 Gobernación de Risaralda	<p align="center">Departamento de Risaralda Dirección de Control Interno</p> <p align="center">PROCESO EVALUACION INDEPENDIENTE</p> <p align="center">Informe Final de Auditoria Interna</p>
Versión: 3	Vigencia: 08-2013

AUDITORIA INTERNA: Seguimiento y Evaluación a la Seguridad Informática y Licenciamiento de Software.	FECHA ELABORACIÓN: Noviembre de 2017
DIRECTIVO RESPONSABLE: Ruby Lucia Aguirre Torres. AUDITOR: Luis Alexander Vásquez Hernández	DESTINATARIO: Dirección de Informática y Sistemas.

ASPECTOS GENERALES



OBJETIVO(S):

1. Verificar el Cumplimiento de la Políticas de Operación de Seguridad Informática, dispuestas por la Dirección de Informática y Sistemas.
2. Verificar el inventario de equipos de cómputo con que cuenta la Administración Departamental
3. Identificar el tipo de software instalado en los equipos de cómputo de la Administración Departamental y su licenciamiento.
4. verificar la existencia y aplicación de directrices para evitar la utilización e instalación de software no licenciados.
5. verificar cuál es el destino final del software dado de baja en la Administración Departamental.

ALCANCE:

Se verificará en el subproceso Gestión de Tecnologías de la Información, la adquisición de software licenciado para los equipos de cómputo de la Administración Departamental.

Se inspeccionarán los equipos de cómputo de los funcionarios y contratistas con los que cuentan las diferentes Dependencias y Secretarías de la Administración Departamental, verificando el tipo de software instalado. Así mismo se validará el cumplimiento de las Políticas de Operación de Seguridad Informática.

 	<p align="center">Departamento de Risaralda Dirección de Control Interno</p> <p align="center">PROCESO EVALUACION INDEPENDIENTE</p> <p align="center">Informe Final de Auditoria Interna</p>
Versión: 3	Vigencia: 08-2013

CRITERIOS:

- ✓ Ley 23 de 1982
- ✓ Circular 7 de 2005 Departamento Administrativo de la Función Pública.
- ✓ Directiva 2 de 2002 Presidencia de la Republica.
- ✓ Políticas de Operación
- ✓ Procedimientos establecidos para la mitigación del riesgos plasmado en las Políticas de Operación de Seguridad Informática tomado como base bibliográfica y de consultoría la NTC ISO/IEC 27001

METODOLOGIA:

- ✓ Observación
- ✓ Revisión Analítica
- ✓ Entrevista
- ✓ Muestreo Estadístico



DESARROLLO DE LA AUDITORÍA

En el desarrollo de la auditoria de Evaluación y Seguimiento al software adquirido y/o administrado por el Departamento de Risaralda, de conformidad con el plan de auditorías establecido para el año 2017 por la Dirección de Control Interno y con lo dispuesto en la Circular 07 de 2005 del Departamento Administrativo de la Función Pública DAFP, se realizó la respectiva visita a la Dirección de Informática y Sistemas, con el fin de verificar el proceso de adquisición de las licencias de software para los aplicativos utilizados por la Administración Departamental. De igual manera se solicitó el inventario de equipos de cómputo con los cuales cuenta a la fecha la Administración, con el fin de realizar un muestreo razonable y así proceder con la validación en los puestos de trabajo en cuanto a la aplicación de las políticas de seguridad informática y revisión del software instalado en cada máquina.

Con el fin de realizar una revisión más eficiente de los equipos de cómputo, la Dirección de Informática y Sistemas nos 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 puede utilizarse para visualizar el inventario a través de una interfaz web”.

Relación de Equipos revisados OCS INVENTORY:



  <p>Gobernación de Risaralda</p>	<p align="center">Departamento de Risaralda Dirección de Control Interno</p> <p align="center">PROCESO EVALUACION INDEPENDIENTE</p> <p align="center">Informe Final de Auditoria Interna</p>
Versión: 3	Vigencia: 08-2013

ESPACIO MUESTRAL			
DATOS POBLACION SEGÚN INVENTARIO EQUIPOS			680
DIRECCIÓN INFORMÁTICA Y SISTEMAS			
MUESTRA			120
No.	No. AUDITADOS	DEPENDENCIA	EQUIPO AUDITADO
1	8	Despacho del Gobernador	GOBE57951
2			GOBE67099
3			GOBE64067
4			GOBE64185
5			GOBE65088
6			GOBE61845
7			GOBE72712
8			GOBE65091
9	6	Infraestructura	GOBE72711
10			GOBE68315
11			GOBE57902
12			GOBE65070
13			GOBE68314
14			GOBE68210

No.	No. AUDITADOS	DEPENDENCIA	EQUIPO AUDITADO
9	6	Infraestructura	GOBE72711
10			GOBE68315
11			GOBE57902
12			GOBE65070
13			GOBE68314
14			GOBE68210
15	20	Administrativa	GOBE65111
16			GOBE65064
17			GOBE64337
18			GOBE67064
19			GOBE63985
20			GOBE67061
21			GOBE57914
22			GOBE57898
23			GOBE63997
24			GOBE64023
25			GOBE67082
26			GOBE67837
27			GOBE80012
28			GOBE68254
29			GOBE67070
30			GOBE67348
31			GOBE67830
32			GOBE67065
33			GOBE61896
34			GOBE65079
35	18	Hacienda	GOBE80011
36			GOBE63998
37			GOBE67881
38			GOBE67880
39			GOBE65191
40			GOBE67888
41			GOBE67886
42			GOBE67882
43			GOBE65194
44			GOBE65104
45			GOBE67884
46			GOBE67834
47			GOBE68331
48			GOBE01074
49			GOBE67066
50			GOBE67833
51			GOBE67904
52			GOBE67835

  <p>Gobernación de Risaralda</p>	<p align="center">Departamento de Risaralda Dirección de Control Interno</p> <p align="center">PROCESO EVALUACION INDEPENDIENTE</p> <p align="center">Informe Final de Auditoria Interna</p>
Versión: 3	Vigencia: 08-2013

No.	No. AUDITADOS	DEPENDENCIA	EQUIPO AUDITADO
53	8	Juridica	GOBE63996
54			GOBE78575
55			GOBE76508
56			GOBE65093
57			GOBE65068
58			GOBE65190
59			GOBE65178
60			GOBE72598
61	4	Planeación	GOBE67875
62			GOBE64198
63			GOBE67889
64			GOBE68311
65	3	Desarrollo Agropecuario	GOBE67353
66			GOBE64097
67			GOBE64226
68	10	Gobierno	GOBE57872
69			GOBE64002
70			GOBE64248
71			GOBE64032
72			GOBE65045
73			GOBE64635
74			GOBE67847
75			GOBE68047
76			GOBE67058
77			GOBE64000
78	18	Educación	GOBE61969
79			GOBE71668
80			GOBE92EK9
81			GOBEMJ92DV8
82			GOBE72710
83			GOBE68101
84			GOBEMJ0302MD
85			GOBE71670
86			GOBEM79628
87			GOBE1D61
88			GOBE64082
89			GOBE67018
90			GOBE68083
91			GOBE68070
92			GOBE79636
93			GOBE67141
94			GOBE67139
95			GOBE68074

