ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"IMPLEMENTACIÓN DE UNA SOLUCIÓN DATA LOSS PREVENTION (DLP) EN UNA EMPRESA CON ACTIVIDADES DE SERVICIOS ALIMENTICIOS"

EXAMEN DE GRADO (COMPLEXIVO)

PREVIO A LA OBTENCIÓN DEL GRADO DE:

MAGÍSTER EN SEGURIDAD INFORMÁTICA APLICADA

LEONARDO ANTONIO HEINERT VILLACIS

GUAYAQUIL – ECUADOR

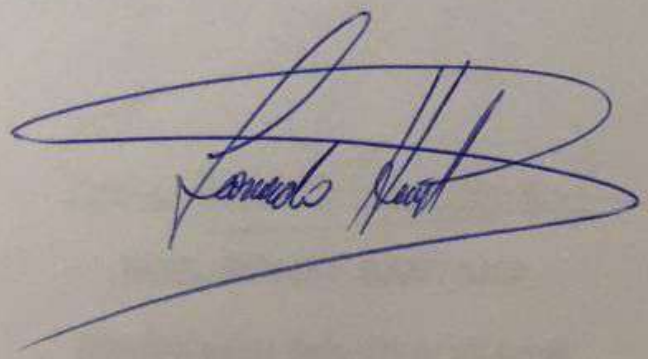
AÑO: 2016

AGRADECIMIENTO

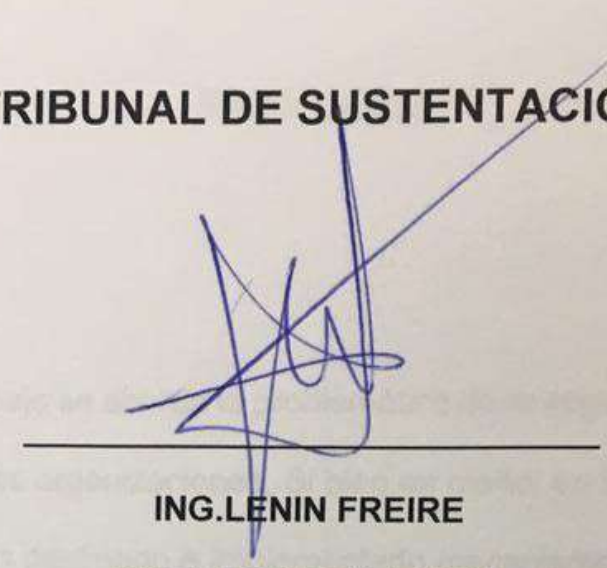
Quiero agradecer a mi familia ya que es el pilar fundamental en mi vida, sin ellos hubiera sido imposible culminar mi proyecto. A mi madre por su fortaleza y dedicación. A mis hermanos por su guía en todo instante, en especial a mis hermanas Olga Maria y Dora Leonor. A mi esposa por todo el apoyo incondicional, a mis amigos por su amistad a lo largo de mi vida.

DEDICATORIA

Dedico este proyecto a mi esposa, mi hijo Leonardo Antonio (Mi campeón) y nuestro hijo que está por nacer, ellos han sido la energía para continuar cada día. Los amo.

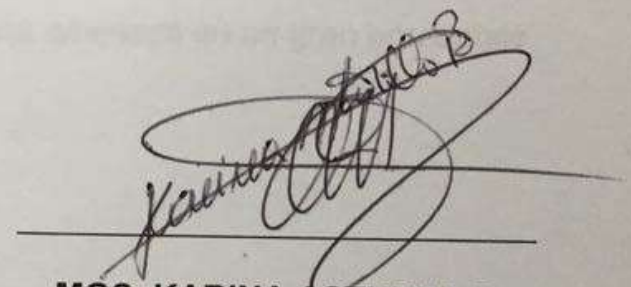


TRIBUNAL DE SUSTENTACIÓN



ING.LENIN FREIRE

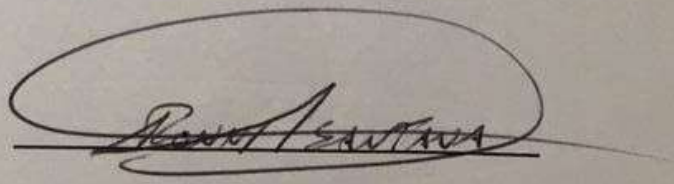
DIRECTOR DE LA MSIA



MGS. KARINA ASTUDILLO

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA



MGS. RONNY SANTANA

PROFESOR DELEGADO POR

LA UNIDAD ACADÉMICA

RESUMEN

En el presente trabajo se aborda la problemática de la seguridad referente a la fuga de datos en las organizaciones. Si bien en cierto, en los últimos años las organizaciones han destinado e implementado mecanismos de seguridad, no está cubierto en su totalidad, los factores internos es una afectación aun considerada como una amenaza en un gran porcentaje.

En la actualidad, existen soluciones en el mercado, de las cuales se presentan sus características principales, destacando la solución seleccionada. Se realiza la implementación, presentando los resultados de acuerdo a las configuraciones realizadas.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

BYOD	Bring Your Our Device
Code QR	Quick Response code
DLP	Data Loss Prevention (Prevención de pérdida de datos)
MDM	Mobile Device Management
SMS	Short Message Service
SMTP	Simple Management Transfer Protocol

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En la actualidad, el concepto de seguridad informática ha tomado mucha importancia, no solo por la gran cantidad de ataques cibernéticos que han sufrido importantes organizaciones, y otras más pequeñas, que tal vez se encuentren en el anonimato, sino por el crecimiento acelerado y cuantiosas pérdidas que se han generado. Por todo lo anterior, las organizaciones se han visto en la necesidad, de destinar presupuesto para la implementación de nuevos mecanismos de seguridad.

