIDOR DL380	Ubicación: Centro de Computo Estado: en Uso Servidor
40	009501	SERVIDOR DL180	Ubicación: Centro de Computo Estado: en Uso Servidor
41	009502	USB EXTERNA DE DVDRW	Ubicación: Sexto (6) piso Oficina Tics Estado: En Uso. Bueno **No tiene placa física.**

A continuación se resumen las compras realizadas de equipos de cómputo detallándolo, por descripción, cantidad, valor, fecha de comprar y detalle de entrega:

DESCRIPCIÓN	CANTIDAD	VALOR TOTAL	observación de auditoria
COMPUTADOR AIO	23	$ 44.827.000,00	• Compra realizada el 17 de mayo de 2017 proveedor ALKOSTO S. A. • Se entregaron así: 7 a la departamental Guaviare, 3 a la departamental Guainía, 5 a las departamental Vichada, 4 a la departamental Vaupés, 1 a la Unidad misional de servicios, 1 a la Unidad de Tics y 2 al Departamento de subsidio familiar
Computador HP Pro 400	3	$ 6.999.999,00	• Compra realizada el 25 de agosto de 2016 proveedor DISCOVERY ENTERPRISE BUSINES S.A.S. • Se entregaron a los trabajadores de la Sección de Presupuesto y tesorería.

COMPUTADOR PORTATIL	10	$ 12.990.000,00	• Compra realizada el 24 de Noviembre de 2017 proveedor ALKOSTO S. A. • Se entregaron así: 1 a la departamental Guaviare, 1 a la departamental Guainía, 1 a las departamental Vichada, 1 a la departamental Vaupés, 1 a la Unidad de Planeación y 5 a la Unidad de Tics.
MULTIFUNCIONAL	3	$ 1.887.000,00	• Compra realizada el 17 de Agosto de 2017 proveedor ALKOSTO S. A. • Se entregaron así: 1 a la departamental Guaviare, 1 a las departamental Vichada, 1 a la Unidad Misional de servicios.
SERVIDOR PROLIANT DL180 Y DL 380	3	$ 78.799.706,00	• Compra realizada el 28 de diciembre de 2017 proveedor H&C SOLUCIONES INFORMATICAS DE COLOMBIA SAS. • Se evidenció que su ubicación es el centro de cómputo en el Nivel central su uso es para la Virtualización Aplicativos Sysman, SISU, Orfeo.
USB EXTERNA DE DVDRW	1	$ 533.751,00	• 1. Compra realizada el 28 de diciembre de 2017 proveedor H&C SOLUCIONES INFORMATICAS DE COLOMBIA SAS. • Se evidenció que su ubicación es la Oficina Tics en el Nivel central y está en uso.
Total general	43	$ 146.037.456,00	

Situación Observada No. 2	Gestionar el Inventario a cargo de la Unidad de Tics	**OM**	**X**
		D	**X**

Descripción de la Situación Observada

Conforme la verificación realizada en esta auditoría al inventario a cargo de la unidad de observaron novedades están pendientes de gestionar con la Unidad de Gestión administrativa, tales como:

- Se evidenciaron elementos de inventario que están en mal estado y/o en desuso los cuales están pendientes por dar de baja.
- No se observaron soportes de solicitudes de baja realizadas a la Unidad de gestión administrativa de los equipos de cómputo, portátiles y servidores y demás elementos de inventario que se encuentran en desuso y/o mal estado. Según lo validado con la Unidad de Gestión de Tics, a partir del mes de septiembre del año 2018 se comenzó el proceso de control de movimientos de inventario y elementos de desuso y/o mal estado. A la fecha de auditoría dicho proceso continúa en gestión debido a la observancia de algunos elementos faltantes y novedades presentadas.
- El área no cuenta con fichas técnicas – hojas de vida actualizadas de los equipos de cómputo que describan las especificaciones técnicas del hardware, software instalado, conectividad mantenimientos físicos y de software, entre otras.
- En casos puntuales y descritos en la revisión de auditoría, se observó que los soportes de entrega de los elementos de cómputo y/o tecnología no se encontraban diligenciados y/o con firma de recibido por parte de quien recibe.
- Al momento de la auditoria y según lo manifestado por la Unidad de Tics no se cuenta con soporte de mantenimientos realizados al hardware de la Caja en las vigencias 2017 y 2018, está en proceso de gestión por parte del área.