 	<p align="center">Departamento de Risaralda Dirección de Control Interno</p> <p align="center">PROCESO EVALUACION INDEPENDIENTE</p> <p align="center">Informe Final de Auditoria Interna</p>
Versión: 3	Vigencia: 08-2013

No.	No. AUDITADOS	DEPENDENCIA	EQUIPO AUDITADO
96	18	Salud	GOBE66868
97			GOBE6048
98			GOBE68060
99			GOBE67002
100			GOBE61832
101			MJ44YR3
102			MJ92EG6
103			GOBE68091
104			GOBE67854
105			GOBE64237
106			GOBE68456
107			MXL4321GM8
108			GOBE5004
109			GOBE67864
110			GOBE2
111			GOBE67009
112			GOBE64769
113			GOBE68063
114	4	Desarrollo Economico	GOBE64016
115			GOBE65080
116			GOBE2DY7
117			GOBE67911
118	3	Deportes	GOBE67375
119			GOBE64603
120			GOBE61892



De la revisión realizada se encontraron los siguientes aspectos:

1. Verificación Cumplimiento de las Políticas de Operación de la Seguridad informática

1.1. Correcta utilización de la infraestructura tecnológica.

1.1.1 Manejo de toma corriente regulado.

Se evidenció que el toma corriente regulado en la mayoría de los casos está siendo bien utilizado, toda vez que de las visitas realizadas solo el 3%

  <p>Gobernación de Risaralda</p>	<p>Departamento de Risaralda Dirección de Control Interno</p> <p>PROCESO EVALUACION INDEPENDIENTE</p> <p>Informe Final de Auditoria Interna</p>
<p>Versión: 3</p>	<p>Vigencia: 08-2013</p>

de los funcionarios tenían conectados sus equipos de cómputo a un toma corriente diferente al regulado (Color Naranja). Se tomó evidencia de este hecho y se socializó el motivo por el cual se deben conectar dichos dispositivos a la red regulada. (Ver imagen 1).



Imagen 1

1.1.2 Exposición a líquidos.

Se evidenció en las visitas realizadas que el 3% de los usuarios auditados, tenían líquidos cerca a sus equipos de cómputo, lo cual constituye un alto riesgo para el equipo en caso de derrames. (Ver Imagen 2).

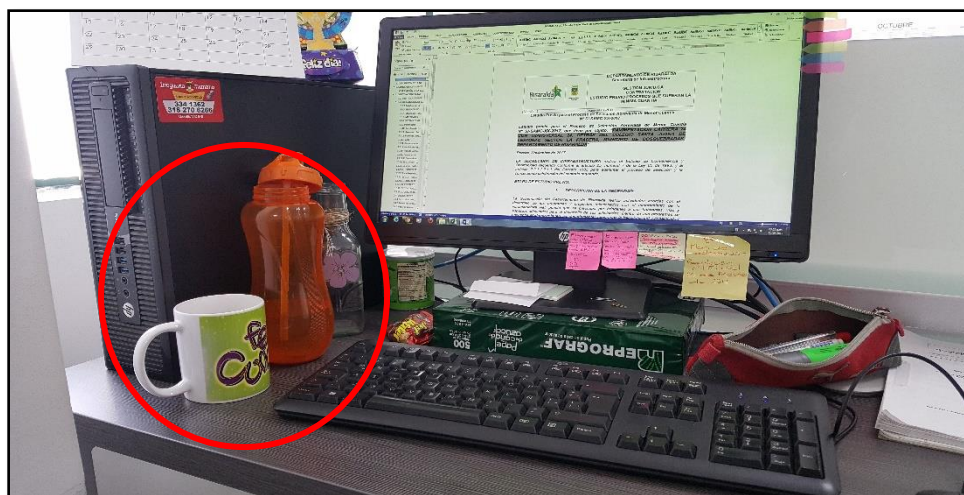




Imagen 1

  <p>Gobernación de Risaralda</p>	<p>Departamento de Risaralda Dirección de Control Interno</p> <p>PROCESO EVALUACION INDEPENDIENTE</p> <p>Informe Final de Auditoria Interna</p>
<p>Versión: 3</p>	<p>Vigencia: 08-2013</p>

1.2 Acceso al sistema y seguridad.

1.2.1 Manipulación del sistema.

Se evidenció que 32% de los equipos auditados cuentan con permisos de administrador, siendo esto una causa que vulnera al sistema y compromete así la seguridad de la información, teniendo en cuenta que un usuario de estas características tiene la facultad de realizar todo tipo de cambios en el equipo, ejemplo de esto instalar o desinstalar programas. (Ver imagen 3).

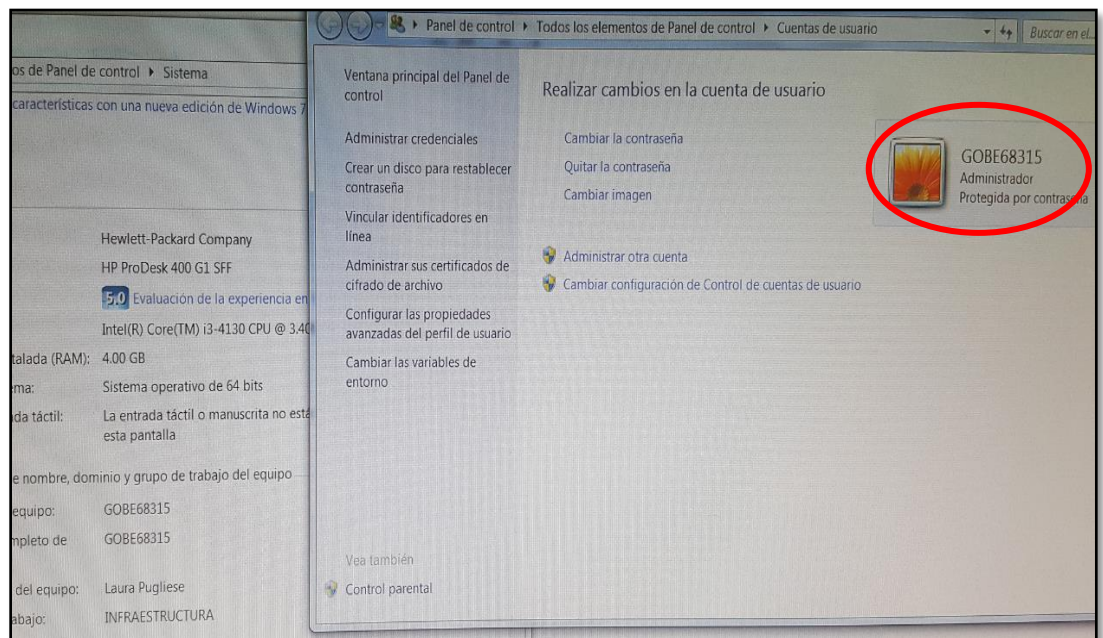




Imagen 3

1.2.2 Uso de indebido de almacenamiento en el equipo (información personal).

Se evidenció almacenamiento de archivos personales en los equipos de cómputo por parte del 12% de los usuarios auditados, como lo son fotografías, videos y archivos de música (Ver imagen 4 y 5).

