 Gobernación de Risaralda	<p align="center">Departamento de Risaralda Oficina Asesora 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: Auditoría Interna Evaluación y Seguimiento al proceso de Gestión Informática Y Servicios Tecnológicos.	FECHA ELABORACIÓN: Abril de 2019
DIRECTIVO RESPONSABLE: Héctor Fabio Álzate AUDITOR: Luis Alexander Vásquez Hernández	DESTINATARIO: Proceso de Gestión Informática Y Servicios Tecnológicos.

ASPECTOS GENERALES

OBJETIVO(S):

Examinar y evaluar la adecuada y eficaz aplicación de los sistemas de control interno en el procedimiento de Gestión Informática Y Servicios Tecnológicos, permitiendo adoptar las acciones correctivas pertinentes que generar valor agregado y mejorar las operaciones de la Administración Departamental, así como contribuir al cumplimiento de los objetivos y metas institucionales.

ALCANCE:



La presente auditoria se enfocará en el cumplimiento de las normas y procedimientos establecidos en materia de Seguridad y Privacidad de la información y de licenciamiento de software, así mismo de las Políticas de Operación del proceso Gestión Informática y Servicios Tecnológicos de la Administración Departamental.

CRITERIOS:

- Ley 1915 de 2018
- Circular 7 de 2005 Departamento Administrativo de la Función Pública.
- Norma Técnica Colombiana ISO/IEC 27001
- Políticas de Operación del proceso Gestión Informática y Servicios Tecnológicos.

METODOLOGIA:

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

 	<p align="center">Departamento de Risaralda Oficina Asesora 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

DESARROLLO DE LA AUDITORÍA

De conformidad con el plan de auditorías establecido para el año 2019 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 realizó la respectiva visita a la Dirección de Informática y Sistemas, con el fin de verificar el cumplimiento de las normas y procedimientos establecidos en materia de Seguridad y Privacidad de la información y de licenciamiento de software, así mismo de las Políticas de Operación del proceso Gestión Informática y Servicios Tecnológicos de la Administración Departamental..

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



1. **Licenciamiento de Software.**
2. **Políticas de Operación Seguridad Informática.**
3. **Riesgos de gestión.**
4. **Riesgos de corrupción.**

1. **Licenciamiento de Software.**

A la fecha la Administración Departamental cuenta con un total de 861 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 a lo anterior y en con el fin de verificar que la Administración cumpla con lo ordenado en la Ley 23 de 1982, se tomó como muestra un total de 150 equipos de cómputo y se procedió con la respectiva verificación del Software instalado en cada uno de ellos, corroborando los controles organizacionales establecidos para la detección de software o aplicaciones ofimáticas no licenciados.

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”.

  <p>Gobernación de Risaralda</p>	<p align="center">Departamento de Risaralda Oficina Asesora 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



1.1. Relación de Equipos revisados:

ESPACIO MUESTRAL			
DATOS POBLACION SEGÚN INVENTARIO EQUIPOS DIRECCIÓN INFORMÁTICA Y SISTEMAS			861
MUESTRA			150
No.	No. AUDITADOS	DEPENDENCIA	EQUIPO AUDITADO
1	20	Despacho del Gobernador	GOBE65088
2			GOBE88931
3			GOBE65143
4			GOBE67879
5			GOBE67099
6			GOBE88830
7			GOBE64043
8			GOBE72715
9			GOBE67878
10			GOBE83339
11			GOBE79796
12			GOBE64042
13			GOBE83622
14			GOBE83444
15			GOBE67877
16			GOBE67090
17			GOBE83345
18			GOBE83388
19			GOBE88863
20			GOBE83443
21	12	Infraestructura	GOBE68261
22			GOBE83647
23			GOBE83592
24			GOBE83646
25			GOBE65097
26			GOBE83448
27			GOBE83361
28			GOBE68313
29			GOBE68264
30			GOBE83595
31			GOBE76504
32			GOBE68298

	No. AUDITADOS	DEPENDENCIA	EQUIPO AUDITADO
33	25	Administrativa	GOBE97947
34			GOBE83599
35			GOBE64045
36			GOBE65045
37			GOBE68248
38			GOBE83153
39			GOBE97946
40			GOBE68048
41			DESKTOP-43MNMIP
42			GOBE83152
43			GOBE83623
44			GOBE64759
45			GOBE97972
46			GOBE67378
47			GOBE50891
48			GOBE83151
49			GOBE67354
50			GOBE83635
51			GOBE97971
52			GOBE83602
53			GOBE64074
54			GOBE76513
55			GOBE88971
56			GOBE83634
57			GOBE67847
58	18	Hacienda	GOBE67073
59			GOBE61893
60			GOBE67893
61			GOBE88885
62			GOBE68334
63			GOBE65076
64			GOBE67081
65			GOBE61861
66			GOBE64269
67			GOBE67079
68			GOBE68333
69			GOBE85416
70			GOBE88884
71			GOBE67834
72			GOBE67624
73			GOBE68046
74			GOBE68332
75			GOBE50865
76			

 	<p align="center">Departamento de Risaralda Oficina Asesora 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