- Se observó la renovación de los equipos de cómputo de las cuatro departamentales y parcialmente en el Nivel Central, dicho proceso se llevó a cabo en el transcurso de los años 2017 y 2018.

Contar con un inventario actualizado permite conocer en tiempo real la infraestructura, agilizar la toma de decisiones sobre los equipos y automatizar cambios de manera más eficiente en la Caja.

Oportunidad de Mejora

- Mantener el inventario de elementos de la Unidad actualizado, gestionando continuamente las novedades presentadas con sus respectivos soportes y formatos diligenciados.
- Dar trámite a los procesos de baja de activos del inventario de la Unidad de los elementos que se encuentran en mal estado y/o en desuso, conforme la competencia de la Unidad de Gestión de Tics.
- Levantar Inventario y/o fichas técnicas – hojas de vida de los servidores y equipos de cómputo que describan las especificaciones técnicas del hardware, software instalado, conectividad mantenimientos físicos y de software, entre otras. como una herramienta de control y seguimiento de los equipos.
- Adelantar proceso de mantenimiento de hardware conforme a lo establecido en los procesos y procedimientos vigentes de la caja.

Situación Observada No. 3	Carencia de una Política para la Gestión e Inventario de software Autorizado y no Autorizado	**OM**	**X**
		D	**X**

Descripción de la Situación Observada

No existe una gestión activa de software donde se pueda observar un inventario, seguimiento y corrección de software, de tal manera que solo software autorizado pueda ejecutarse. Se evidencio Sistemas Operativos desactualizados y sin soporte por el fabricante. "**Ver Sección 3 Informe Técnico**"

Los dispositivos poco controlados tienen más posibilidades de ejecutar software innecesario desde el punto de vista de negocio (introduciendo posibles fallas de seguridad) o de ejecutar software malicioso introducido por un atacante después de que un sistema se vea comprometido.

Oportunidad de Mejora

Definir por parte del área que corresponda una **Política de Inventario de Software Autorizado,** donde se incluya:

- Mantener un inventario de software autorizado
- Verificar soporte de fabricante para Software gestionado en la organización.
- Solución para el inventario de software.
- Gestión de software no aprobado.

COMCAJA
CAJA DE COMPENSACION FAMILIAR CAMPESINA

3.2. EVALUACIÓN DE POLÍTICAS Y PLANES DE SEGURIDAD INFORMÁTICA

Situación Observada No. 4	Carencia de una Política para la Gestión administración de Vulnerabilidades	**OM**	**X**
		D	**X**

Descripción de la Situación Observada

No se tiene una Política ni proceso para la **Gestión de Vulnerabilidades.** *Evaluar y tomar medidas continuamente sobre nueva información para identificar vulnerabilidades, remediar y minimizar la ventana de oportunidad para los atacantes.* **Ver Sección 1 Informe Técnico**"

Las organizaciones que no buscan vulnerabilidades y abordan de manera proactiva las fallas detectadas se enfrentan una probabilidad significativa de que sus sistemas informáticos se vean comprometidos

Oportunidad de Mejora

Definir por parte del área que corresponda una **Política y un Proceso para la gestión y administración de vulnerabilidades,** donde se incluya:

- Proceso de gestión de activos.
- Proceso de gestión de riesgo.
- Proceso de gestión de vulnerabilidades
- Proceso para gestión automatizada de parches en Sistema operativo Software.
- Llevar a cabo por lo menos tres veces al año pruebas de vulnerabilidades a los activos de información

Situación Observada No. 5	Definir una Política para la Protección del correo electrónico	**OM**	**X**
		D	**X**

Descripción de la Situación Observada

No se tiene una Política ni proceso para la protección de correo electrónico.