 	<p align="center">Departamento de Risaralda Dirección de Control Interno</p> <p align="center">PROCESO EVALUACION INDEPENDIENTE</p> <p align="center">Informe Final de Auditoria Interna</p>
<p>Versión: 3</p>	<p>Vigencia: 08-2013</p>

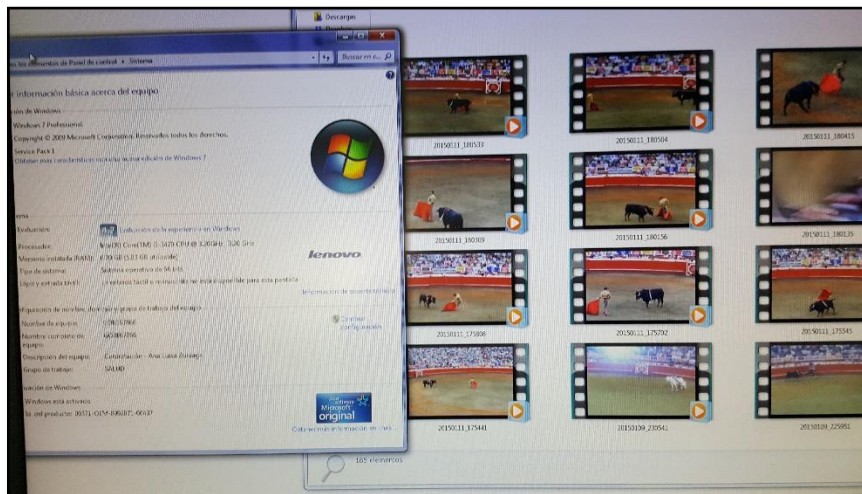


Imagen 4

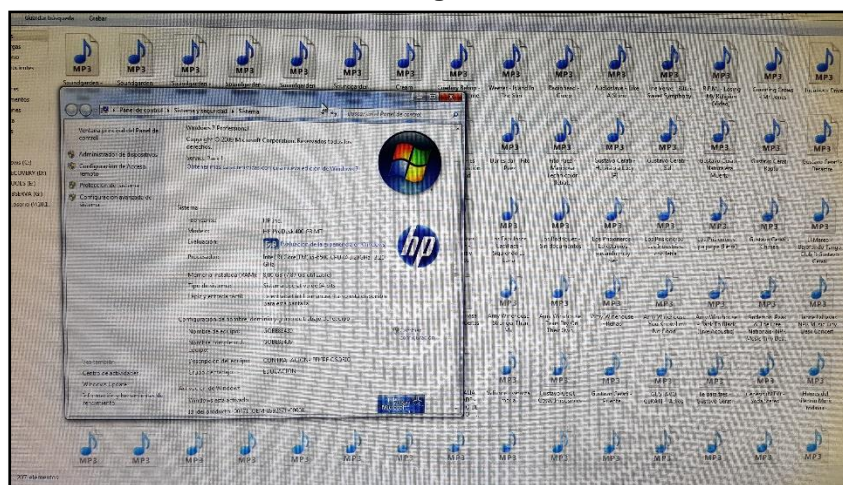




Imagen 5

1.3 Buenas prácticas en el uso de internet e intranet.

1.3.1 Bloqueo de contenido inapropiado y redes Sociales.

Se evidenció que en el 45% de los equipos de cómputo auditados, no existen restricciones para la navegación en redes sociales y páginas de contenido sexual. (Ver imagen 6)

  <p>Gobernación de Risaralda</p>	<p>Departamento de Risaralda Dirección de Control Interno</p> <p>PROCESO EVALUACION INDEPENDIENTE</p> <p>Informe Final de Auditoria Interna</p>
<p>Versión: 3</p>	<p>Vigencia: 08-2013</p>

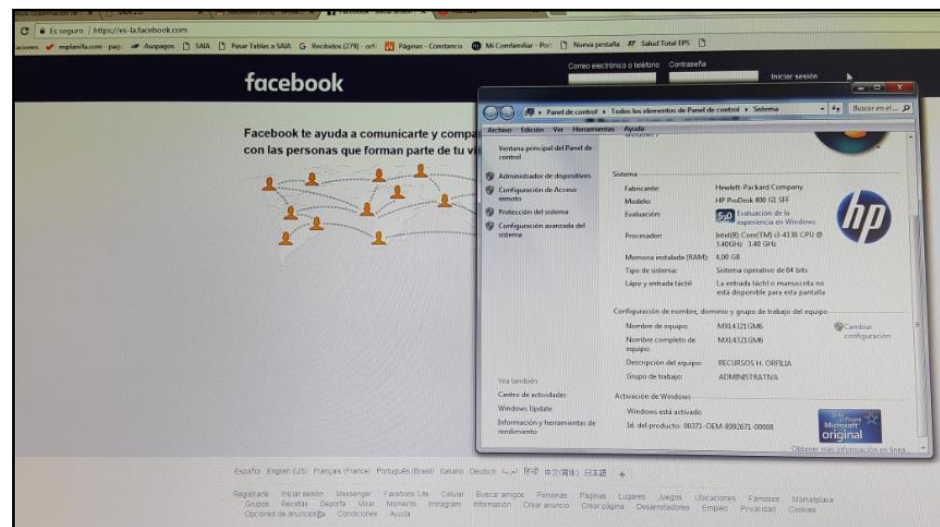


Imagen 6

1.3.2 Juegos.

Se evidencio que en el 3% de los equipos auditado, se encontraba el paquete de juegos de Windows habilitado (Ver imagen 7).

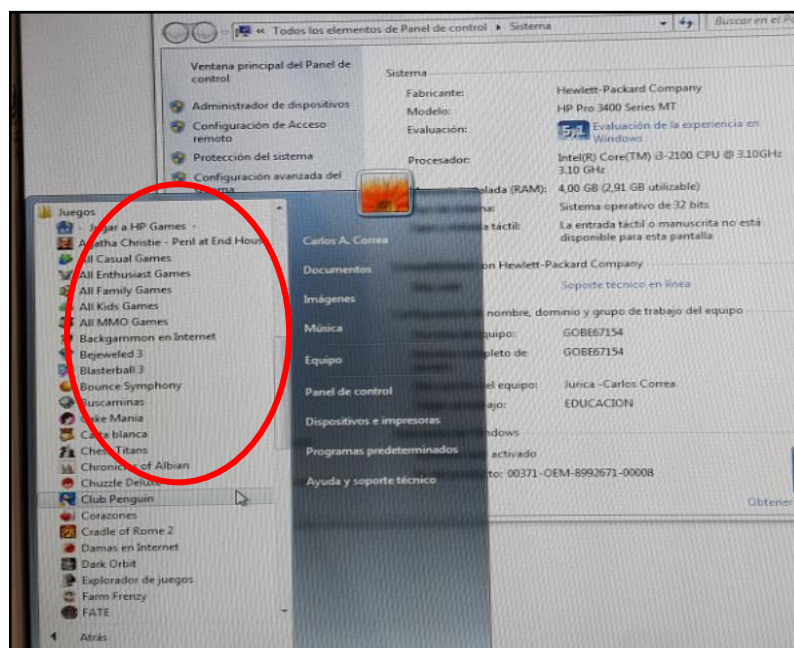




Imagen 7

  Gobernación de Risaralda	<p align="center">Departamento de Risaralda Dirección de Control Interno</p> <p align="center">PROCESO EVALUACION INDEPENDIENTE</p> <p align="center">Informe Final de Auditoria Interna</p>
Versión: 3	Vigencia: 08-2013

1.3.3 Uso del correo electrónico.

Se evidenció el correcto uso del correo electrónico institucional por parte de las personas auditadas, comprobando un buen tratamiento de los correos sospechosos por parte de los usuarios.