Sin embargo, estos mecanismos previenen la pérdida de información y ataques informáticos desde el exterior, pero otra amenaza que se debe enfrentar, son las del factor interno: Los empleados, donde generalmente la pérdida de información se da en forma intencional o por desconocimiento.

En el capítulo I, se aborda de forma general todo lo relacionado a la seguridad en las organizaciones, las amenazas y riesgos a los que están expuestos. En el capítulo II, se realiza un estudio de varias soluciones DLP, existentes en el mercado, con sus principales características, destacando la solución seleccionada.

En el capítulo III, se presenta la instalación y configuración de la solución, así como el detalle de las pruebas realizadas posteriormente, evidenciando las fortalezas de la solución para la prevención de fuga de datos.

CAPÍTULO 1

GENERALIDADES

1.1. DESCRIPCIÓN DEL PROBLEMA

En la actualidad, para muchas organizaciones sin importar su giro de negocio, la información se ha convertido en el activo más importante que pueden poseer, y de acuerdo con las últimas tendencias, donde las tecnologías de la información crecen de forma exponencial, provocando la generación de información digital, la cual se ha incrementado por su facilidad de uso, almacenamiento y transportación, considerándolo como un recursos dependiente para alcanzar los objetivos fijados por las organizaciones [1].

Por lo general, la información puede clasificarse en información “Sensible”, que es utilizada por personas privilegiadas dentro de la organización, e información “Registrada” que es utilizada por usuarios con permisos para manipularla [1]. Sin embargo, para cualquiera de estas clasificaciones el riesgo de pérdida, robo o mala utilización es alto, debido a factores como:

- *Empleados de la organización*: Quienes son considerados como uno de los peligros más significativos para la información, inclusive más que un hacker, debido a que poseen acceso legitimo a las aplicaciones y sistemas internos [2].
- *Movilidad:* Debido al uso creciente de información digital, ha simplificado su transportación a través de correos electrónicos, dispositivos móviles, y la nube, cada vez, es más frecuente que dentro de la organización los empleados conecten sus dispositivos móviles que se conectan a las redes wifi, generando más posibilidades de fugas de información [3].
- *Accesos externos:* Provocados por personas malintencionadas cuyo propósito es robar la información o causar daño a la organización. Para ello, los administradores de sistemas implementan herramientas y mecanismos de protección existentes.

1.2. SOLUCIÓN PROPUESTA

La solución que se propone es la implementación de una herramienta para la Prevención de fuga de datos (DLP), que tiene como objetivo evitar la fuga de información ya sea a través de puertos o dispositivos móviles u otros canales de comunicación como Correo electrónico, mensajería instantánea, redes sociales o la nube [4].

Las soluciones DLP, incluyen un conjunto de tecnologías que persiguen tres objetivos claves:

- Ubicar y catalogar información sensitiva almacenada en la empresa.
- Monitorear y controlar el movimiento de información sensitiva a través de las redes de la empresa.
- Monitorear y controlar el movimiento de información sensitiva en sistemas de usuarios finales [1].

Para ello, es importante comprender todo lo relacionado con la información sensible de la organización, es decir, conocer ¿dónde se encuentra almacenada?, ¿Quiénes son los usuarios que poseen permisos para manipularla?, ¿Cómo la están usando?, para poder establecer una estrategia que comprenda la creación de políticas y mecanismos que controlen y eviten la fuga de la información.

La tecnología incluida en las soluciones DLP, permiten abarcar los tres estados básicos de la información:

- **Datos en Reposo:** Información que puede estar almacenada, compartida o incluso en estaciones de trabajo. Las soluciones DLP poseen rastreadores, que proporciona la posibilidad de ubicar archivos con determinadas extensiones, buscar dentro de ellos información específica, por ejemplo: Números de tarjetas de crédito, o números de seguridad social.
- **Datos en movimiento**: Consiste en un monitoreo en dispositivos específicos de la red, analizando de manera pasiva el tráfico de la red. Posteriormente la información es analizada, de una forma similar a los datos en reposo, para identificar si alguna parte del contenido está restringido en el conjunto de reglas.

- **Datos en Uso**: Es una de las funcionalidades más destacadas, ya que el análisis se realiza en las estaciones de trabajo, para identificar el movimiento de información a dispositivos móviles (USB), o la clonación de información de los sistemas de la organización.

***Figura 1**. Esquema de control de datos*

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

2.1 ANÁLISIS PREVIO A IMPLEMENTACIÓN

2.1.1 ANÁLISIS INICIAL DE LA INFRAESTRUCTURA

Actualmente la organización cuenta con una red distribuida de 30 usuarios, un servidor de archivos y un enlace de datos hacia su Data Center por donde navegan hacia el Internet.

El servidor de Active Directory, firewall, contable, base de datos y el servidor web se encuentran ubicados en el Data Center, por lo tanto, la implementación de la solución de DLP se lo realizará en el servidor disponible en su oficina principal.

2.1.2 ESTUDIO DE SOLUCIONES EXISTENTES

En la actualidad las soluciones DLP han tomado mayor fuerza, debido al incremento de ciberdelincuencia e inseguridad de la información. De acuerdo con un estudio de seguridad global, realizado por la empresa Deloitte, se indica que, aunque muchas organizaciones grandes como bancos, seguros y gobiernos. Han implementado infraestructura y políticas de seguridad para preservar la seguridad de la información, existen aún un gran porcentaje de organizaciones que no han implementado ninguna seguridad, siendo blanco fácil de ataques y perdida de información [5].

Según, el estudio mencionado el 70 % de las organizaciones encuestadas, habían destinado presupuesto para implementar mecanismos de seguridad, y aunque hacen uso de nuevas tecnologías como la nube, mensajería instantánea y redes sociales, un tercio de los encuestados había optado por restringir el uso de las redes, y el 50 % implementado políticas de utilización de la nube [5].