Los navegadores web y los clientes de correo electrónico son puntos de entrada para ataque muy comunes debido a su complejidad técnica, flexibilidad y su interacción directa con los usuarios y con los otros sistemas y sitios web. En la actualidad se puede llevar a cabo suplantación de correo electrónico.
"Ver Seccion2 Informe Técnico"

Oportunidad de Mejora

Definir por parte del área que corresponda una **Política y un Proceso para la protección del correo electrónico la cual contenga**

- Utilizar Servicio de filtrado de DNS
- Implementar Dmark y habilitar la verificación por parte del receptor
- Bloquear tipo de archivos innecesarios.

COMCAJA
CAJA DE COMPENSACION FAMILIAR CAMPESINA

Situación Observada No. 6	Definir una Política de seguridad para limitar y controlar los puertos de red, protocolos y servicios.	**OM**	**X**
		D	**X**

Descripción de la Situación Observada

No se tiene una Política ni procedimiento para administrar el uso operacional continuo de puertos, protocolos y servicios, con el objetivo de minimizar la exposición a amenazas, vulnerabilidades.

Los atacantes buscan servicios de red remotamente accesibles que sean vulnerables a la explotación
"Ver Seccion2 Informe Técnico"

Oportunidad de Mejora

Definir por parte del área que corresponda una **Política para limitar y controlar los puertos de red, protocolos y servicios.** La política debe incluir:

- Asociar al inventario de activos la lista de puertos, servicios y protocolos
- Asegurar que solo protocolos, servicios y puertos permitidos se estén ejecutando
- Realizar regularmente escaneos de puertos en la red.

Situación Observada No. 7	Definir una Política de cambio de contraseña e implementación del doble factor de autenticación	**OM**	**X**
		D	**X**

Descripción de la Situación Observada

No se evidencia una Política para el cambio de contraseña

El no tener definido una política de contraseñas ni un doble factor de autenticación, hace que la probabilidad de sufrir ataques de fuerza bruta sea mayor. **Ver Seccion2 Informe Técnico"**

Oportunidad de Mejora

Definir por parte del área que corresponda una Política para el cambio de contraseñas y si se puede implementar un doble factor de autenticación, la política debe contener:

- Tiempo de caducidad de contraseña
- Longitud mínima de 10 caracteres (números, letras, caracteres especiales).
- Se debe tener un histórico de máximo tres contraseñas, ósea no podrá repetir la contraseña hasta el tercer cambio.
- Como mínimo se debe implementar a usuarios administradores de infraestructura el doble factor de autenticación.

Situación Observada No. 8	Implementar un programa de concienciación y entrenamiento de seguridad.	**OM**	**X**
		D	**X**

Descripción de la Situación Observada

No se cuenta con un proceso de capacitación y concienciación de usuarios.

Riesgos

El método más efectivo que utilizan los Ciber delincuentes ha sido el factor humano, ya que a través de campañas de phishing y engaños a los usuarios se ha logrado vulnerar cientos de empresas. ,

Oportunidad de Mejora

Definir por parte del área que corresponda un proceso, donde se brinde cursos y charlas de concienciación de los usuarios.

4. RIESGOS Y CONTROLES

En el año 2018 la Unidad de Gestión de Tics no reportó a la Unidad de Control Interno la presencia de nuevos riesgos y controles en sus procesos.

5. SEGUIMIENTO PLAN DE MEJORAMIENTO DE LA SUPERINTENDENCIA DEL SUBSIDIO FAMILIAR

Al momento de la auditoria la Unidad de Gestión de Tics no tenía hallazgos pendientes o en ejecución con la Superintendencia de subsidio familiar.