77	No. AUDITADOS	DEPENDENCIA	EQUIPO AUDITADO
78	10	Jurídica	GOBE97961
79			GOBE97965
80			GOBE67060
81			GOBE97958
82			GOBE97957
83			GOBE97950
84			GOBE67048
85			GOBE97956
86			GOBE97962
87			GOBE65190
88	4	Planeación	GOBE64198
89			GOBE61890
90			DESKTOP-R8CCC54
91			GOBE97916
92	5	Desarrollo Agropecuario	GOBE88967
93			GOBE64182
94			GOBE88966
95			GOBE65071
96			GOBE72721
97	10	Gobierno	GOBE61895
98			GOBE68047
99			GOBE88853
100			GOBE65093
101			GOBE88852
102			GOBE64014
103			GOBE64032
104			GOBE88851
105			GOBE61839
106			GOBE65065
107	No. AUDITADOS	DEPENDENCIA	EQUIPO AUDITADO
108	18	Educación	GOBE68083
109			GOBE83364
110			GOBE61865
111			GOBE79783
112			GOBE67796
113			GOBE83463
114			GOBE64308
115			GOBE61972
116			GOBE64079
117			GOBE61968
118			GOBE64077
119			GOBE68080
120			GOBE83070
121			GOBE83652

 	<p align="center">Departamento de Risaralda Oficina Asesora 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

122			GOBE61934
123			GOBE71671
124			CALIDADEQUIPO1
125			GOBE78826
	No. AUDITADOS	DEPENDENCIA	EQUIPO AUDITADO
126	18	Salud	GOBE1VBTPN1
127			GOBE67007
128			GOBE68196
129			GOBE90385
130			GOBE67855
131			GOBE61897
132			GOBE65189
133			GOBE79736
134			GOBE68015
135			GOBE64237
136			GOBE79991
137			GOBE68058
138			GOBE88955
139			GOBE65198
140			GOBE61836
141			GOBE64765
142			GOBE90384
143			GOBE68193
144	4	Desarrollo Económico	GOBE61892
145			GOBE64016
146			ARTESANIA
147	6	Deportes	6QRM7L2
148			GOBE67374
149			GOBE67367
150			GOBE88940
151			GOBE67366
152			GOBE64513
153			GOBE79756

De la revisión se encontraron los siguientes aspectos:

1.2. SOFTWARE INSTALADO:

En la verificación realizada a los 150 equipos relacionados en la tabla anterior, los cuales hacen parte de la muestra tomada, se pudo establecer que en un 90% el software encontrado es el preinstalado por el fabricante.

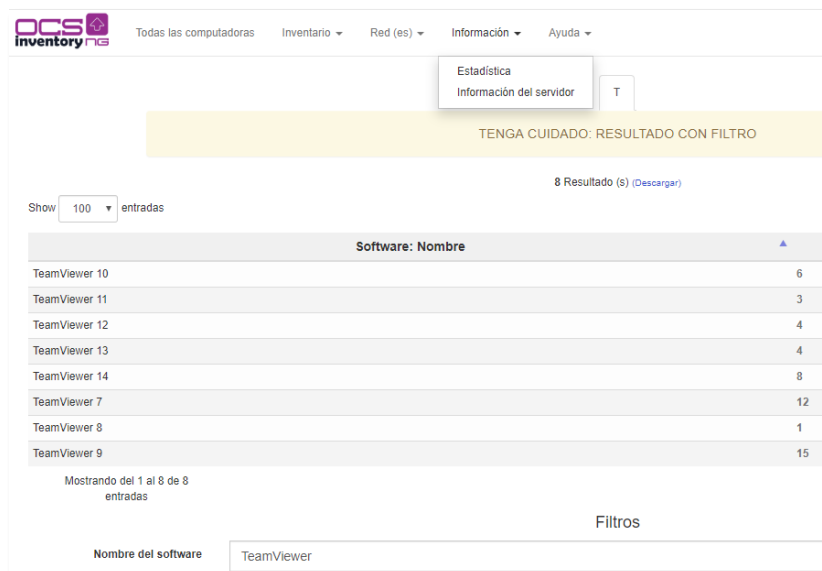
Así mismo se evidencio la existencia de Software instalado por los usuarios finales, de los cuales, tras el análisis y la validación realizada, son considerados software libre, versiones de prueba, aplicaciones para acceder al contenido de equipos móviles (celulares).

Lo anterior se puede considerar como un riesgo, teniendo en cuenta que, por el desconocimiento de estos usuarios, pueden estar instalando software que si requiera de licencia para su uso, lo que acarrearía sanciones a la administración si no se cuenta con las mismas. Por esta razón es un aspecto a tener en cuenta para reforzar las medidas 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, así mismo esto ayuda a aumentar 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 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 al informe arrojado por la herramienta **OCS INVENTORY**:

- Equipo: [GOBE67847](#) / Software: **TeamViewer**: es un software informático 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. Además del equipo referenciado, esta aplicación se encuentra instalada en 52 equipos más, como se observa en la siguiente imagen.

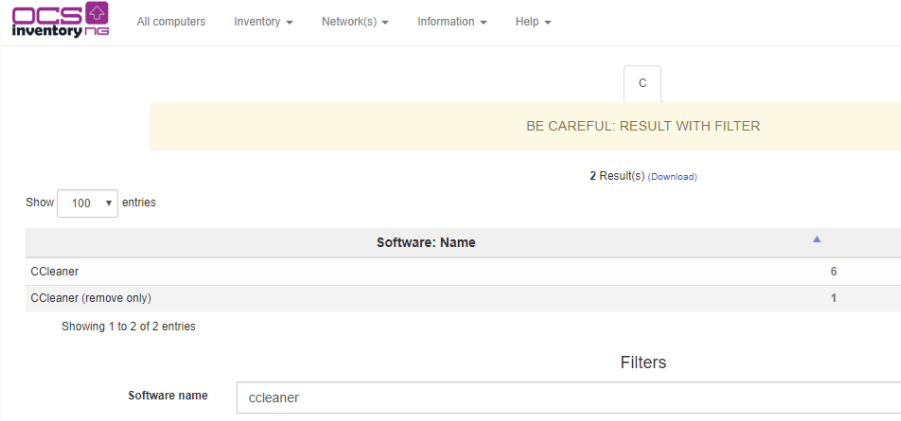


The screenshot shows the OCS Inventory NG web interface. At the top, there are navigation tabs: 'Todas las computadoras', 'Inventario', 'Red(es)', 'Información', and 'Ayuda'. A dropdown menu is open under 'Información', showing 'Estadística' and 'Información del servidor'. Below this, a yellow banner reads 'TENGA CUIDADO: RESULTADO CON FILTRO'. The main content area shows a table of results for 'TeamViewer'. The table has two columns: 'Software: Nombre' and a numerical count. The results are as follows:

Software: Nombre	Count
TeamViewer 10	6
TeamViewer 11	3
TeamViewer 12	4
TeamViewer 13	4
TeamViewer 14	8
TeamViewer 7	12
TeamViewer 8	1
TeamViewer 9	15

Below the table, it says 'Mostrando del 1 al 8 de 8 entradas'. At the bottom, there is a search bar with the text 'Nombre del software' and a filter button labeled 'Filtros'.

- Equipo: [GOBE67378](#) / **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. Además del equipo referenciado, esta aplicación se encuentra instalada en 6 equipos más, como se observa en la siguiente imagen.

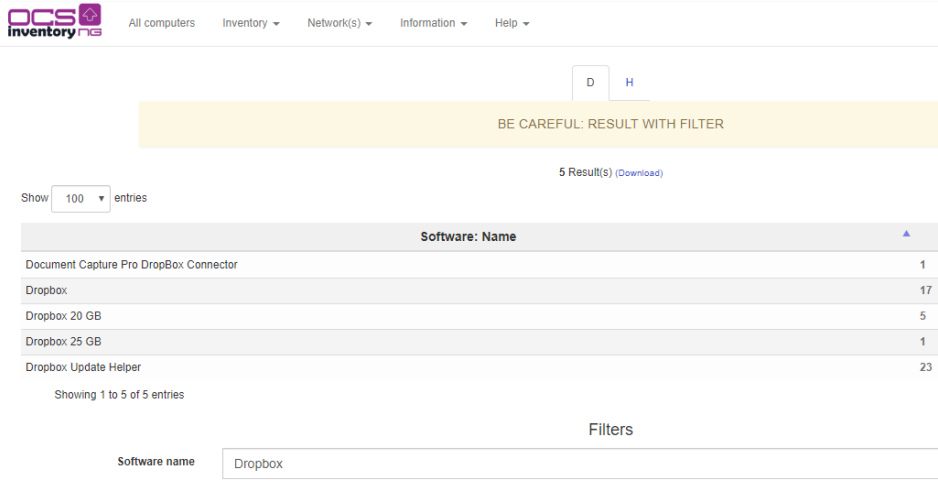


The screenshot shows the OCS Inventory NG web interface. At the top, there are navigation tabs: 'All computers', 'Inventory', 'Network(s)', 'Information', and 'Help'. Below these, a search bar contains the letter 'C'. A yellow banner displays the message 'BE CAREFUL: RESULT WITH FILTER'. Below the banner, it indicates '2 Result(s) (Download)'. A dropdown menu is set to 'Show 100 entries'. The main table has a header 'Software: Name' and a column for the count. The results are as follows:

Software: Name	Count
CCleaner	6
CCleaner (remove only)	1

Below the table, it says 'Showing 1 to 2 of 2 entries'. At the bottom, there is a 'Filters' section with a text input labeled 'Software name' containing the value 'ccleaner'.

- Equipo: [GOBE67090](#) / **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 46 equipos más, como se observa en la siguiente imagen.