McAfee es un fabricante reconocido especialista en Antivirus, en la actualidad ha sumado a su portafolio con diversidad de productos, protección para datos a través de soluciones DLP. Si bien es cierto, es un fabricante conocido, tiene pocos años en la línea de DLP. Además, su sistema de licenciamiento hace su adquisición compleja y dependiente de la utilización de sus productos bases (antivirus).

Por otra parte, Symantec también posee dentro de su portafolio de productos una solución DLP, que posee herramientas de monitoreo, protección y gestión de políticas de seguridad, sin embargo, no cuenta con una cobertura total, a través de un solo producto, es decir, posee una diversidad segmentada de protección de datos en la nube, en móviles, en puestos de trabajo etc., lo que encarece la solución y hace compleja su implementación.

EndPoint Protector, pertenece al fabricante CoSoSys, fundado en 2004, desarrollador líder totalmente orientado a la protección y seguridad de los datos de las organizaciones, "Data Loss Prevention" (DLP), con un amplio portfolio de soluciones de seguridad para protección de contenidos, monitorización de la actividad de los dispositivos, cifrado de datos, sincronización de datos y mucho más.

La implementación de esta solución, se centra en dos etapas: Monitorización y configuración de los controles, buscando disminuir numerosas vulnerabilidades [6].

2.1.3 SOLUCIÓN DEFINITIVA

Los fabricantes mencionados anteriormente, se encuentran mundialmente reconocidos por sus soluciones, en la actualidad se han enfocado en mercado específicos de la seguridad de la información como son los DLP, sin embargo, por su diversidad y segmentación de servicios, se vuelve compleja la implementación de estas soluciones.

Por su parte, Endpoint Protector, está incluida entre las 50 compañías de tecnología de más rápido crecimiento por Deloitte Technology FAST 50 central Europe en 2011, ganador de la mejor solución DLP en el año 2014,2015 entre otros reconocimientos a su destacada trayectoria y especialización en productos de seguridad específicamente soluciones DLP. No posee segmentación de los servicios, al estar todos incluidos en un solo producto, que permitirá monitorizar los datos no estructurados en cualquier ubicación [7].

Figura 2. Esquema general de la descripción de servicios de EndPoint Protector

Entre las opciones que incluye Endpoint Protector, está el control de dispositivos, que de forma granular permite administrar dispositivos USB, así como otros dispositivos de almacenamiento.

Figura 3. Descripción general de los dispositivos compatibles.

Por otro parte, el servicio de Content Aware protection permite la administración y monitorización de datos considerados como confidenciales o sensibles, a través de diversos puntos de salida como: E-mail, redes sociales, mensajería instantánea, almacenamiento en la nube, estableciendo permisos, filtros y alertas como parte de su conjunto de reglas.

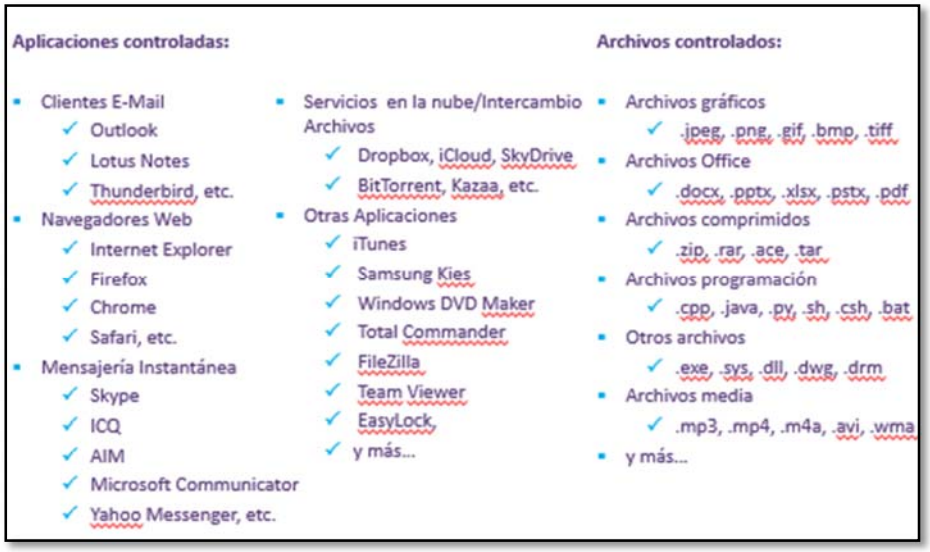


Figura 4. Esquema general del tipo de aplicaciones soportadas por DLP Endpoint protector

2.2 DISEÑO

El diseño de red donde se implementaría la solución DLP es la siguiente:

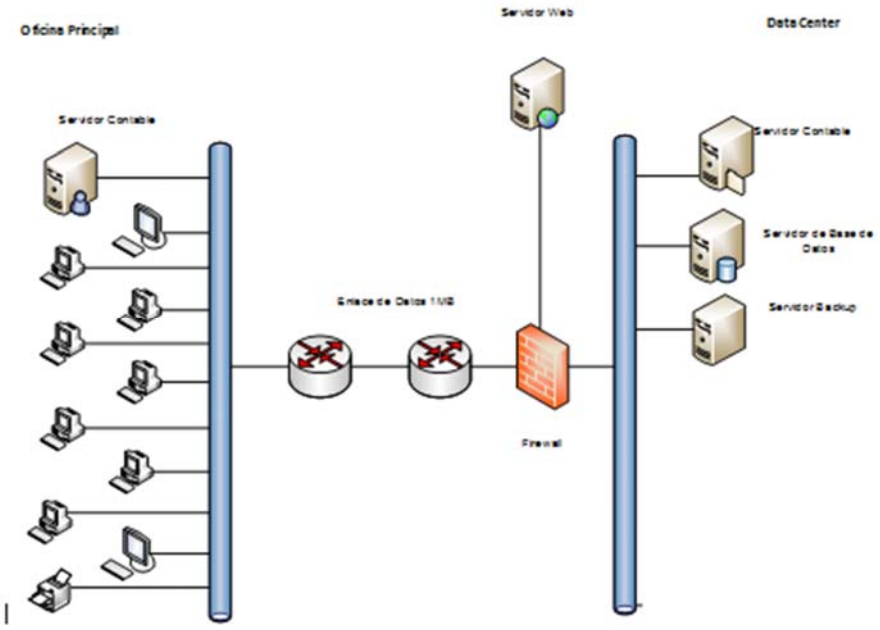


Figura 5. Diseño de la red donde se implementará la solución DLP.