6. SEGUIMIENTO RECOMENDACIONES DE LA REVISORIA FISCAL

Al momento de la auditoria la Unidad de Gestión de Tics no tenía hallazgos pendientes o en ejecución con la revisoría fiscal.

7. SEGUIMIENTO RECOMENDACIONES DE LA AUDITORÍA ANTERIOR

Al momento de la auditoria el ingeniero Carlos Naranjo Líder de la Unidad de Gestión de Tics dio cierre en el formato establecido a las acciones de mejora que tenía en ejecución con la Unidad de Control Interno Corporativo.

8. RECOMENDACIONES DE AUDITORIA

A continuación se relacionan las recomendaciones establecidas en esta auditoría:

8.1. Recomendación de Auditoria No 1:

Se sugiere a la Unidad actualizar la Política de respaldo y restauración de los sistemas de información, datos y configuraciones. La política debe incluir:

- Diagrama del proceso de back-up actualizado.
- Diagrama del proceso de restauración de copias de respaldo actualizado.
- Componentes y Programación Copias de Respaldo (Back-ups) actualizado.
- Formatos de control de back- up actualizado.

- Definir la metodología para la custodia de documentación digital (custodia de los archivos online, custodia de los archivos offline y/o Empresa especialista en la custodia de documentación esencial entre otros) y diversificar los riesgos como estrategia de back-up.

8.2. Recomendación de Auditoria No 2:

Se sugiere a la Unidad de Gestión de Tics fortalecer la Gestión del Inventario a cargo de la Unidad, teniendo en cuenta;

- Mantener el inventario de elementos de la Unidad actualizado, gestionando continuamente las novedades presentadas con sus respectivos soportes y formatos diligenciados.
- Dar trámite a los procesos de baja de activos del inventario de la Unidad de los elementos que se encuentran en mal estado y/o en desuso, conforme la competencia de la Unidad de Gestión de Tics.
- Levantar Inventario y/o fichas técnicas – hojas de vida de los servidores y equipos de cómputo que describan las especificaciones técnicas del hardware, software instalado, conectividad mantenimientos físicos y de software, entre otras. como una herramienta de control y seguimiento de los equipos.
- Adelantar proceso de mantenimiento de hardware conforme a lo establecido en los procesos y procedimientos vigentes de la caja.

8.3. Recomendación de Auditoria No 3:

Se sugiere a la Unidad de Gestión de Tics definir una **Política de Inventario de Software Autorizado,** donde se incluya:

- Mantener un inventario de software autorizado
- Verificar soporte de fabricante para Software gestionado en la organización.
- Solución para el inventario de software.
- Gestión de software no aprobado.

8.4. Recomendación de Auditoria No 4:

Se sugiere a la Unidad de Gestión de Tics definir una **Política y un Proceso para la gestión y administración de vulnerabilidades,** donde se incluya:

- Proceso de gestión de activos.
- Proceso de gestión de riesgo.
- Proceso de gestión de vulnerabilidades
- Proceso para gestión automatizada de parches en Sistema operativo Software.
- Llevar a cabo por lo menos tres veces al año pruebas de vulnerabilidades a los activos de información

8.5. Recomendación de Auditoria No 5:

Se sugiere a la Unidad de Gestión de Tics definir una **Política y un Proceso para la protección del correo electrónico la cual contenga**

- Utilizar Servicio de filtrado de DNS
- Implementar Dmark y habilitar la verificación por parte del receptor
- Bloquear tipo de archivos innecesarios.

8.6. Recomendación de Auditoria No 6:

Se sugiere a la Unidad de Gestión de Tics definir una **Política para limitar y controlar los puertos de red, protocolos y servicios.** La política debe incluir:

- Asociar al inventario de activos la lista de puertos, servicios y protocolos
- Asegurar que solo protocolos, servicios y puertos permitidos se estén ejecutando
- Realizar regularmente escaneos de puertos en la red.

