UNIVERSIDAD DEL AZUAY

FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN.

ESCUELA DE INGENIERÍA DE SISTEMAS Y TELEMÁTICA.

“PREVENCIÓN Y MINIMIZACIÓN DE FUGA DE INFORMACIÓN IMPLEMENTANDO DLP (DATA LOSS PREVENTION)”.

MONOGRAFÍA PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS Y TELEMÁTICA.

AUTOR: MOISES RENDON TERREROS.

DIRECTOR: ING. FERNANDO AGUILAR OCHOA, MAE.

CUENCA, ECUADOR

2014

Dedicatoria

Se lo quiero dedicar a Dios, a mi Madre y mi Padre que han hecho posible que pueda cumplir las metas que he soñado, a toda mi familia que son un apoyo incondicional, y a mis bellos sobrinos que me inspiran todos los días a continuar hacia adelante.

Agradecimiento

Quiero agradecer a todos mis amigos y compañeros que me acompañaron a lo largo de mi carrera universitaria, a cada uno de los docentes que no solo se limitaron a enseñarme lo que dice los libros sino sobre la vida, en especial al Ing. Fernando Aguilar Ochoa que me ayudo con la elaboración de esta monografía por sus consejos y sugerencias.

Índice de Contenidos

Índice de Figuras y Tablas

Resumen

Este documento explica que es un DLP (*Data Loss Prevention* - Prevención de perdida de información) y sus principales funcionalidades, de igual manera propone una guía estándar de implementación, que puede ser acogida por cualquier organización y así puedan prevenir una pérdida de sus datos. Se ha elaborado un trabajo investigativo compuesto por cuatro capítulos, que puede servir como fuente bibliográfico para trabajos académicos o para implementar una herramienta DLP en cualquier organización.

ABSTRACT

This document explains what a DLP (Data Loss Prevention) and its main features are. Similarly, it proposes a standard implementation guide which can be used by any organization in order to prevent loss of data. We have developed a research paper which consists of four chapters that can serve as bibliographic source for academic work or for implementing a DLP tool in any organization. Also, the steps to install a DLP Open Source tool so as to perform a scan of sensitive information from a PC are explained as a proof of concept.

UNIVERSIDAD DEL AZUAY
DPTO. IDIOMAS

Translated by,
Lic. Lourdes Crespo

Introducción.

Dentro de este documento se propone una solución que ayude a la prevención de fuga de información, siendo la información en la actualidad el principal activo que posee cualquier organización, y su protección debe ser una prioridad, es por ello que se debe contar con mecanismos y una metodología que permita protegerla.

Se elaboró un trabajo de investigación compuesto por cuatro capítulos, en el Capítulo I se explica que es un DLP y sus principales funcionalidades, en el capítulo II se propone una guía estándar de implementación, que puede ser acogida por cualquier empresa y así puedan prevenir una pérdida de sus datos, en el Capítulo III se presenta los pasos de como instalar una aplicación DLP *Opensource*, y así realizar un escaneo de información sensible de un PC, que servirá como una prueba de concepto. Por ultimo en el Capítulo IV se presentan las conclusiones y recomendaciones que se han obtenido a lo largo del desarrollo de este documento.

El trabajo investigativo se desarrolló recopilando información de libros, libros digitales, revistas etc., elaborando este documento para que sirva en un futuro como fuente bibliográfica para trabajos académicos o para implementar una solución DLP en cualquier organización.

Descripción de la Problemática.

Durante el año 2010 se dio un caso de fuga de información muy discutido denominado el caso "*Wikileaks*", pero lo importante a enfatizar es que esta problemática no es nueva dentro del campo de la seguridad de la Información, sin embargo la evolución tecnológica y empresarial ha ido dando mayor relevancia a la gestión efectiva de la información, llegando a convertirse en la actualidad en el principal activo de toda empresa.

La fuga de información no es tan reciente, desde el año 2007 se han denunciado el robo y vulneración de cuentas de usuarios de diversas empresas como "*Monster*", "*Tuenti*", entre otros. En el Ecuador también se han dado casos de fuga de información, la Fiscalía de Chone denuncio que existió y aseguro que nadie conocía la existencia de este incidente (Diario, 2013), otro caso fue el que El ministro de Defensa, Miguel Carvajal, en el año 2012 reveló una posible fuga de información desde el interior de las Fuerzas Armadas o de la Policía Nacional (Mercurio, 2012).

Muchas organizaciones no saben cómo proteger sus datos, ni la importancia que poseen, por lo tanto no tienen un correcto manejo de su información, no poseen buenas practicas ni políticas que les permita salvaguardarla, esto genera un riesgo muy alto y da paso a que exista un fuga de información. Los diferentes dispositivos portátiles y de almacenaje extraíbles, también representa una amenaza muy grande, y las organizaciones no cuentan con políticas ni implementaciones que permitan evitar que estas se convierten en víctimas de fugas de información, así evitándoles gastos muy altos que muchas veces se representan en pérdidas de clientes o indemnizaciones sin dejar de lado el coste de recuperar la confianza de una empresa cuya información ha sido robada o falsificada. Esto abarca lo referente a riesgo operativo, riesgo legal y riesgo reputacional.