2.3 INSTALACIÓN Y CONFIGURACIÓN

Para la instalación del servidor virtual, se debe considerar la cantidad de usuarios que se van a monitorizar, de acuerdo con esto se establecen unos requerimientos mínimos de virtualización.

Tabla 1 .Requerimiento mínimos para la virtualización.

REQUERIMIENTOS	CLIENTES 24	CLIENTES 60	CLIENTES 100	CLIENTES 300	CLIENTES > 1200
CAPACIDAD	20	50	100	250	1000
CAPACIDAD ADICIONAL	4	10	20	50	200
PROCESADOR	Single - core	Single - core	Dual - core	Dual - core	Quad- core 1X
DISCO	320 Gb	320 Gb	500 Gb	1 Tb – 2 Tb	2X 1 Tb (raid 1 si es NAS)
MEMORIA RAM	2048 Mb	2048 Mb	2048 Mb	4096 Mb	>= 4096

Fuente: Datasheet Endpoint Protector

Posteriormente, se realiza la Importación de la máquina virtual versión 4.4.0.4 en el servidor de virtualización del cliente. La solución de DLP es compatible en los siguientes entornos virtuales.

Entornos Virtuales Soportados	Versión	.ovf	.vmx	.vhd	.xva	.pvm
VMware Workstation	7.1.4	-	*	-	-	-
VMware Workstation *	9.0.2	*	*	-	-	-
VMware Player *	6.0.0	*	*	-	-	-
VMware Fusion *	5.0.0	-	*	-	-	-
VMware vSphere (ESXi)	5.1.0	*	-	-	-	-
Oracle VirtualBox	4.2.18	*	-	-	-	-
Parallels Desktop for Mac	9.0.2	-	-	-	-	*
Microsoft Hyper-V Server	2008/2012	-	-	*	-	-
Citrix XenServer 64bit	6.2.0	-	-	-	*	-

Figura 6.Servidores de virtualización compatibles

- De acuerdo al tipo de Licenciamiento de los módulos se debe Introducir las claves de acuerdo al producto adquirido.

2.3.1 Configuración de la herramienta

Una vez que se importa el servidor virtual, se puede acceder al panel de administración del Endpoint protector, donde se realizan

las configuraciones de las reglas o políticas en diferentes niveles: un equipo especifico, un grupo o a nivel global.

La configuración en los equipos o grupos, no son obligatorias, mas no así la configuración global; al no existir las dos primeras, automáticamente la herramienta asume lo establecido en la configuración global. Se configuran aspectos como tiempos de actualización, tipos de archivos que serán expuestos a monitorización, filtros por palabras o términos específicos, informes etc.

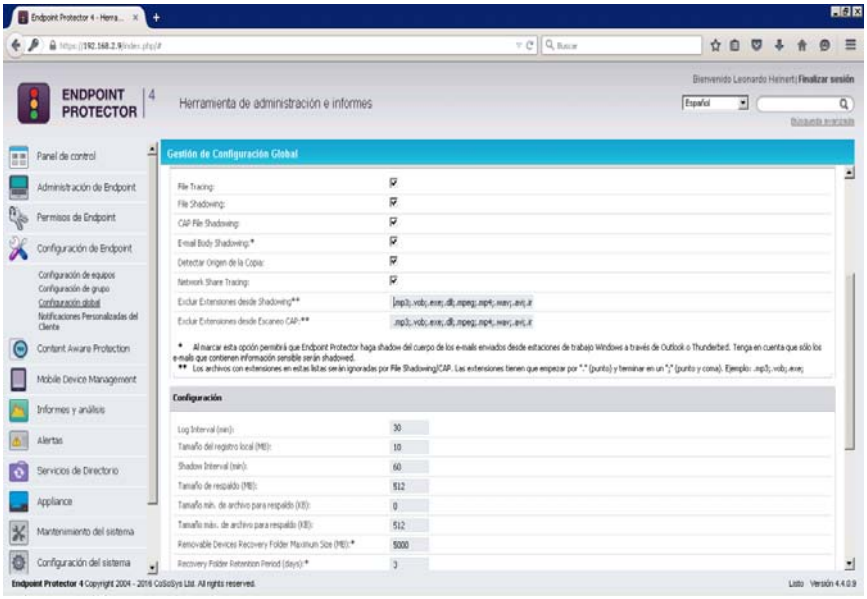


Figura 7. Ventana de configuración de políticas globales

- Configuración Content Aware Protection:

Ofrece un control detallado de los datos confidenciales que salen de la red de la empresa. A través de la inspección eficaz de contenido, las transferencias de documentos importantes de la compañía se registrarán, se notificarán y se bloquearán [7].

- Recolección de informes para el respectivo análisis.

File Tracing registra todos los datos que han sido copiados a y desde dispositivos USB u otros dispositivos de almacenamiento directamente desde la interfaz basada en la web. Con File Shadowing activado, usted puede guardar una copia de todos los archivos transferidos. Un registro detallado de todo el flujo de información en la red es esencial para las auditorías y para controlar las fugas de datos.