8.7. Recomendación de Auditoria No 7:

Se sugiere a la Unidad de Gestión de Tics definir una Política para el cambio de contraseñas y si se puede implementar un doble factor de autenticación, la política debe contener:

- Tiempo de caducidad de contraseña
- Longitud mínima de 10 caracteres (números, letras, caracteres especiales).
- Se debe tener un histórico de máximo tres contraseñas, ósea no podrá repetir la contraseña hasta el tercer cambio.
- Como mínimo se debe implementar a usuarios administradores de infraestructura el doble factor de autenticación.

8.8. Recomendación de Auditoria No 8:

Se sugiere a la Unidad de Gestión de Tics definir un proceso, donde se brinde cursos y charlas de concienciación de los usuarios.

9. FIRMAS

CARLOS ALIRIO NARANJO AMAYA
Líder Unidad Gestión de Tics

VANESSA SOTO BEJARANO
Líder Unidad de Control Interno Corporativo

JHON JAIRO QUINTERO ALONSO
Profesional Senior I
Unidad de Control Interno Corporativo

COMCAJA
CAJA DE COMPENSACION FAMILIAR CAMPESINA

INFORME TECNICO

1. ALCANCE

1.1 Activos

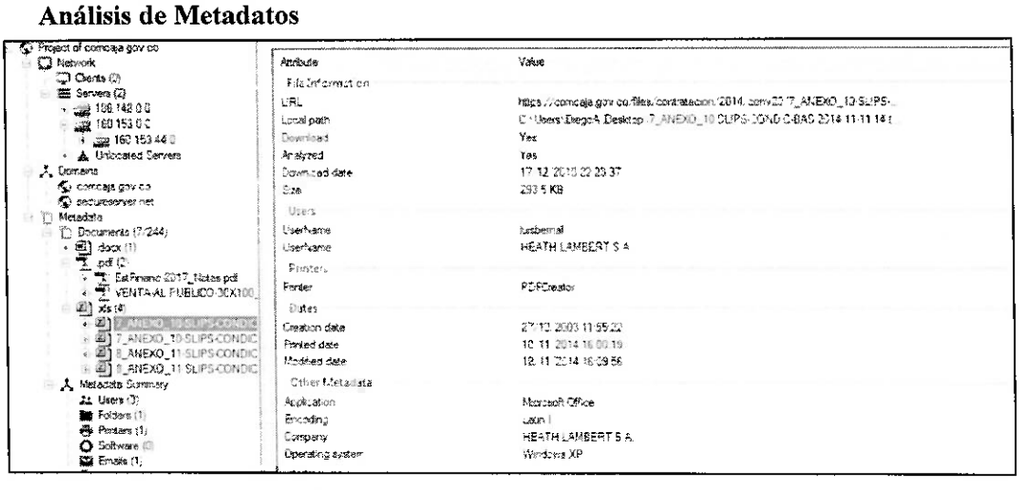
Nombre	Tipo	Dirección
correo.comcaja.gov.co	Host	186.148.191.204

2.*TABLA VULNERABILIDADES ENCONTRADAS POR TIPO Y SEVERIDAD*

Activo	Vulnerabilidad	Severidad (1min - 10 max)
correo.comcaja.gov.co	TLS/SSL Server Supports Anonymous Cipher Suites	5.8
	http-cookie-http-only-flag	5.0
	Missing Secure Flag From SSL Cookie	5.0
	TLS/SSL Birthday attacks on 64-bit block ciphers	5.3
	TLS Server Supports TLS version 1.0	4.3
	TLS/SSL Server is enabling the BEAST attack	4.3
	Click Jacking	4.3
	TLS/SSL Server Supports RC4 Cipher Algorithms	5.9
	TLS Server Supports TLS version 1.1	2.6
	TLS/SSL Server Supports The Use of Static Key Ciphers	2.6
	Diffie-Hellman group smaller than 2048 bits	2.6

2. PUERTOS Y SERVICIOS EXPUESTOS

Análisis de Metadatos



COMCAJA
CAJA DE COMPENSACION FAMILIAR CAMPESINA

Correo.comcaja.gov.co(186.148.191.204)