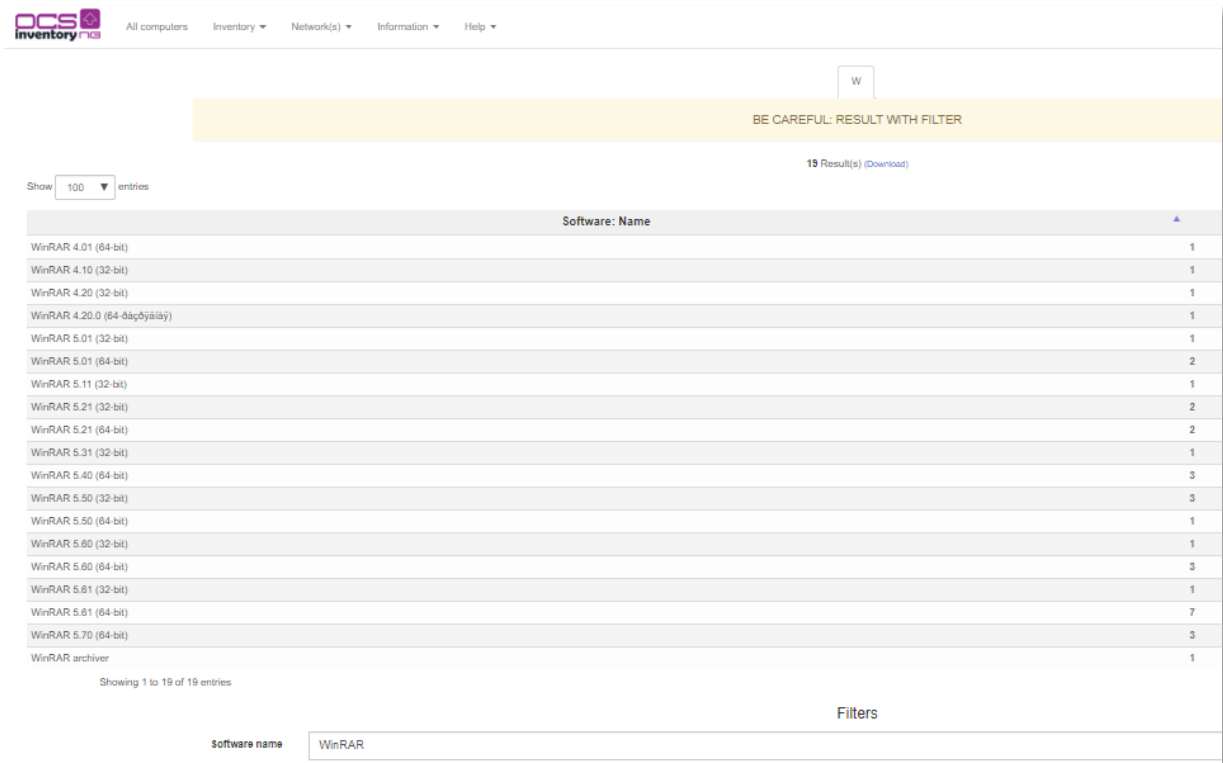


The screenshot shows the OCS Inventory NG web interface. At the top, there are navigation tabs: 'All computers', 'Inventory', 'Network(s)', 'Information', and 'Help'. Below these, a search bar contains the letters 'D' and 'H'. A yellow banner displays the message 'BE CAREFUL: RESULT WITH FILTER'. Below the banner, it indicates '5 Result(s) (Download)'. A dropdown menu is set to 'Show 100 entries'. The main table has a header 'Software: Name' and a column for the count. The results are as follows:

Software: Name	Count
Document Capture Pro DropBox Connector	1
Dropbox	17
Dropbox 20 GB	5
Dropbox 25 GB	1
Dropbox Update Helper	23

Below the table, it says 'Showing 1 to 5 of 5 entries'. At the bottom, there is a 'Filters' section with a text input labeled 'Software name' containing the value 'Dropbox'.

- Equipo: [GOBE88884](#) / 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. Además del equipo referenciado, esta aplicación se encuentra instalada en 35 equipos más, como se observa en la siguiente imagen.





The screenshot shows the OCS Inventory web interface. A search filter 'W' is applied, resulting in 19 entries. The table lists various versions of WinRAR installed on different computers, along with the count of each version.

Software: Name	Count
WinRAR 4.01 (64-bit)	1
WinRAR 4.10 (32-bit)	1
WinRAR 4.20 (32-bit)	1
WinRAR 4.20.0 (64-bit) (64-bit)	1
WinRAR 5.01 (32-bit)	1
WinRAR 5.01 (64-bit)	2
WinRAR 5.11 (32-bit)	1
WinRAR 5.21 (32-bit)	2
WinRAR 5.21 (64-bit)	2
WinRAR 5.31 (32-bit)	1
WinRAR 5.40 (64-bit)	3
WinRAR 5.50 (32-bit)	3
WinRAR 5.50 (64-bit)	1
WinRAR 5.60 (32-bit)	1
WinRAR 5.60 (64-bit)	3
WinRAR 5.61 (32-bit)	1
WinRAR 5.61 (64-bit)	7
WinRAR 5.70 (64-bit)	3
WinRAR archiver	1

1.3. OFFICE

De acuerdo a los registros de Microsoft, La Administración Departamental posee las siguientes licencias en modalidad perpetua. Esta cantidad corresponde a las existentes a la fecha de auditoria:

- 126 Office Pro Plus 2007
- 58 Office Pro Plus 2010
- 3 Office Pro Plus 2016
- 307 Office Pro Plus 2019
- 27 Office Std 2007

 	<p align="center">Departamento de Risaralda Oficina Asesora 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

- 105 Office Std 2010
- 227 Office Std 2013
- 252 Office Std 2016
- 103 Office Std 2019

Para un total de 1208 licencias de Office.

1.4. ANTIVIRUS

Culminada la revisión de los 150 (muestra) equipos de cómputo, se logró evidenciar que cada una de las maquinas cuentan con el Antivirus **KASPERSKY** instalado y vigente; al mismo tiempo se procedió a solicitar a la Dirección de Informática y Sistemas el respectivo contrato de las licencias de uso para el total de equipos de la Administración Departamental.

Por parte del Director de Sistemas, fue suministrado el contrato No. 1612 del 29 de octubre de 2018. Una vez revisado dicho contrato, encontramos que el alcance de este compromete la renovación de 800 licencias del Antivirus **KASPERSKY** ya instalado en los equipos de cómputo de la Administración Departamental, allí mismo encontramos que se contrata el suministro de 100 licencias más. De lo anterior y teniendo en cuenta que el inventario de equipos de cómputo de la Administración Departamental es de 861, se puede establecer que hay cobertura para el total de equipos de cómputo.



1.5. 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:

1.5.1. 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

 	<p align="center">Departamento de Risaralda Oficina Asesora 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

a criterios de búsqueda. Además, tiene muchas opciones más como escanear la red por medio del IPDiscovery, o instalar aplicaciones remotamente creando Builds”.

1.5.2. Revisión y Barrido.

Esta actividad se realiza periódicamente con el apoyo del personal adscrito a la Dirección de Informática y Sistemas y los practicantes del SENA. Para el presente año la Dirección de Informática y Sistemas contrató al técnico Wilson Andrés García, con el fin de apoyar entre otras esta labor.

1.5.3. Implementación 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 está liderando la implementación de un directorio activo, el cual traerá muchos 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.