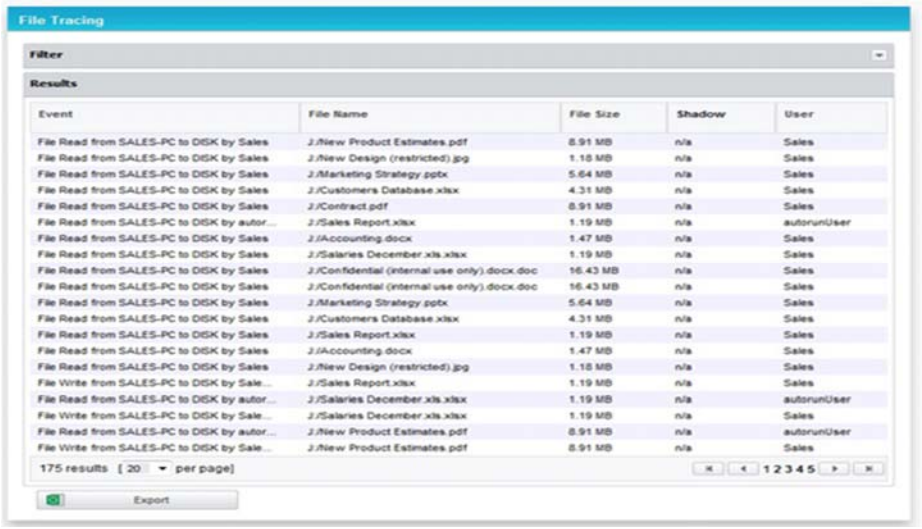


Figura 8. Ventana de configuración de los servicios de la solución DLP

- Mobile Device Management de Endpoint Protector

Es la solución perfecta para las organizaciones que utilizan sus propios dispositivos móviles o adoptan el modelo BYOD (Traiga-

Su-Propio-Dispositivo) para proteger los datos confidenciales de la empresa. A través del monitoreo detallado, el registro y los informes de toda la actividad de dispositivos móviles y la aplicación remota de políticas fuertes de seguridad, las compañías ganarán una mayor protección tanto contra las amenazas internas, como externas.

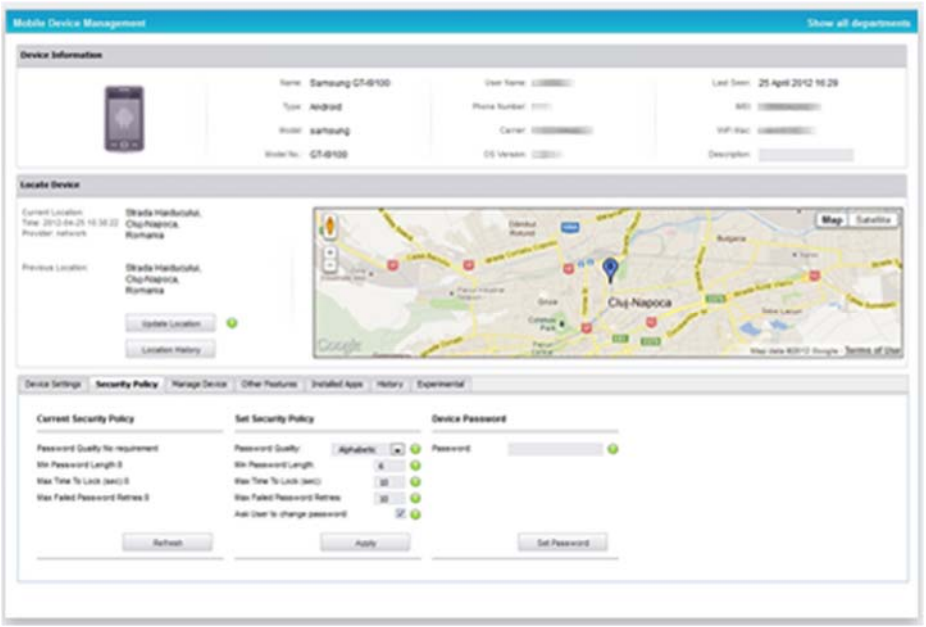
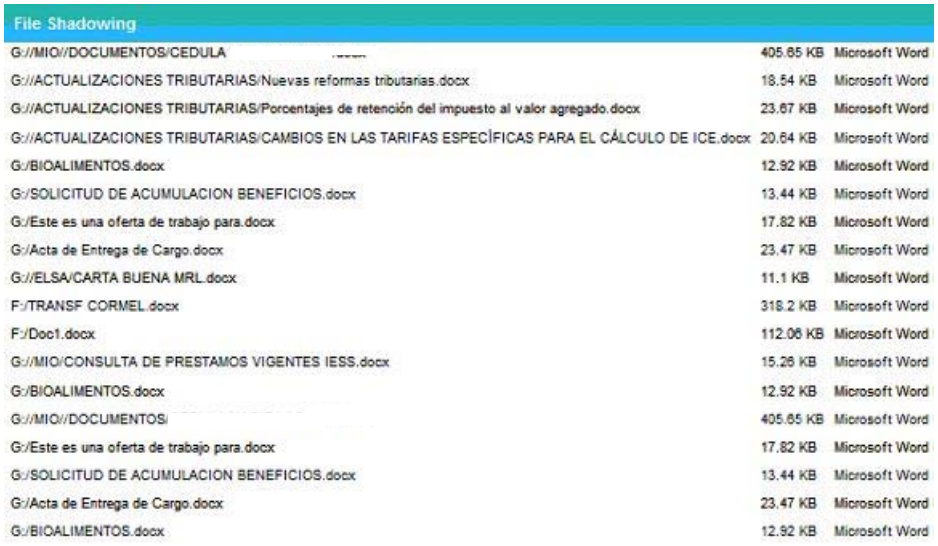


Figura 9.*Ventana de configuración de geolocalización para dispositivos móviles*

2.4 PRUEBAS

Una vez realizada la instalación y configuración del Endpoint Protector, se genera un informe de File Tracing que consiste en un seguimiento de los

archivos catalogados como “confidenciales” y sus interacciones con los dispositivos, es decir, al trasferir un archivo esta regla realiza un seguimiento origen y destino y lo almacena en un log. Otro informe es el File shadowing que permite que el mismo archivo sea almacenado como una copia en el servidor y poder verificar si el archivo es o no confidencial. A continuación, se presenta los reportes con los tipos de extensiones más utilizados dentro de la organización, como son las hojas de cálculo, mensajería de correo electrónico y documento de texto.