OS	Servidor
	ip-160-153-44-70.ip
	correo.comcaja.go
	azteca-comunicaci

Puerto	Protocolo	Estado	Servicio	Versión
25	tcp	open	smtp	Postfix smtpd
80	tcp	open	http	
110	tcp	open	pop3	Zimbra Collabration Suite pop3d
113	tcp	closed	ident	
443	tcp	open	http	Zimbra http config
465	tcp	open	smtp	Postfix smtpd
993	tcp	open	imaps	
995	tcp	open	pop3	Zimbra Collabration Suite pop3d
2000	tcp	open	cisco-sccp	
5060	tcp	open	sip	
8008	tcp	open	http	Fortinet FortiGuard block page
8010	tcp	open	http-proxy	FortiGate Web Filtering Service
8080	tcp	closed	http-proxy	
8443	tcp	open	http	Zimbra http config

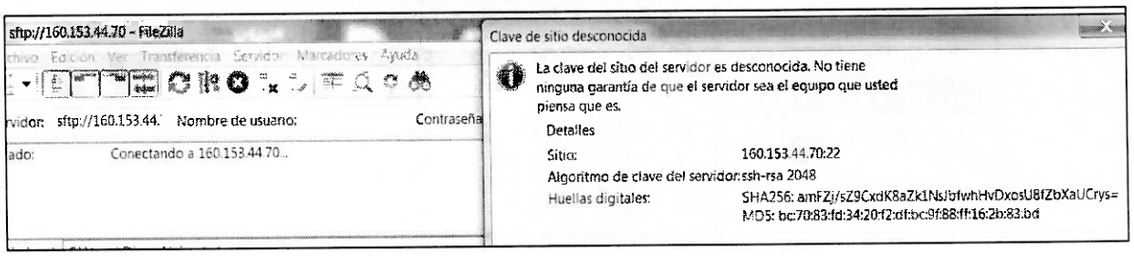
Sitio web comcaja.gov.co

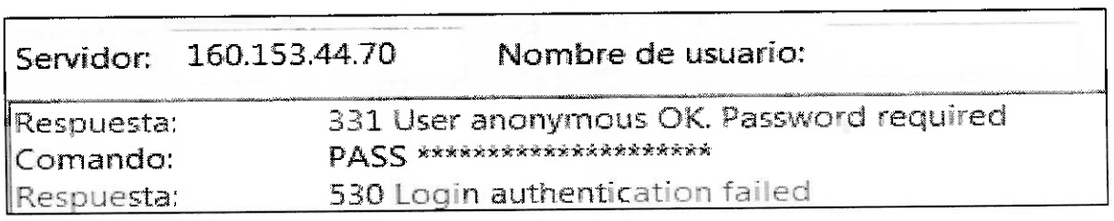
	ip-160-153-44-70.ip
	correo.comcaja.go
	azteca-comunicaci

21	tcp	open	ftp	Pure-FTPd
22	tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
25	tcp	open	smtp	
26	tcp	closed	rsftp	
80	tcp	open	http	
110	tcp	open	pop3	Dovecot pop3d
113	tcp	closed	ident	
143	tcp	open	imap	Dovecot imapd
443	tcp	open	https	
465	tcp	open	smtp	Exim smtpd 4.91
587	tcp	open	smtp	Exim smtpd 4.91
993	tcp	open	imap	Dovecot imapd
995	tcp	open	pop3	Dovecot pop3d
1248	tcp	open	hermes	
2000	tcp	open	cisco-sccp	
3306	tcp	open	mysql	MySQL 5.6.39-cll-lve
5060	tcp	open	sip	
5222	tcp	closed	xmpp-client	
8008	tcp	open	http	Fortinet FortiGuard block page
8010	tcp	open	http-proxy	FortiGate Web Filtering Service