CAPÍTULO 1: CONCEPTOS GENERALES

1.1 ¿Qué es un DLP?

El termino DLP, *Data Loss Prevention*, cuyo significado en español es Prevención de pérdida de datos, se encarga de prevenir el robo, acceso o salida de datos de una empresa, ya sea accidental o de manera consciente.

Es un término que se emplea en el área de seguridad de la información, haciendo referencia a los sistemas que identifican, supervisan y protegen los datos que se procesan, transmiten o almacenan. Los sistemas están diseñados para detectar y prevenir el uso no autorizado y la transmisión de información privada, sensible y confidencial, principalmente acorde a la clasificación de la información de cada entidad.

El DLP surge en el mercado en 2006, frente a la necesidad que tienen las organizaciones de proteger la información sensible a una fuga de datos.

En la siguiente figura se resumen el esquema del DLP.

Figura 1: Esquema DLP (Rendón Moisés).

1.2 Función del DLP.

Según Prathaben Kanagasingham "La función de un DLP es la de identificar, monitorear detectar e intentar prevenir la fuga de información considerado como confidencial o sensitiva por las organización y/o uso no autorizado. Por lo general esto se lleva a cabo a través de herramientas que cuentan con una gestión centralizada y permiten el monitoreo y control de los datos en el puesto de trabajo"[1].

Es decir que DLP protege los datos sensibles, además de proporcionar información sobre el uso de estos datos dentro de la organización, ayudando a que se pueda entender de mejor manera la clasificación y manejo de su información.

[1] (Kanagasingham, 2008)

La función principal de los DLP es proteger los datos de la organización que se pueden encontrar como:

- Datos en Reposo: Son los datos que se encuentran almacenados en un disco duro, CD, memoria USB, o cualquier otro medio de almacenamiento.

- Datos en movimiento: Son aquellos datos que son transmitidos en una red.
  Estos datos son particularmente vulnerables, ya que los atacantes no necesitan estar cerca de la computadora donde estos datos están almacenados: solo requieren estar en ubicados en algún punto de la ruta en que esos datos están recorriendo.

- Datos en Uso: Son los datos que se están utilizando en ese momento como, estados financieros, roles de pago, creación de un documento.

1.3 Características de un DLP.

Como ya se mencionó anteriormente los DLP ayudan a las organizaciones a que tengan mejor control y manejo de sus datos, además de proteger los datos sensibles. En el artículo *Understanding and Selecting a DLP solution Websense*[2] (Mogull, 2008), describe varias de sus características, de las cuales las más marcadas son:

- Profundo análisis de Contenido: DLP tienen la capacidad de analizar a profundidad el contenido empleando diferentes técnicas dependiendo en donde se encuentre la información.

- Gestión de políticas centrales: Las soluciones DLP incluyen un servidor que permite una gestión central y así permite administrar los puntos de detección, creación como la gestión de las políticas implementadas.

[2] (Mogull, 2008)

- Amplia cobertura de contenido a través de múltiples plataformas y locaciones.

1.4 Prevención de Fuga de información.

Antes de adentrarse en el tema, debemos conocer que la fuga de información es una salida no controlada de la información, ocasionando que esta llegue a mano de personas no autorizadas o que el dueño de la información pierda el control de la misma. En muchos casos ocurre cuando un sistema de información que está diseñado para restringir el acceso sólo a personas autorizadas, revela parte de la información debido a errores en los procedimientos del diseño o concepción del sistema.

La prevención de Fuga de información tienen propósito principal: identificar, monitorizar, detectar y prevenir la fuga de información, que es considerada como confidencial por las organizaciones. Siendo administrado desde una consola central donde tiene la capacidad de detectar y prevenir uso no autorizado así como transmisión de información confidencial.

1.5 Causas y Factores principales para que exista perdida de datos en las empresas.

En el artículo “Prevención de pérdida de datos Data Loss Prevention” (Cardozo González & García Severiche, 2013), expone que hoy en día las organizaciones usan dispositivos inalámbricos como: celulares, tabletas, *laptops* como herramientas de trabajo el cual están sincronizados con su correo electrónico, manejan pedidos, poseen cartera de clientes, agenda de contactos, etc. Si bien estas herramientas facilitan a los empleados en sus actividades, representan una gran posibilidad que existan una pérdida de confidencialidad.

Otro factor importante es que estos dispositivos pueden manejar diferentes conexiones como: *Wireless*, *Bluetooth* y si estas no poseen procedimientos o

mecanismos para proteger la información, existe riesgo que la información que maneje este comprometida, ya que muchas veces las personas utilizan sus dispositivos en lugares públicos sin considerar que pueden ser víctimas de robo de información.