File Shadowing

G://MIO//DOCUMENTOS/CEDULA	405.65 KB	Microsoft Word
G://ACTUALIZACIONES TRIBUTARIAS/Nuevas reformas tributarias.docx	18.54 KB	Microsoft Word
G://ACTUALIZACIONES TRIBUTARIAS/Porcentajes de retención del impuesto al valor agregado.docx	23.67 KB	Microsoft Word
G://ACTUALIZACIONES TRIBUTARIAS/CAMBIOS EN LAS TARIFAS ESPECÍFICAS PARA EL CÁLCULO DE ICE.docx	20.64 KB	Microsoft Word
G:/BIOALIMENTOS.docx	12.92 KB	Microsoft Word
G:/SOLICITUD DE ACUMULACION BENEFICIOS.docx	13.44 KB	Microsoft Word
G:/Este es una oferta de trabajo para.docx	17.82 KB	Microsoft Word
G:/Acta de Entrega de Cargo.docx	23.47 KB	Microsoft Word
G://ELSA/CARTA BUENA MRL.docx	11.1 KB	Microsoft Word
F:/TRANSF CORMEL.docx	318.2 KB	Microsoft Word
F:/Doc1.docx	112.06 KB	Microsoft Word
G://MIO/CONSULTA DE PRESTAMOS VIGENTES IESS.docx	15.26 KB	Microsoft Word
G:/BIOALIMENTOS.docx	12.92 KB	Microsoft Word
G://MIO//DOCUMENTOS/	405.65 KB	Microsoft Word
G:/Este es una oferta de trabajo para.docx	17.82 KB	Microsoft Word
G:/SOLICITUD DE ACUMULACION BENEFICIOS.docx	13.44 KB	Microsoft Word
G:/Acta de Entrega de Cargo.docx	23.47 KB	Microsoft Word
G:/BIOALIMENTOS.docx	12.92 KB	Microsoft Word

Figura 10. Resultado del Informe File Shadowing, con filtrado de documentos de texto

File Shadowing

Nombre de archivo	Tamaño de archivo	Tipo de archivo	Usuarios	Equipo	Fecha/hora(Cliente)
F:/PEDIDO DOMINGO 21-06-2015.msg	85 KB	Elemento de Outlook	Usuario	COMERCIAL2	2015-07-13 18:01:57
F:/Pedido semanal.msg	82 KB	Elemento de Outlook	auditoria1	AUDITORIAI	2015-07-11 12:51:23
F:/PEDIDO DOMINGO 21-06-2015.msg	85 KB	Elemento de Outlook	auditoria1	AUDITORIAI	2015-07-11 12:51:23
F:/Pedido semanal.msg	82 KB	Elemento de Outlook	auditoria1	AUDITORIAI	2015-07-07 17:35:34
F:/PEDIDO DOMINGO 21-06-2015.msg	85 KB	Elemento de Outlook	auditoria1	AUDITORIAI	2015-07-07 17:35:34
F:/Pedido semanal.msg	82 KB	Elemento de Outlook	auditoria1	AUDITORIAI	2015-07-04 13:51:13
F:/PEDIDO DOMINGO 21-06-2015.msg	85 KB	Elemento de Outlook	auditoria1	AUDITORIAI	2015-07-04 13:51:13
F:/PEDIDO DOMINGO 21-06-2015.msg	85 KB	Elemento de Outlook	auditoria1	AUDITORIAI	2015-07-03 16:50:00
F:/Pedido semanal.msg	82 KB	Elemento de Outlook	auditoria1	AUDITORIAI	2015-07-03 16:50:00
F:/PEDIDO DOMINGO 21-06-2015.msg	85 KB	Elemento de Outlook	auditoria1	AUDITORIAI	2015-07-03 10:29:48
F:/Pedido semanal.msg	82 KB	Elemento de Outlook	auditoria1	AUDITORIAI	2015-07-03 10:29:48
F:/PEDIDO DOMINGO 21-06-2015.msg	85 KB	Elemento de Outlook	auditoria1	AUDITORIAI	2015-07-02 10:04:41

Figura 11. Resultado del Informe File Shadowing, con filtrado de documentos de correo electrónico.