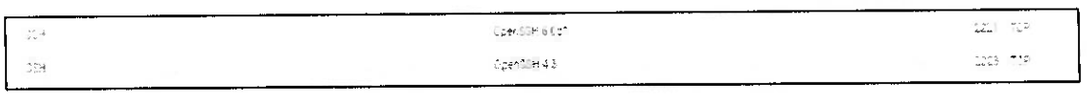
COMCAJA
CAJA DE COMPENSACION FAMILIAR CAMPESINA

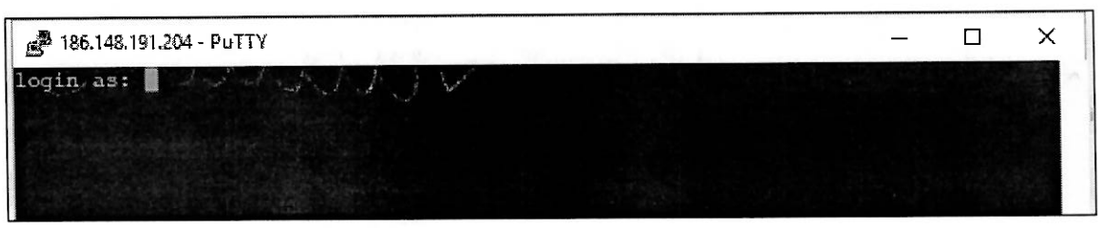
Protocolo Sftp





Protocolo SSH expuesto



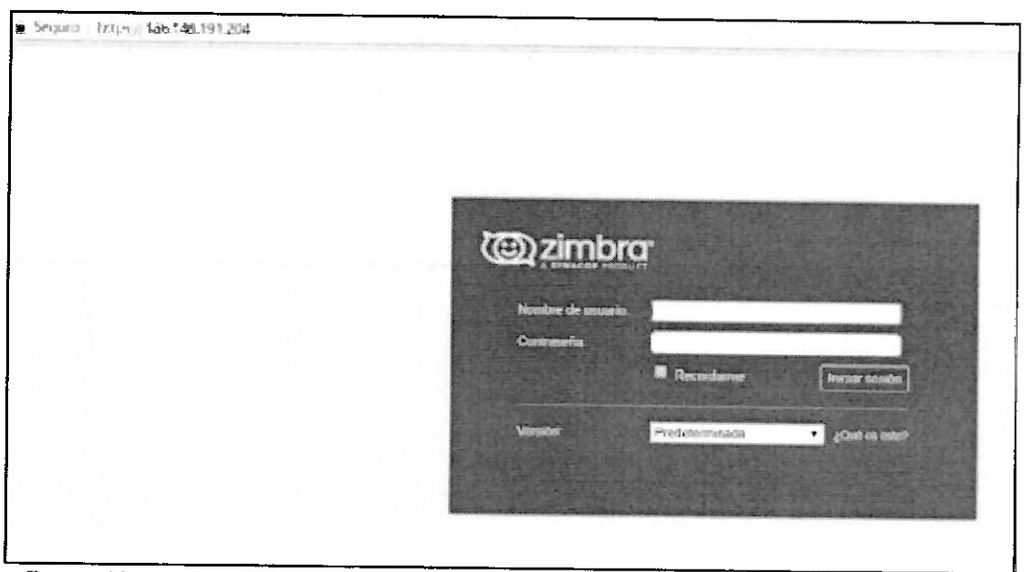


COMCAJA
CAJA DE COMPENSACION FAMILIAR CAMPESINA

```
[-] 186.148.191.204:2221 - SSH - User 'acorn' not found
[-] 186.148.191.204:2221 - SSH - User 'acosmism' not found
[+] 186.148.191.204:2221 - SSH - User 'acosta' found
[+] 186.148.191.204:2221 - SSH - User 'acotyledon' found
[-] 186.148.191.204:2221 - SSH - User 'acoustic' not found
[-] 186.148.191.204:2221 - SSH - User 'acoustician' not found
[-] 186.148.191.204:2221 - SSH - User 'acoustics' not found
[-] 186.148.191.204:2221 - SSH - User 'acquah' not found
[-] 186.148.191.204:2221 - SSH - User 'acquaint' not found
[-] 186.148.191.204:2221 - SSH - User 'acquaintance' not found
[-] 186.148.191.204:2221 - SSH - User 'acquainted' not found
[-] 186.148.191.204:2221 - SSH - User 'acquiesce' not found
[-] 186.148.191.204:2221 - SSH - User 'acquiescence' not found
[-] 186.148.191.204:2221 - SSH - User 'acquiescent' not found