 	<p align="center">Departamento de Risaralda Oficina Asesora 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

- Replicación: implementa características para la replicación de todos los datos entre servidores del directorio activo.

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



2. Políticas de Operación Seguridad Informática.

“La implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, en la Entidad está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la misma, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.”

Con el fin de mitigar los diferentes riesgos que surgen a causa del valor que cobra el mayor activo de las organizaciones, la información, la Administración Departamental a través del proceso Gestión Informática y Servicios Tecnológicos, liderado por la Dirección de Informática y Sistemas, tiene establecidas las políticas de operación:

- ✓ POLÍTICAS DE OPERACIÓN ACCESO AL CENTRO DE DATOS DEPARTAMENTAL.
- ✓ POLÍTICAS DE OPERACIÓN INTERNA DIS DE SEGURIDAD DE LA INFORMACION.
- ✓ POLÍTICAS DE OPERACIÓN DE SEGURIDAD INFORMÁTICA.

Además de estas se cuenta con el Plan de Seguridad y Privacidad de la Información y la política de seguridad informática, los cuales fueron implementados y socializados, cumpliendo con los lineamientos dados por el Ministerio de las Tecnologías de la Información y Comunicaciones, enmarcado dentro de la Política de Gobierno Digital.

 	<p align="center">Departamento de Risaralda Oficina Asesora 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 acuerdo a lo anterior y en concordancia por lo dispuesto en la Norma Técnica Colombiana ISO 27001/2013 y las Políticas de Operación de Seguridad Informática, establecidas por la Administración Departamental, se efectuó la evaluación respectiva, de los siguientes puntos:

2.1. NTC ISO 27001 V2013

2.1.1. A.5 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

2.1.1.1. A.5.1.1 Políticas de la seguridad de la información.

“Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la Dirección, publicada y comunicada a los empleados y partes externas pertinentes.”

Se evidenció la socialización de las políticas para la seguridad de la información, la cual se realiza por medio de correos electrónicos y SAIA.

2.1.1.2. A.5.1.2 Revisión de las Políticas para la seguridad de la información.

“Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si se producen cambios significativos, para asegurar su conveniencia, suficiencia y eficacia continua.”



Se evidenció la revisión y actualización de las Políticas de seguridad de la información por parte de los responsables del proceso de Gestión Informática y Servicios Tecnológicos, tal como se evidencia en el memorando No. 11849 del 24 de agosto de 2018.

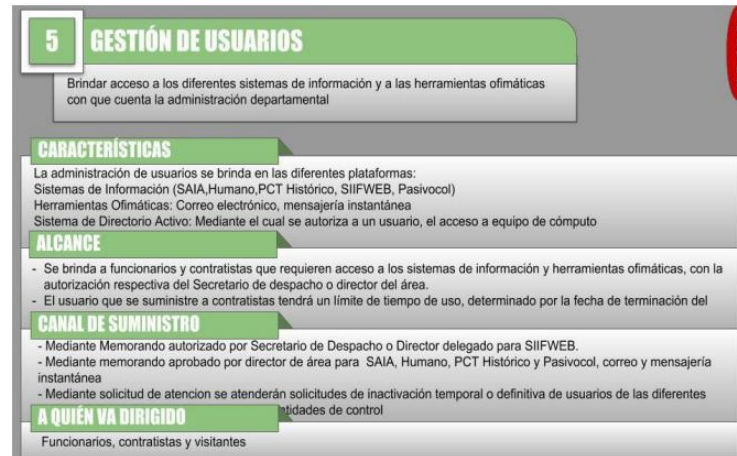
2.1.2. A.9 CONTROL DE ACCESO

2.1.2.1. A.9.2.1 Registro y Cancelación del registro de usuarios.

“Se debe implementar un proceso formal para el registro y cancelación de registro de usuarios, para posibilitar la asignación de derechos de acceso.”

El proceso de Gestión Informática y Servicios Tecnológicos implementó el catálogo de servicios, en el cual se crea la Gestión de Usuarios y en este se explica el procedimiento de registro y cancelación de usuarios.

  <p>Gobernación de Risaralda</p>	<p align="center">Departamento de Risaralda Oficina Asesora 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



2.1.2.2. A.9.2.3 Gestión de Derechos de Acceso privilegiado.

“Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.”

Con la implementación del catálogo de Servicios, se crea la Gestión de Usuarios, esto apoyado del Directorio Activo, mediante el cual se realizará la asignación de privilegios a los usuarios.

2.1.2.3. A.9.2.5 Revisión de los derechos de acceso de los usuarios.



“Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.”

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. Además de estas acciones, la entrada en funcionamiento del Directorio Activo, será una herramienta muy eficiente para realizar este tipo de controles.

2.1.3. A.9 SEGURIDAD FISICA Y DEL ENTORNO

2.1.3.1. Controles de Acceso Físicos

“Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado.”

 	<p align="center">Departamento de Risaralda Oficina Asesora 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 se evidenciaron controles de acceso apropiados por parte de la Dirección de Informática y Sistemas, ya que, en el momento de la visita de auditoria se evidenció el ingreso de personas ajenas a ese Despacho. Según lo manifestado por el Director, esto es debido a que desde hace algunos meses fue trasladada la oficina de cobro coactivo a ese Despacho, y por lo tanto las personas que frecuentan esta oficina son ciudadanos realizando las respectivas reclamaciones o acuerdos de pago, lo que vulnera potencialmente la seguridad de la información que se gestiona en la Dirección.

En este punto debemos tener en cuenta que el objetivo de la “Seguridad Física y del Entorno” es *“evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información y de los servicios de procesamiento de información”*.