1.3.4 Acceso a información de equipos en red sin autorización.

No se evidenció el acceso a equipos ajenos a través de intranet sin autorización del propietario o del área de Sistemas por parte de las personas auditadas.



2. Inventario

A la fecha la Administración Departamental cuenta con un total de 680 equipos de cómputo, según la información suministrada por el software de inventario utilizado por la Dirección de Informática y Sistemas. De acuerdo a lo anterior y en con el fin de verificar que la Administración cumpla con lo ordenado en la Ley 23 de 1982 y que los usuarios estén aplicando correctamente las políticas de la seguridad informática implementadas por la Dirección de Informática y Sistemas, se tomó como muestra un total de 120 equipos de cómputo y se procedió con la respectiva verificación en cada uno de ellos, corroborando los controles organizacionales establecidos para la detección de software o aplicaciones ofimáticas no licenciados y la aplicación de las políticas de la seguridad informática.

3. SOFTWARE INSTALADO:

En la verificación realizada a los 120 equipos relacionados en la tabla anterior, los cuales hacen parte de la muestra tomada, se pudo establecer que en un 99% el software encontrado es el preinstalado por el fabricante.

Así mismo se evidencio la existencia de Software instalado por los usuarios finales, de los cuales tras el análisis y la investigación realizada, son considerados software libre, versiones de prueba, aplicaciones para acceder al contenido de equipos móviles (celulares), lo cual no implica estar incumpliendo las normas de Derecho de autor en cuanto al no pago de derechos o tener programas, aplicaciones o software “pirata” o no licenciados debidamente, siendo un aspecto a tener en cuenta para reforzar las medidas

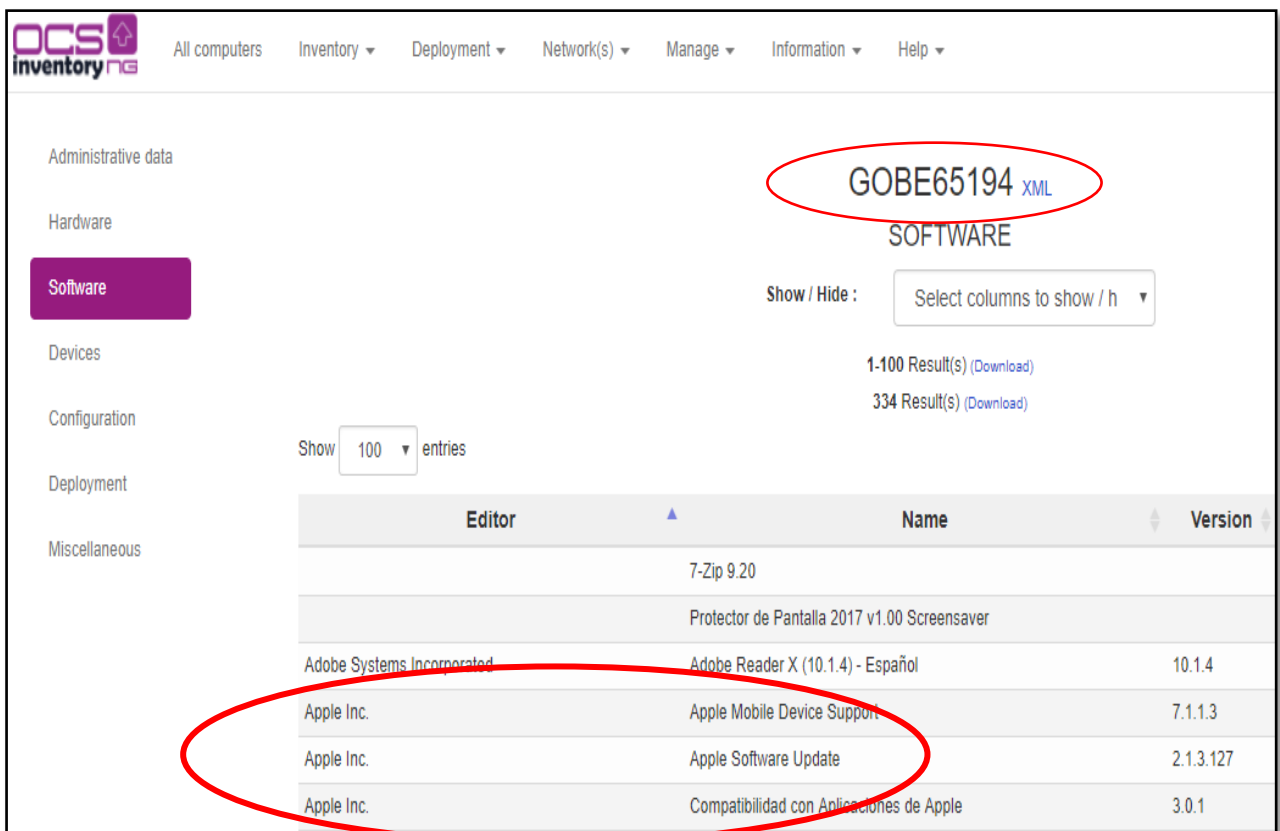
  <p>Gobernación de Risaralda</p>	<p align="center">Departamento de Risaralda Dirección de Control Interno</p> <p align="center">PROCESO EVALUACION INDEPENDIENTE</p> <p align="center">Informe Final de Auditoria Interna</p>
Versión: 3	Vigencia: 08-2013

de Seguridad y los controles, con el fin de restringir el acceso a las páginas donde ofrecen este tipo de software y/o permiten la descarga del mismo de manera gratuita incumpliendo

con el pago de licencias corporativas y así mismo se aumenta el riesgo de infectar los equipos con virus informáticos al acceder a este tipo de páginas.

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 que no forme parte del anterior.



Teniendo en cuenta lo anterior, se encontraron aplicaciones tales como:

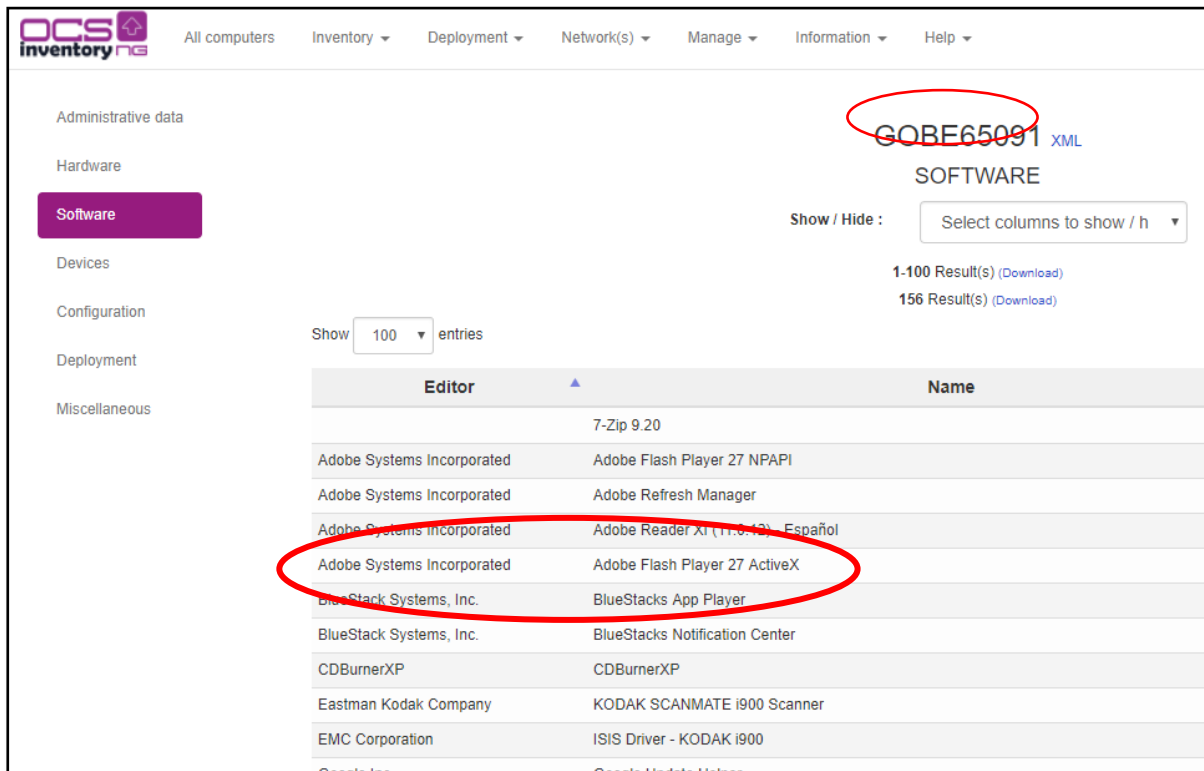


The screenshot shows the OCS Inventory NG web interface. The top navigation bar includes links for All computers, Inventory, Deployment, Network(s), Manage, Information, and Help. The left sidebar lists various categories, with 'Software' currently selected. The main content area displays the software inventory for a specific device, identified by the ID 'GOBE65194' (circled in red). Below the device ID, the word 'SOFTWARE' is displayed. A 'Show / Hide' dropdown menu is visible, set to 'Select columns to show / h'. Below this, there are links for '1-100 Result(s) (Download)' and '334 Result(s) (Download)'. A table lists the installed software with columns for Editor, Name, and Version. The table includes entries for 7-Zip 9.20, Protector de Pantalla 2017 v1.00 Screensaver, Adobe Reader X (10.1.4) - Español, and three Apple-related entries: Apple Mobile Device Support (7.1.1.3), Apple Software Update (2.1.3.127), and Compatibilidad con Aplicaciones de Apple (3.0.1). A red circle highlights the three Apple-related entries.

Editor	Name	Version
	7-Zip 9.20	
	Protector de Pantalla 2017 v1.00 Screensaver	
Adobe Systems Incorporated	Adobe Reader X (10.1.4) - Español	10.1.4
Apple Inc.	Apple Mobile Device Support	7.1.1.3
Apple Inc.	Apple Software Update	2.1.3.127
Apple Inc.	Compatibilidad con Aplicaciones de Apple	3.0.1

- Equipo: **GOBE65194** / Software: Apple Mobile Device Support: plugin para que otro programa soporte archivos en formato Apple.

 	<p align="center">Departamento de Risaralda Dirección de Control Interno</p> <p align="center">PROCESO EVALUACION INDEPENDIENTE</p> <p align="center">Informe Final de Auditoria Interna</p>
Versión: 3	Vigencia: 08-2013



Administrative data

Hardware

Software

Devices

Configuration

Deployment

Miscellaneous

Gobe65091 XML

SOFTWARE

Show / Hide :

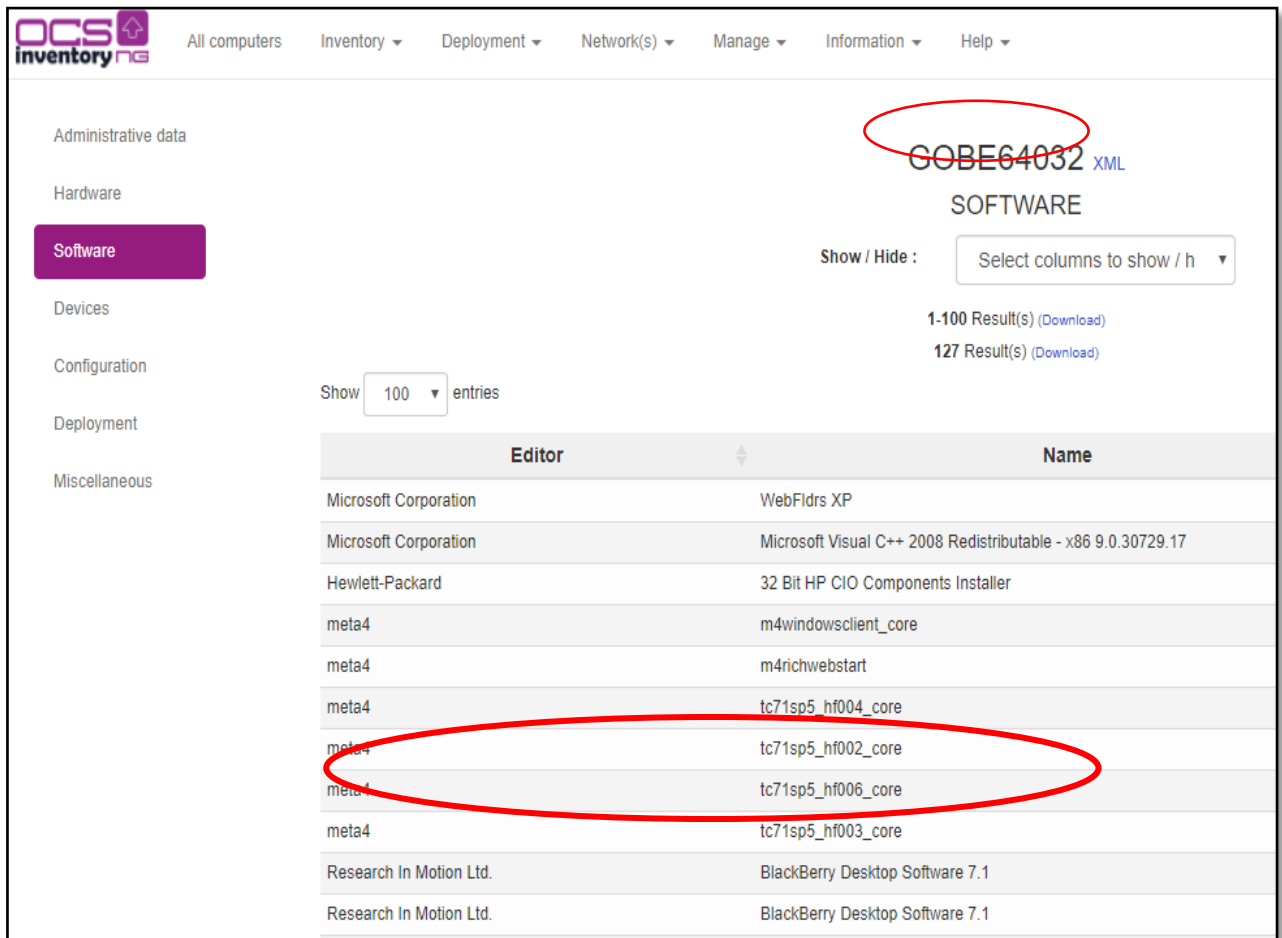
1-100 Result(s) (Download)