[-] 186.148.191.204:2221 - SSH - User 'acquire' not found
[-] 186.148.191.204:2221 - SSH - User 'acquirement' not found
[-] 186.148.191.204:2221 - SSH - User 'acquisition' not found
[-] 186.148.191.204:2221 - SSH - User 'acquisitive' not found
[-] 186.148.191.204:2221 - SSH - User 'acquit' not found
[-] 186.148.191.204:2221 - SSH - User 'acquittal' not found
[-] 186.148.191.204:2221 - SSH - User 'acquittance' not found
```

Protocolo SMTP

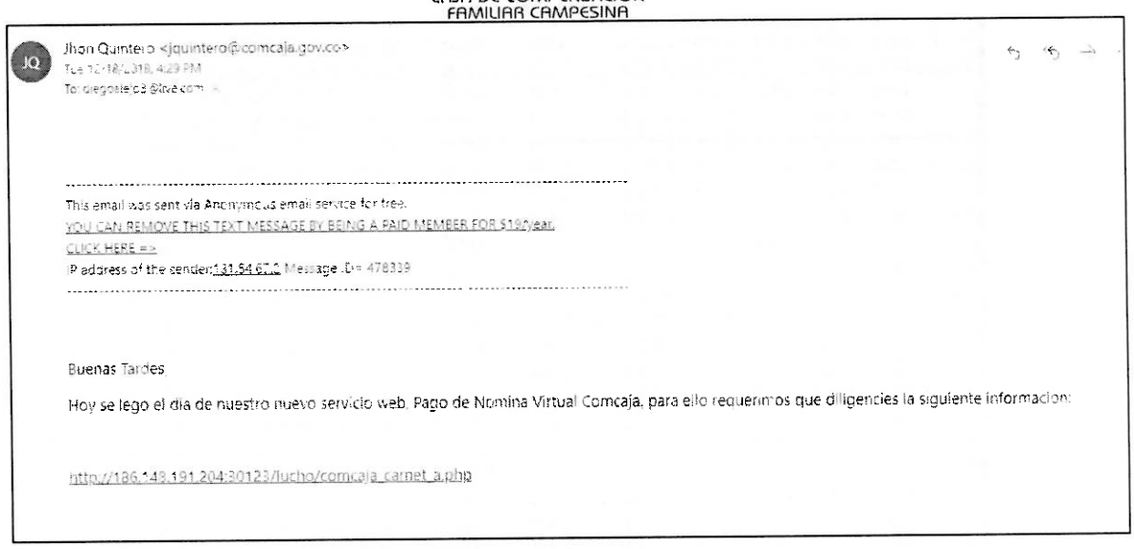
```
[*] 186.148.191.204:25   - 186.148.191.204:25 Banner: 220-correo.comcaja.gov.co ESMTP Postfix
[+] 186.148.191.204:25   - 186.148.191.204:25 Users found: dbadmin, karaf, operator, sys, xpdb
[*] Scanned 1 of 1 hosts (100% complete)
```



Configuración registro Dkim

Debido a que no se tiene configurado en el dominio de correo electrónico los registros SPF y DKIM, un atacante puede a cabo una suplantación de email y distribuir a través de este spam, correo malicioso

COMCAJA
CAJA DE COMPENSACION
FAMILIAR CAMPESINA



Exposición de directorios y código de desarrollo