2.2. POLITICAS DE OPERACIÓN DE SEGURIDAD INFORMATICA.



2.2.1. *“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.”.*

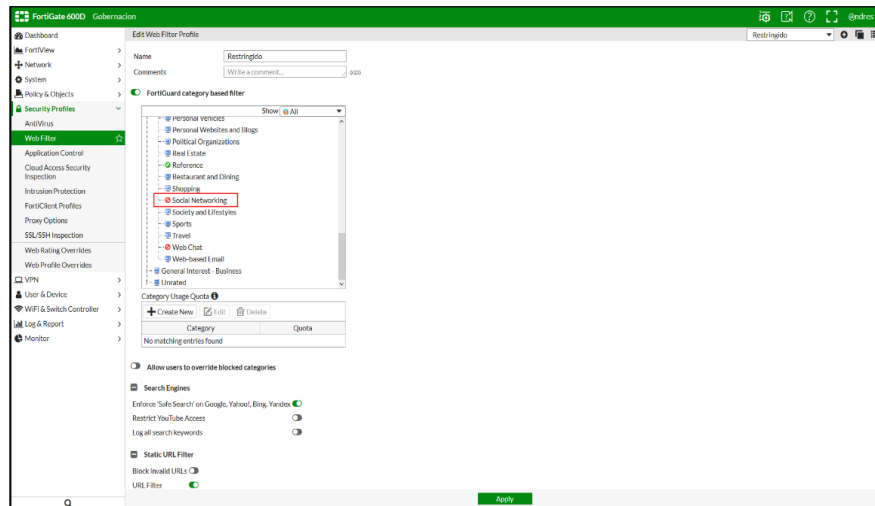
La suspensión de cualquiera de los servicios es notificada mediante los canales de comunicación habilitados al interior de la Administración Departamental tales como:

- ✓ SAIA
- ✓ SPARK
- ✓ Correo Electrónica

2.2.2. *“No se permite el acceso a redes Sociales y contenido multimedia a excepción de las solicitudes específicas 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 evidencia la aplicación de políticas de restricción y bloqueo para páginas web con contenido sexual y redes sociales, mediante firewall Fortigate, por parte de la Dirección de Informática y Sistemas.

 	<p align="center">Departamento de Risaralda Oficina Asesora 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

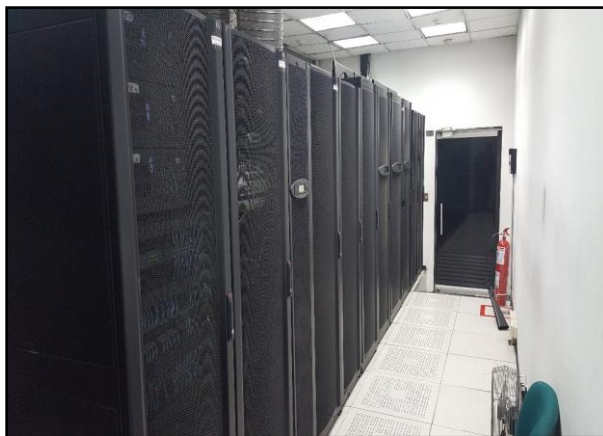




2.3. POLÍTICAS DE OPERACIÓN INTERNA DIS DE SEGURIDAD DE LA INFORMACION.

2.3.1. ÁMBITO FÍSICO

2.3.1.1. “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 evidencio 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.



 	<p align="center">Departamento de Risaralda Oficina Asesora 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

2.4. ÁMBITO DE ADMINISTRACIÓN DE LAS BASES DE DATOS DE LOS SISTEMAS DE INFORMACIÓN.

2.4.1. *“La Dirección de Informática y Sistemas asignará por escrito los administradores de cada base de datos, a razón de la ejecución de sus funciones.”*

Se evidenció que mediante el formato denominado “ASIGNACIÓN DE PERMISOS A BASE DE DATOS” se están realizando los registros de la asignación formal para la administración de bases de datos.



2.4.2. *“Cada administrador deberá llevar bitácora de actualizaciones de base de datos directamente desde el motor.”*

Se evidenció que el administrador de Bases de Datos de la Dirección de Informática y Sistemas lleva el registro de las actualizaciones de las BD.

EVENTO	DESCRIPCION	DOCUMENTO	NUMERO	DISPOSITIVO
Actualización de sistema operativo	Se ejecutó comando "yum update -y" para actualizar el sistema operativo	/var/log/yum.log	N/A	Servidor de Bases de Datos PostgreSQL (Nuevo)
Actualización de sistema operativo	Se ejecutó comando "yum update -y" para actualizar el sistema operativo	/var/log/yum.log	N/A	Servidor de Bases de Datos PostgreSQL (Nuevo)
Actualización de sistema operativo	Se ejecutó comando "yum update -y" para actualizar el sistema operativo	/var/log/yum.log	N/A	Servidor de Bases de Datos PostgreSQL (Nuevo)
Actualización de sistema operativo	Se ejecutó comando "yum update -y" para actualizar el sistema operativo	/var/log/yum.log	N/A	Servidor de Bases de Datos Oracle 12c
Actualización de sistema operativo	Se ejecutó comando "yum update -y" para actualizar el sistema operativo	/var/log/yum.log	N/A	Servidor de Bases de Datos Oracle 12c
Actualización de sistema operativo	Se ejecutó comando "yum update -y" para actualizar el sistema operativo	/var/log/yum.log	N/A	Servidor de Bases de Datos PostgreSQL (Nuevo)
Actualización de sistema operativo	Se ejecutó comando "yum update -y" para actualizar el sistema operativo	/var/log/yum.log	N/A	Servidor de Bases de Datos Oracle 12c
Actualización de sistema operativo	Se ejecutó comando "yum update -y" para actualizar el sistema operativo	/var/log/yum.log	N/A	Servidor de Bases de Datos PostgreSQL (Nuevo)
Actualización de sistema operativo	Se ejecutó comando "yum update -y" para actualizar el sistema operativo	/var/log/yum.log	N/A	Servidor de Bases de Datos Oracle 12c
Actualización de sistema operativo	Se ejecutó comando "yum update -y" para actualizar el sistema operativo	/var/log/yum.log	N/A	Servidor de Bases de Datos Oracle 12c
Actualización de sistema operativo	Se ejecutó comando "yum update -y" para actualizar el sistema operativo	/var/log/yum.log	N/A	Servidor de Bases de Datos PostgreSQL (Nuevo)