156 Result(s) (Download)

Show entries

Editor	Name
	7-Zip 9.20
Adobe Systems Incorporated	Adobe Flash Player 27 NPAPI
Adobe Systems Incorporated	Adobe Refresh Manager
Adobe Systems Incorporated	Adobe Reader XI (11.0.12) - Español
Adobe Systems Incorporated	Adobe Flash Player 27 ActiveX
BlueStack Systems, Inc.	BlueStacks App Player
BlueStack Systems, Inc.	BlueStacks Notification Center
CDBurnerXP	CDBurnerXP
Eastman Kodak Company	KODAK SCANMATE i900 Scanner
EMC Corporation	ISIS Driver - KODAK i900

- Equipo: Gobe65091 / Software: **BlueStacks** App Player es una herramienta que le permite ejecutar aplicaciones creadas para el sistema operativo Android en Windows y Mac.



Administrative data

Hardware

Software

Devices

Configuration

Deployment

Miscellaneous

GOBE64032 XML

SOFTWARE

Show / Hide :

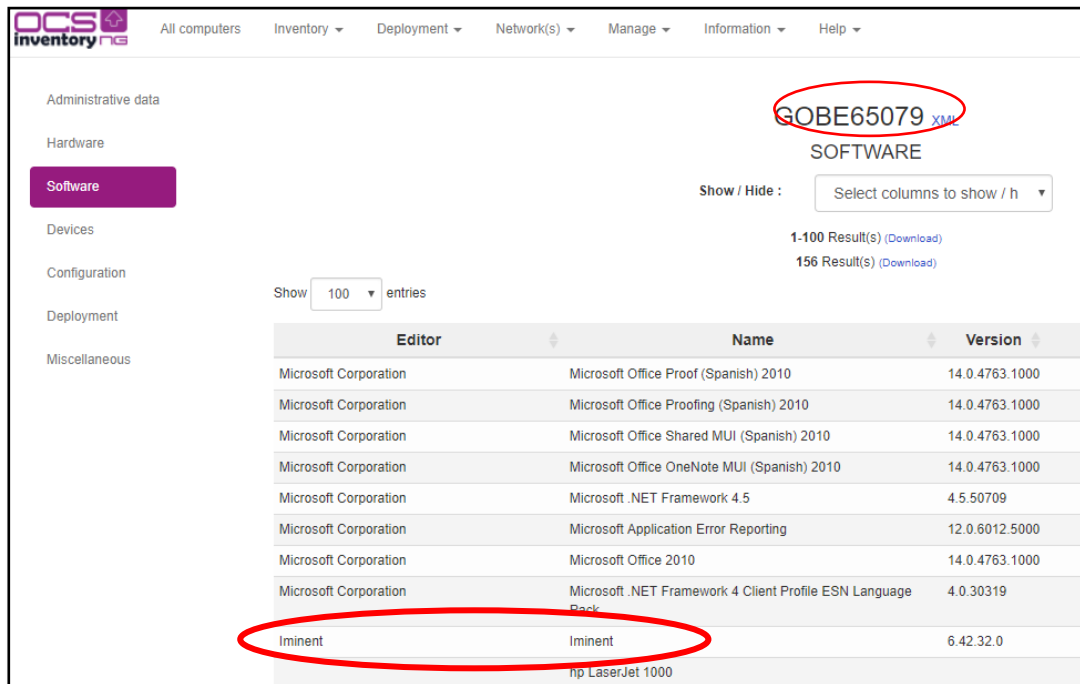
1-100 Result(s) (Download)

127 Result(s) (Download)

Show entries

Editor	Name
Microsoft Corporation	WebFldrs XP
Microsoft Corporation	Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.17
Hewlett-Packard	32 Bit HP CIO Components Installer
meta4	m4windowsclient_core
meta4	m4richwebstart
meta4	tc71sp5_hf004_core
meta4	tc71sp5_hf002_core
meta4	tc71sp5_hf006_core
meta4	tc71sp5_hf003_core
Research In Motion Ltd.	BlackBerry Desktop Software 7.1
Research In Motion Ltd.	BlackBerry Desktop Software 7.1

- Equipo: GOBE64032 / Software: **BlackBerry Desktop Software** es un programa con el que se pueden sincronizar los teléfonos **BlackBerry** con un ordenador con Windows de manera eficaz, haciendo se puedan realizar copias de seguridad y compartir archivos.



Administrative data

Hardware

Software

Devices

Configuration

Deployment

Miscellaneous

GOB65079 XML

SOFTWARE

Show / Hide :

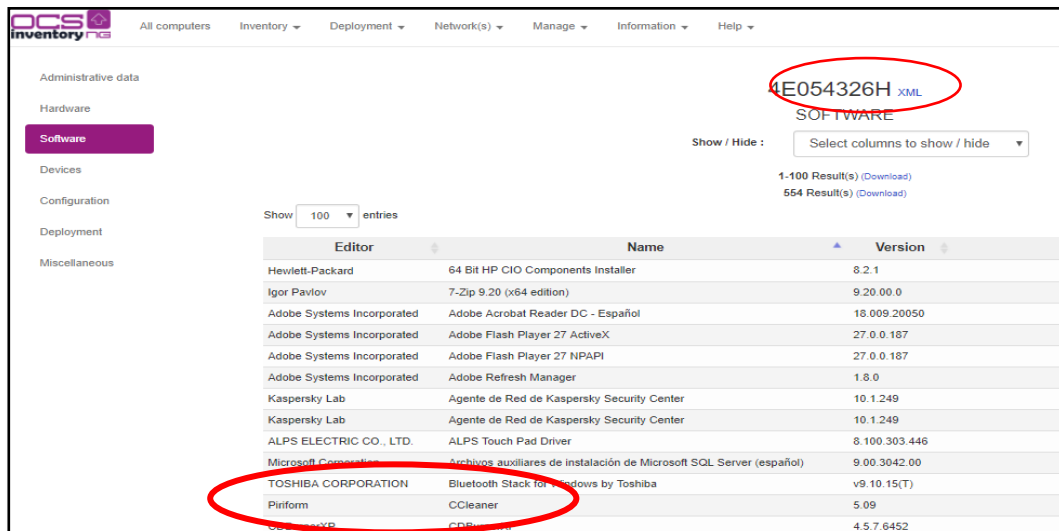
1-100 Result(s) (Download)

156 Result(s) (Download)

Show 100 entries

Editor	Name	Version
Microsoft Corporation	Microsoft Office Proof (Spanish) 2010	14.0.4763.1000
Microsoft Corporation	Microsoft Office Proofing (Spanish) 2010	14.0.4763.1000
Microsoft Corporation	Microsoft Office Shared MUI (Spanish) 2010	14.0.4763.1000
Microsoft Corporation	Microsoft Office OneNote MUI (Spanish) 2010	14.0.4763.1000
Microsoft Corporation	Microsoft .NET Framework 4.5	4.5.50709
Microsoft Corporation	Microsoft Application Error Reporting	12.0.6012.5000
Microsoft Corporation	Microsoft Office 2010	14.0.4763.1000
Microsoft Corporation	Microsoft .NET Framework 4 Client Profile ESN Language Pack	4.0.30319
Iminent	Iminent	6.42.32.0
HP	HP LaserJet 1000	

- Equipo: **GOB65079** / Software: **Iminent** Esta aplicación puede ser considerada como un malware o spyware. En sí, la barra de herramientas de la aplicación no es maliciosa y no infecta el computador de manera directa con algún virus, pero es una aplicación que puede volver lento el equipo donde está instalado.