File Shadowing

F://CIERRES	D/Cierre de Cajas Diario 19 DE JULIO.xlsx	17.05 KB	Hoja de cálculo
F://CIERRES (	D/CONTROL DE COMANDAS - 19 DE JULIO DE	24.93 KB	Hoja de cálculo
F://CIERRES (	O/Cierre de Cajas Diario 18 DE JULIO.xlsx	17.01 KB	Hoja de cálculo
F://CIERRES (	CONTROL DE COMANDAS - 18 DE JULIO DE	22.31 KB	Hoja de cálculo
F://CIERRES (	Cierre de Cajas Diario 17 DE JULIO.xlsx	16.99 KB	Hoja de cálculo
F://CIERRES (	CONTROL DE COMANDAS - 17 DE JULIO DE	16.97 KB	Hoja de cálculo
F://CIERRES	Cierre de Cajas Diario 16 DE JULIO.xlsx	16.92 KB	Hoja de cálculo
F://CIERRES	CONTROL DE COMANDAS - 16 DE JULIO DE	17.03 KB	Hoja de cálculo
F://CIERRES	Cierre de Cajas Diario 19 DE JULIO.xlsx	17.05 KB	Hoja de cálculo
F://CIERRES	Cierre de Cajas Diario 19 DE JULIO.xlsx	17 KB	Hoja de cálculo
F://CIERRES	CONTROL DE COMANDAS - 19 DE JULIO DE	24.93 KB	Hoja de cálculo
F://CIERRES	Cierre de Cajas Diario 18 DE JULIO.xlsx	17.01 KB	Hoja de cálculo
F://CIERRES	Cierre de Cajas Diario 17 DE JULIO.xlsx	16.99 KB	Hoja de cálculo
F://CIERRES	Cierre de Cajas Diario 17 DE JULIO.xlsx	16.99 KB	Hoja de cálculo
F://CIERRES	Cierre de Cajas Diario 16 DE JULIO.xlsx	16.92 KB	Hoja de cálculo
F://CIERRES	Cierre de Cajas Diario 16 DE JULIO.xlsx	16.96 KB	Hoja de cálculo
F://CIERRES	Cierre de Cajas Diario 15 DE JULIO.xlsx	16.96 KB	Hoja de cálculo
F://CIERRES (	5/~$Libro1.xlsx	165 B	Hoja de cálculo
F://CIERRES C	5//04 DE JULIO/CONTROL DE COMANDAS - (	22.73 KB	Hoja de cálculo

Figura 12. Resultado del Informe File Shadowing, con filtrado de hojas de cálculo.

CAPÍTULO 3

ANÁLISIS DE RESULTADOS

3.1. TIPOS DE ANOMALIAS DETECTADAS

Después de realizar la implementación del DLP Endpoint Protector, se puedo evidenciar ciertas violaciones que guardaban relación con la información considerada como confidencial o sensible para la organización:

- Archivos compartidos en la red.
- Manipulación de archivos con información confidencial.
- Copia/ envió de información confidencial o sensible a dispositivos de almacenamiento USB.
- Movimiento de información a otros lugares de la red corporativa.

3.2. DETECCIÓN DE PROBLEMAS

Luego de la implementación y configuración de las políticas del DLP Endopoint Protection, se evidenciaron algunos tipos de problemas que denotan la manipulación y extracción de información sensible de la organización.

Se encontraron varios registros relacionados con la palabra clave que fue configurada como “Facturación” dando resultado varios logs de manipulación de este archivo tanto compartido en la red como en dispositivos periféricos.

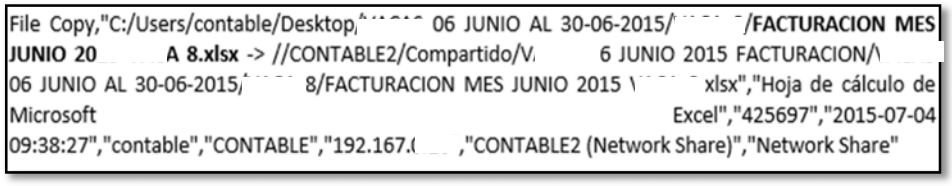


Figura 13. Evidencia (Logs) del informe de archivos manipulados.

El siguiente log mostrado hace referencia a la lectura de archivos como este, se tiene varios interpretando el log se puede determinar que los usuarios manipulan archivos que contienen palabras confidenciales o sensibles para la empresa en este claro ejemplo se puede apreciar que existe un archivo de balances siendo manipulado desde una unidad extraíble. Con una política restrictiva aplicada en Endpoint Protector se puede controlar la fuga de este y otro tipo de información gracias a las políticas de content aware protection de Cososys Endpoint Protector.

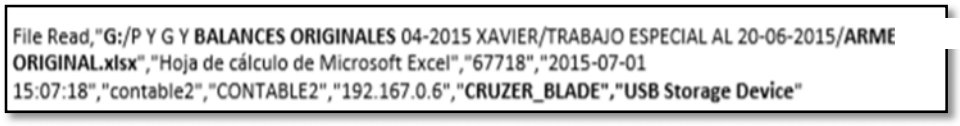


Figura 14. Evidencia del informe del Content aware protection

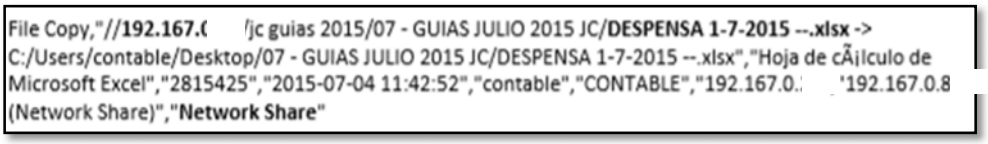


Figura 15. Evidencia del informe donde se presenta archivos compartidos.

Como parte de la configuración, se establecieron reglas basadas en un SMTP interno, el cual informa de cualquier política que haya sido violada.

***Figura 16**. Evidencia de la fuga de datos, a través de correo electrónico*

En el evento anterior se tuvo un registro SMTP indicando la copia de un archivo sensible que se encontraba en una unidad extraíble F: y fue copiada a otra unidad extraíble G: por el usuario auditoria1, este archivo fue cierre de cajas y comandas no facturadas, un archivo de Excel. Ahora nos encontramos con una alerta de contenido,

interpretando el log se puede entender que el usuario auditoria1 manipula el archivo cierre de cajas.xls y lo guarda en una unidad extraíble luego de haberlo editado.