2.4.3. *“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.”*

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

 	<p align="center">Departamento de Risaralda Oficina Asesora 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

un ajuste a su aplicación a nivel de BD, este envía al Administrador el Script para ejecutar la respectiva actualización.

2.4.4. *“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 solo para el aplicativo SAIA, para el resto de aplicaciones no se tiene implementado, ya que no se cuenta con la infraestructura tecnológica (Licencias adicionales de Oracle + infraestructura) para su implementación.

2.4.5. *“Los administradores de base de datos deberán verificar la realización de las copias de seguridad y comprobar su correcta restauración al menos una vez al mes.”.*

Se evidenció que el administrador de las Bases de Datos verifica la realización de copias de seguridad, pero que, por falta de infraestructura tecnológica, no se pueden realizar las pruebas de restauración a las mismas.

2.5. ÁMBITO DE ADMINISTRACIÓN DE LOS DISPOSITIVOS ACTIVOS DE RED.

2.5.1. *“La Dirección de Informática y Sistemas asignará por escrito la administración de los dispositivos de red.”.*



No se evidenciaron registros de la asignación formal para la administración de dispositivos de red.

2.5.2. *“La Dirección de Informática y Sistemas asignará por escrito la administración de servidores en sus sistemas operativos y configuraciones.”.*

No se evidenciaron registros de la asignación formal para la administración de Servidores.

2.5.3. *“Todas las claves deben ser cambiadas por lo menos cada 3 meses y actualizadas en el archivo de claves.”.*

Se evidenció el cumplimiento de esta política por parte de la Dirección de Informática y Sistemas.

 	<p align="center">Departamento de Risaralda Oficina Asesora 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

2.6. POLÍTICAS DE OPERACIÓN ACCESO AL CENTRO DE DATOS DEPARTAMENTAL.

2.6.1. *“El Director de Informática y Sistemas delegará mediante memorando la administración del control de acceso.”*

No se evidenció el cumplimiento de esta política por parte de la Dirección de Informática y Sistemas.

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

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



1. *Interrupción del servicio de red de datos.*
2. *Inoperatividad de elementos de hardware en estaciones de trabajo.*
3. *Ausencia del Servicio de Internet.*
4. *Pérdida de la Información.*
5. *Sanciones de tipo legal por uso de software no licenciado.*

Una vez validados estos riesgos, se evidenció lo siguiente:

RIESGO	OBSERVACIONES	VALORACIÓN DE CONTROLES
1 - Interrupción del servicio de red de datos	No se evidenciaron segundo y tercer seguimiento (septiembre 2018 y enero 2019)	los controles están valorados, pero no cuenta con responsable para el control No. 1
2 - Inoperatividad de elementos de hardware en estaciones de trabajo.		los controles están valorados, pero no cuenta con responsable para el control No. 1
3 - Ausencia del Servicio de Internet		Controles valorados y con sus respectivos responsables
4 - Pérdida de la Información		Controles valorados y con sus respectivos responsables
5 - Sanciones de tipo legal por uso de software no licenciado		Controles valorados y con sus respectivos responsables

4. Riesgos de Corrupción del proceso Gestión Informática y Servicios Tecnológicos.

El proceso de Gestión Informática y Servicios Tecnológicos, tiene identificado un riesgo de corrupción dentro de su proceso:

 	<p align="center">Departamento de Risaralda Oficina Asesora 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. *Manipulación, adulteración o destrucción de la información digital de la entidad por parte de los administradores de las bases de datos a beneficio particular o de terceros.*

Una vez validados estos riesgos, se evidenció lo siguiente:

- El segundo seguimiento se realizó extemporáneamente.
- No se evidenció el tercer seguimiento, correspondiente al tercer cuatrimestre.

HALLAZGOS

HALLAZGOS POSITIVOS:

- Existe una muy buena disposición por parte de los responsables del proceso de Gestión Informática y Servicios Tecnológicos, esto de acuerdo a su proactividad y el querer trabajar en pro de garantizar la seguridad y privacidad 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. Con la implementación del Directorio Activo seguramente este riesgo será mitigado con mayor eficacia.
- Se valora la buena adquisición y administración de las licencias de uso de los Sistemas de Información utilizados por la Administración Departamental.
- Es de valorar el esfuerzo hecho por la Administración Departamental para la adquisición de nuevas licencias de Antivirus, logrando con ello cobertura total de los equipos, con oportunidad de escalamiento, y mitigando un riesgo de seguridad.



HALLAZGOS NEGATIVOS:

I. Hallazgo No. 1

2.1.3 A.9 SEGURIDAD FISICA Y DEL ENTORNO

2.1.3.1 11.1.2 Controles de Acceso Físicos

“Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado.”.