Administrative data

Hardware

Software

Devices

Configuration

Deployment

Miscellaneous

4E054326H XML

SOFTWARE



Show / Hide :

1-100 Result(s) (Download)

554 Result(s) (Download)

Show 100 entries

Editor	Name	Version
Hewlett-Packard	64 Bit HP CIO Components Installer	8.2.1
Igor Pavlov	7-Zip 9.20 (x64 edition)	9.20.0.0
Adobe Systems Incorporated	Adobe Acrobat Reader DC - Español	18.009.20050
Adobe Systems Incorporated	Adobe Flash Player 27 ActiveX	27.0.0.187
Adobe Systems Incorporated	Adobe Flash Player 27 NPAPI	27.0.0.187
Adobe Systems Incorporated	Adobe Refresh Manager	1.8.0
Kaspersky Lab	Agente de Red de Kaspersky Security Center	10.1.249
Kaspersky Lab	Agente de Red de Kaspersky Security Center	10.1.249
ALPS ELECTRIC CO., LTD.	ALPS Touch Pad Driver	8.100.303.446
Microsoft Corporation	Archivos auxiliares de instalación de Microsoft SQL Server (español)	9.00.3042.00
TOSHIBA CORPORATION	Bluetooth Stack for Windows by Toshiba	v9.10.15(T)
Piriform	CCleaner	5.09
Google	CDROM	4.5.7.6452

 	<p align="center">Departamento de Risaralda Dirección de Control Interno</p> <p align="center">PROCESO EVALUACION INDEPENDIENTE</p> <p align="center">Informe Final de Auditoria Interna</p>
Versión: 3	Vigencia: 08-2013

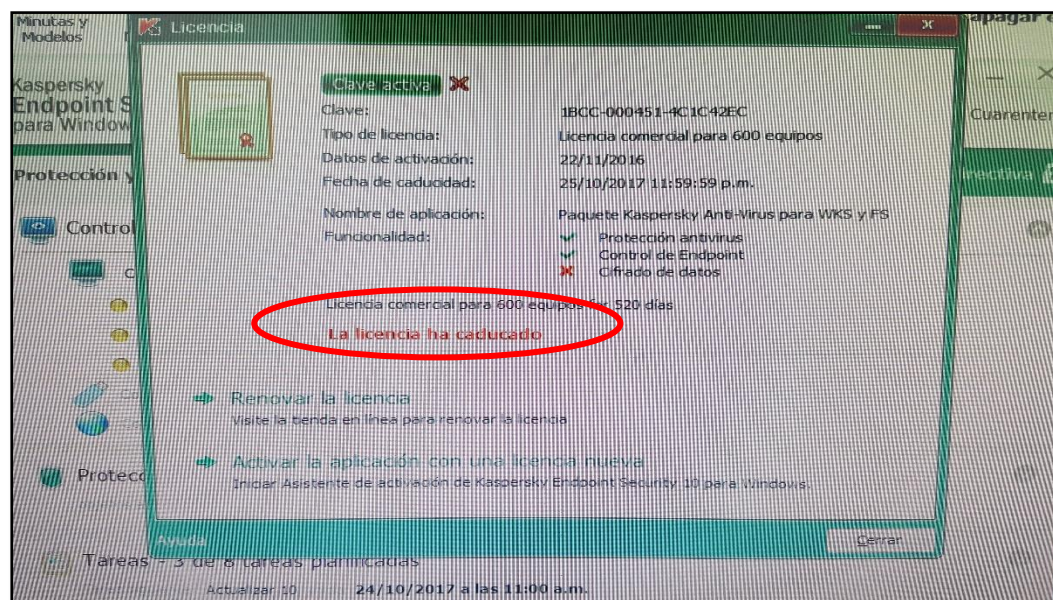
- Equipo: **GOBE67375** / **Software: CCLEANER**. (anteriormente Crap Cleaner) es una aplicación gratuita, de código cerrado, que tiene como propósito mejorar el rendimiento de cualquier equipo que ejecute Microsoft Windows mediante la eliminación de los archivos innecesarios y las entradas inválidas del registro de Windows.

1.1. OFFICE



De los 680 equipos de cómputo, 529 cuentan con Microsoft Office debidamente licenciado, 44 tienen instalado Libre Office y 35 Open Office. Los dos últimos paquetes ofimáticos son de uso libre.

1.2. ANTIVIRUS

Una vez culminada la revisión de los 120 equipos de cómputo, se logró evidenciar que cada una de las maquinas cuentan con el Antivirus **KASPERSKY** instalado; pero que al verificar su licencia, para 20 de ellos esta se encontraba caducada, como se puede evidenciar en la siguiente imagen ejemplo:



Por lo anterior se procedió a solicitar a la Dirección de Informática y Sistemas el contrato mediante el cual se adquieren las licencias de uso del mismo.



 	<p align="center">Departamento de Risaralda Dirección de Control Interno</p> <p align="center">PROCESO EVALUACION INDEPENDIENTE</p> <p align="center">Informe Final de Auditoria Interna</p>
Versión: 3	Vigencia: 08-2013

Una vez revisado dicho contrato, se evidencia que este tiene como alcance la Actualización y soporte para 700 licencias y adquisición de 50 licencias adicionales del antivirus **KASPERSKY**, por lo cual es evidente que hace falta el proceso de actualización de las licencia en estos equipos por parte de la Dirección de Informática y Sistemas.

1.3. SOFTWARE UTILIZADO Y/O ADMINISTRADO POR SECRETARÍAS:

Teniendo en cuenta que las Secretarias de Hacienda, Planeación, Educación Y Salud, son dependencias que tratan los procesos más relevantes de la Administración Departamental y que por ende requieren del uso de aplicativos adicionales a los preinstalados en los equipos de cómputo, se procedió a realizar la relación del software administrado y/o utilizado por cada una de estas, los cuales cuentan con sus respectivas licencias de uso:

No.	SECRETARÍA	SOFTWARE
1	Hacienda	Software PCTG Ltda.
		Software Sistema de Crédito Público.
		Software Humano.
2	Salud	Sistema de Información de Salud Pública SISAP.
		Sistema de ordenamiento de turnos ETURNO.
3	Planeación	BD Sistema de Seguimiento al Plan de Desarrollo.
		Sistema de Información Geográfica ARCGIS Versión 9.3
4	Educación	Software para determinar las competencias en matemáticas.
		Software para determinar las competencias en lectura.
		Sistema de orientación Profesional.
5	Administrativa - Dirección De Informática Y Sistemas	Aplicativos Cliente – Servidor.
		Sistema de Información Financiero PCTG.
		Sistema de Información de la Deuda Pública.
		Sistema de Información de Nómina Humano Web.
		Sistema de Información de Pasivocol.
		Sistema de Información de Gestión Documental SAIA.