Content Aware Event Number :	1
Content Aware Event :	CONTENT THREAT DETECTED
User Name logged on PC :	auditoria1
Nombre del equipo :	AUDITORIA
Tipo de Destinación :	USB Storage Device
Destinación :	TRAVELING_DISK
Nombre de archivo :	F:/CIERRES '14 DE JULIO/CONTROL DE COMANDAS - 14 DE JULIO DE .xlsx
Política de Contenido :	Política de contenido DEMO
Tipo del Artículo :	File Type
Elemento Identificado :	application/vnd.ms-excel
Detalles del Elemento :	Excel
Time of Content Aware Event :	2015-07-29 09:49:47

Figura 17. *Evidencia de la fuga de datos, a través de dispositivos USB.*

Content Aware Protection realiza un escaneo interno al documento en busca de contenido catalogado como confidencial para prevenir la fuga ya sea por dispositivos o aplicativos que utilicen como plataforma el internet, aplica para: mensajería instantánea, navegadores web, webmail, torrents, clouds, ftp, dispositivos, impresoras etc. Para esta

prueba se realizó un escaneo a un archivo que fue transferido vía correo electrónico. El log nos indica él envió de un adjunto.

Figura 18. Evidencia del Informe del escaneo de documentos salientes.

Se revisa el mail enviado y se confirma la tracing realizado por el agente Endpoint Protector así como también el shadowing realizado es decir la copia del adjunto que fue enviado.

Figura 19. Evidencia del escaneo del documento copiado

Activación de MDM, hace referencia a la administración de dispositivos móviles para geolocalización, control de cuentas, administración de contraseña, control de aplicaciones instaladas, gestión de contactos, borrado de memorias interna y externa a distancia. La implementación es realizada mediante SMS, correo electrónico o escaneando un código QR, en cualquiera de los casos la configuración ya viene predefinida con las políticas.

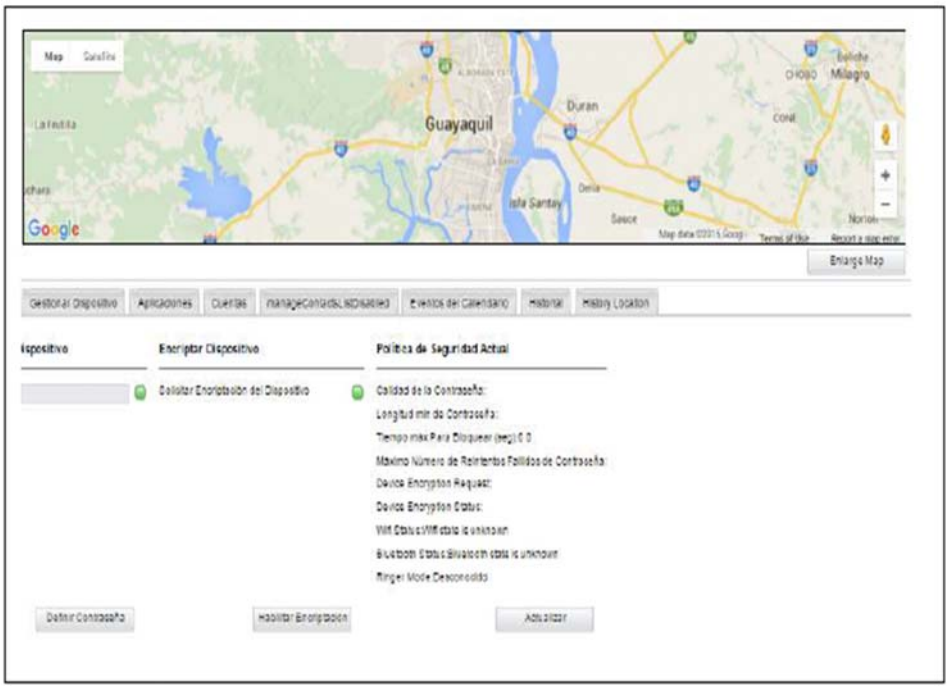


Figura 20. Evidencia de la geolocalización del Dispositivo móvil

CONCLUSIONES Y RECOMENDACIONES

1. Las amenazas internas generadas por los empleados de la organización, se convierten en la amenaza principal de la organización, ya que desde el interior se produce la perdida, mala manipulación y fuga de la información.

2. La solución DLP Endpoint protector, proporciona una consola de administración web, muy amigable desde donde se pueden administrar los servicios disponibles, así como las políticas de seguridad de acuerdo a las necesidades de la organización.

3. Las características del DLP Endpoint protector, permite la fácil configuración y utilización de los servicios incluidos como El content aware protection (para analizar el contenido de la información de la red), así como el File Shadowing (para almacenar una copia del archivo transferido).

4. A diferencia de otras soluciones DLP, Endpoint protector incluye informes gráficos, bastantes intuitivos que permiten realizar un seguimiento completo de la información, auditorias e informes gerenciales.

1. En el mercado existe gran diversidad de soluciones DLP, ofrecidas por reconocidos fabricantes de antivirus, pero debido a su gran portafolio de productos, no ofrecen una solución especializada en la prevención de fuga de datos, como lo hace CoSoSys.

2. Se recomienda la implementación de soluciones dedicadas a la prevención de perdida de información, ya que ofrecen una completa cobertura y monitoreo de la información.

3. Se recomienda, la constante revisión de las políticas de seguridad, y revisión de los informes generados por la herramienta, para dar seguimiento adecuado y prevenir las fugas de información.

BIBLIOGRAFÍA

[1] ISACA, «PREVENCIÓN DE FUGA DE DATOS,» ROLLINGS MEADOWS, 2010.

[2] Symantec, «Symantec Data Loss Prevntion,» Mountain View , 2013.

[3] Symantec, «Data Loss Prevention and Monitoring in the workplace: Best Practice Guide for Europe,» Green Park, 2012.

[4] Secutatis Information Security, «Secutatis Information Security,» 2015. [En línea]. Available: http://www.secutatis.com/?page_id=157.. [Último acceso: 26 12 2015].

[5] Deloitte , «Estudio de Seguridad Global de DTTL 2012 de la Industria Financiera,» 2012.

[6] CoSoSys, «Data Sheet Endpoint Protector,» 2015.

[7] Endpoint Protector, «Endpoint Protector,» 2004. [En línea]. Available: http://www.endpointprotector.es/products/endpoint_protector/features. [Último acceso: 8 01 2016].