 	<p align="center">Departamento de Risaralda Oficina Asesora 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 se evidenciaron controles de acceso apropiados por parte de la Dirección de Informática y Sistemas, ya que en el momento de la visita de auditoria, se evidenció el ingreso de personas ajenas a ese Despacho. Según lo manifestado por el Director, esto es debido a que desde hace algunos meses fue trasladada la oficina de cobro coactivo a ese Despacho, y por lo tanto las personas que frecuentan esta oficina son ciudadanos realizando las respectivas reclamaciones o acuerdos de pago, lo que vulnera potencialmente la seguridad de la información que se gestiona en la Dirección, incumpliendo de esta manera con los requisitos establecidos en la NTC ISO 27001 V2013.

II. Hallazgo No. 2

2.4 ÁMBITO DE ADMINISTRACIÓN DE LAS BASES DE DATOS DE LOS SISTEMAS DE INFORMACIÓN.

***2.4.4** “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.”.*

No se evidenciaron ambientes de prueba para la validación de ajustes y/o actualizaciones de los aplicativos de la Administración Departamental, incumpliendo de esta manera con la política de operación establecida.

III. Hallazgo No. 3



***2.4.5** “Los administradores de base de datos deberán verificar la realización de las copias de seguridad y comprobar su correcta restauración al menos una vez al mes.”.*

No se evidenció la validación de pruebas de restauración, a las copias de seguridad realizadas, incumpliendo de esta manera con la política de operación establecida.

IV. Hallazgo No. 4

2.5 ÁMBITO DE ADMINISTRACIÓN DE LOS DISPOSITIVOS ACTIVOS DE RED.

***2.5.1** “La Dirección de Informática y Sistemas asignará por escrito la administración de los dispositivos de red.”.*

 	<p align="center">Departamento de Risaralda Oficina Asesora 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 se evidenciaron registros de la asignación formal para la administración de dispositivos de red, incumpliendo de esta manera con la política de operación establecida

V. Hallazgo No. 5

2.5.2 *“La Dirección de Informática y Sistemas asignará por escrito la administración de servidores en sus sistemas operativos y configuraciones.”.*

No se evidenciaron registros de la asignación formal para la administración de Servidores, incumpliendo de esta manera con la política de operación establecida.



VI. Hallazgo No. 6

2.6.1 *“El Director de Informática y Sistemas delegará mediante memorando la administración del control de acceso.”.*

No se evidenció el cumplimiento de esta política por parte de la Dirección de Informática y Sistemas, incumpliendo de esta manera con la política de operación establecida.

OBSERVACIÓN:

- I. Sería de gran importancia que la Dirección de Informática y Sistemas realizará revisiones periódicas al software instalado en los equipos de cómputo, esto con el fin de eliminar los aplicativos que no están relacionados directamente con las labores de la Administración (WinRAR, Dropbox, iTunes, Ccleaner, etc.), ocupando espacio en los discos duros y generando posibles accesos a virus informáticos.
- II. Si bien es cierto desde la Dirección de Informática se ha hecho un trabajo importante a través de los informes de obsolescencia y memorandos dirigidos a los Secretarios de Despacho, para dar de baja los equipos de cómputo con Sistema Operativo Windows XP, para el cual Microsoft ha dejado de proporcionar actualizaciones de seguridad y soporte técnico desde el 8 de abril de 2014, en el desarrollo de la auditoría, se evidenció el uso de estos. Por lo anterior es de gran importancia que la Dirección de Informática y Sistemas implemente un plan de acción de migración a otras versiones de software, para dar solución a dicha situación.
- III. Si bien es cierto desde la Dirección de Informática se ha hecho un trabajo importante a través de los informes de obsolescencia y memorandos dirigidos a los Secretarios de Despacho, sobre el uso de software ofimático: Microsoft Office XP (también

 	<p align="center">Departamento de Risaralda Oficina Asesora 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

llamado Office 2002), Office 2003 y Office 2007, para los cuales Microsoft ha dejado de proporcionar actualizaciones de seguridad y soporte técnico, en el desarrollo de la auditoría, se evidenció el uso de estos. Por lo anterior es de gran importancia que la Dirección de Informática y Sistemas implemente un plan de acción de migración a otras versiones de software, para dar solución a dicha situación.

CONCLUSIONES

En el desarrollo de la presente auditoria se evidenció una buena disposición de los funcionarios y contratistas pertenecientes a la Dirección de Informática y Sistemas por promover el cumplimiento de las normas de protección de derechos de autor y por el aseguramiento de la información generada por los diferentes procesos de la Administración Departamental.

Se puede concluir que la Administración Departamental a través de la Dirección de Informática y Sistemas, ha venido realizando un buen trabajo a fin de dar cumplimiento con lo establecido por la Ley en cuanto a la protección de derechos de autor. De igual manera se refleja positivamente la implementación de controles tales como el Directorio activo que es una excelente herramienta para la asignación de permisos a los recursos de la red, mitigando con esto el riesgo de descarga, instalación y uso de software no licenciado por parte de los funcionarios.

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 en garantizar la integridad, oportunidad y calidad 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 al incumplimiento de algunos de los requisitos de la NTC ISO 27001/2013 y las políticas de operación de la seguridad informática del proceso.

Para finalizar, es importante que desde la alta dirección se siga brindando el apoyo necesario para continuar con el cumplimiento de estos objetivos. Esto si tenemos en cuenta los recursos con los que cuenta el área de informática y sistemas. La necesidad de infraestructura tecnológica y de recurso humano para la administración de la misma es evidente.

Luis Alexander Vásquez
Auditor.