 	<p align="center">Departamento de Risaralda Dirección de Control Interno</p> <p align="center">PROCESO EVALUACION INDEPENDIENTE</p> <p align="center">Informe Final de Auditoria Interna</p>
Versión: 3	Vigencia: 08-2013

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

Para evitar 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:

2.1. Vigilancia y Monitoreo.

Para la ejecución de esta actividad es utilizado el aplicativo Web OCS INVENTORY.



“Es un software libre que permite a los usuarios administrar 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 puede utilizarse para visualizar el inventario a través de una interfaz web. Además, OCS comprende la posibilidad de implementación de aplicaciones en los equipos de acuerdo a criterios de búsqueda. Además, tiene muchas opciones más como escanear la red por medio del IPDiscovery, o instalar aplicaciones remotamente creando Builds”.

2.2. Revisión y Barrido.

Esta actividad se realiza periódicamente con el apoyo del personal adscrito a la Dirección de Informática y Sistema. Para los meses de julio y agosto del presente año se inició la revisión de equipos de todas las Secretarías, Direcciones y demás Dependencias de la Administración Departamental, como se pudo evidenciar en el informe adjunto al plan de mejoramiento No. 670.

3. 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. En la práctica significa que NO se puede usar la clave para instalarlo en un equipo distinto.

  <p>Gobernación de Risaralda</p>	<p>Departamento de Risaralda Dirección de Control Interno</p> <p>PROCESO EVALUACION INDEPENDIENTE</p> <p>Informe Final de Auditoria Interna</p>
<p>Versión: 3</p>	<p>Vigencia: 08-2013</p>



HALLAZGOS

HALLAZGOS POSITIVOS:

- Existe una muy buena disposición de los funcionarios por conocer sobre la seguridad de la información.
- Es de resaltar los controles establecidos por parte de la Dirección de Informática y Sistemas, los cuales ayudan a reducir considerablemente el riesgo de instalación de Software no licenciado en los equipos de cómputo de la Administración, evitando así que la Administración Departamental se vea incurso en procesos que puedan acarrear sanciones económicas o penales.
- Se valora la buena adquisición y administración de las licencias de uso de los Sistemas de Información utilizados por la Administración Departamental.

RECOMENDACIONES

- I. Es importante realizar la actualización del nombre de usuario en los equipos de cómputo.
- II. Los equipos informáticos de los funcionarios auditados poseen vulnerabilidad ya que el 32% de las cuentas de los usuario auditadas poseen privilegios administrativos, habilitando al usuario el acceso al sistema con poder de alterarlo en su funcionamiento o la instalación de paquetes informáticos no licenciados, la Norma NTC-ISO-27001 propone procedimientos para mitigar el riesgo como es:
 - NTC-ISO-27001/A.11.2.2 nos sugiere: *“Se debe restringir y controlar la asignación y uso de privilegios.”*
 - NTC-ISO-27001/A.11.2.4 nos sugiere: *“La dirección debe establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios.”*
- III. Es pertinente realizar un barrido por los diferentes puestos de trabajo, con el fin de deshabilitar el paquete de juegos de los equipos de cómputo y con ello dar cumplimiento a las políticas del proceso.

 	<p align="center">Departamento de Risaralda Dirección de Control Interno</p> <p align="center">PROCESO EVALUACION INDEPENDIENTE</p> <p align="center">Informe Final de Auditoria Interna</p>
Versión: 3	Vigencia: 08-2013

- NTC-ISO-27001/A.11.6.1 nos sugiere: *“Se debe restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida de control de acceso.”*
- NTC-ISO-27001/A.12.4.1 nos sugiere: *“Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.”*

IV. Es de gran importancia realizar la actualización de las licencias de antivirus **KASPERSKY** que presentan caducidad.



V. Sería de gran importancia que en los barridos realizados por el personal de Informática y Sistemas, se eliminen los aplicativos que no están relacionados directamente con las labores de la Administración (Dropbox, Skype, iTunes, Ccleaner, Iminent, etc.), ocupando espacio en los discos duros y generando posibles accesos a virus informáticos.

VI. Las cuentas de usuario deben estar ajustadas al perfil de cada funcionario, uno de los riesgos más altos proviene de la descarga e instalación de aplicaciones desde Internet. Algunas de ellas están hechas por delincuentes informáticos, que con la promesa de un juego, canción o aplicación de ocio, engañan al usuario para que las ejecute en su equipo y así, de paso, también instale programas malignos como virus o software espía.

VII. Adelantar campañas para el fomento de la cultura del bloqueo manual de la cuenta de usuario por parte de los funcionarios y con esto evitar el libre acceso por parte de personal ajeno a la Administración Departamental. Así mismo asignar contraseñas a las cuentas de usuario para aquellos equipos que aún no poseen.

- NTC-ISO 27001/A.11.5.5 nos sugiere en los tiempos de inactividad *“Las sesiones inactivas se deben suspender después de un periodo definido de inactividad.”*

VIII. Eliminación de los archivos de música e imágenes personales de los equipos de cómputo.

  Gobernación de Risaralda	<p align="center">Departamento de Risaralda Dirección de Control Interno</p> <p align="center">PROCESO EVALUACION INDEPENDIENTE</p> <p align="center">Informe Final de Auditoria Interna</p>
Versión: 3	Vigencia: 08-2013

- IX.** Es prudente efectuar un debido mecanismo de control y seguimiento de manera periódica, enfocadas a mitigar el acceso a las redes sociales por parte de los funcionarios o contratistas y demás debilidades detectadas en desarrollo de esta auditoría.
- X.** Sería pertinente realizar periódicamente la socialización de las políticas de operación de la seguridad informática a los funcionarios y contratistas de la Administración Departamental por todos los medios (SAIA, SPARK, Correo Electrónico).
- XI.** Con el fin de reforzar las medidas de Seguridad, se recomienda restringir el acceso a las páginas donde ofrecen software de prueba y/o permiten la descarga del mismo de manera gratuita incumpliendo con el pago de licencias y así mismo se aumenta el riesgo de infectar los equipos con virus informáticos al acceder a este tipo de páginas.
- XII.** Sería importante realizar los recorridos para la verificación de los equipos de cómputo y software instalado, de manera más seguida, por lo menos 3 veces en el año. Esto ayudaría a tener un inventario muy preciso y actualizado, así mismo se lograría tener un control más dinámico para que los usuarios no utilicen software no licenciado.

CONCLUSIONES

Teniendo en cuenta los resultados de la auditoría realizada en el año 2016, se puede concluir que la Administración Departamental ha venido mejorando en la administración de los recursos informáticos tanto hardware como software. Así mismos se puede decir que los funcionarios han tomado mayor conciencia del buen uso de estos recursos, los cuales son herramientas que facilitan el cumplimiento de sus funciones en el día a día.

De otro lado, se debe de seguir trabajando enfocados al aseguramiento de la información, teniendo en cuenta que se evidencian fallas y vulnerabilidades en la seguridad y estabilidad de los sistemas de información frente a las situaciones identificadas con respecto a los perfiles de usuario y las licencias de antivirus caducadas.

Luis Alexander Vásquez
Auditor.