En el artículo de (Cardozo González & García Severiche, 2013) menciona que existen diferentes amenazas y vulnerabilidades que pueden llevar a que exista una pérdida de datos, como por ejemplo:

- Redes sociales. Representan un riesgo en la confidencialidad de la información, así que las organizaciones deben realizan campañas de sensibilización para que eviten que los empleados publiquen información de la compañía en dichas redes.

- Publicación de videos. Existen actividades que se realizan al interior de las organizaciones que son grabadas, y muchas veces son subidas a páginas sin tener en cuenta la información que en ellas estén, lo que puede poner en evidencia información que sólo es relevante para la compañía.

- Falta o inadecuada clasificación de activos de información. La mayoría de organizaciones no poseen una adecuada clasificación de activos de información, provocando que los empleados no tengan claro el nivel de protección de cada activo, y de esta manera dificulta la protección de estos.

- Falta de sensibilización a los usuarios. Las organizaciones deben realizar campañas de sensibilización, permitiendo involucrar a los empleados con la seguridad de la información.

- Falta de acuerdos de confidencialidad. Las organizaciones por lo general tratan con diversos proveedores y empleados que llegan a conocer información del funcionamiento de la compañía y no hay un control para que puedan ser expuestos, ya no son confidenciales ni íntegros.

- Virus y Malware. Son una amenaza constante para los datos de las organizaciones, debido a su fácil propagación, y muchas veces su difícil detección.

Además las Organizaciones hoy en día no disponen de un esquema de buenas prácticas que garantice el correcto manejo de la información, esto pone en un riesgo muy alto la información confidencial, no cuentan con políticas ni implementaciones que permitan evitar que estas se convierten en víctimas de fugas de información, así evitándoles gastos muy altos que muchas veces se representan en pérdidas de clientes o indemnizaciones sin dejar de lado el coste de recuperar la confianza de una empresa cuya información ha sido robada o falsificada. Esto abarca lo referente a riesgo operativo, riesgo legal y riesgo reputacional.

1.6 Necesidad de proteger el negocio.

Hoy en día la información es el activo más importante que posee cualquier organización, especialmente la información sensible o confidencialidad, la mayoría de veces esta permite generar ventaja a quien la posee, es por esto que el éxito de una organización o empresa no solo depende del manejo de sus recursos materiales como el capital, también depende de cómo se aprovechen sus activos intangibles, en este caso la información que ellos generan.

A medida que la tecnología crece y evoluciona, hace que salvaguardar la información, necesite de procedimientos más complejos y eficientes para prevenir robos y el mal manejo de la información

Cada vez son más frecuentes las noticias que están relacionadas con el tema de fugas de información intencionadas, casos de espionaje industrial o filtraciones de información por parte de trabajadores que se adueñan de esta información que es crítica y sensible.

Javier Berciano en su artículo de opinión (Berciano, s.f.), menciona que la pérdida de información sensible puede producirse de manera accidental o malintencionada, pero, en cualquier caso, puede y suele acarrear un daño económico y de prestigio, afectando a la empresa y su marca asociada.

Hablando desde un punto técnico existe la necesidad de administrar y gestionar una enorme cantidad de datos que procesan las organizaciones, los usuarios deberán acceder a distintos archivos y datos que viajarán por las redes y se almacenarán en distintas ubicaciones.

Hoy en día con el uso las "tabletas" y el incremento del uso de dispositivos móviles en las empresas, existe la necesidad de administrar, gestionar y proteger los dispositivos móviles y salvaguardar su información,

Es por ello que es de vital importancia proteger el negocio, sobre todo porque podremos generar como principal beneficio un valor agregado sobre la competencia u otras organizaciones.

1.7 Escenario de implementación de DLP.

Existe una infinidad de implementaciones que se pueden realizar, distintos escenarios, protagonizadas por distintas empresas y con distintas necesidades, como ejemplo se mencionaran algunos como:

- Hospitales: La cantidad de información que se maneja en este sector es muy grande, además de muy crítica, se manejan cuadros clínicos, recetas, listados de pacientes y doctores. Una solución DLP permitiría una mejor gestión, además de una monitorización de los datos que se estén usando.

- Cerámica: En este caso, estas empresas manejan diseños que muchas veces deben ser originales, además manejan catálogos que son mostradas en determinadas épocas del año y deben ser desconocidas por su competencia para generar mayor impacto en los compradores. La copia de estos diseños empleando un dispositivo USB externo o enviarlos por email es un riesgo que se puede prevenir con una solución DLP que permite monitorizar cada fichero que se copia a un dispositivo USB, registrar qué usuario y cuando lo hizo permitiendo incluso generar una alerta.

- Centro de investigación: En este sector existe una gran cantidad de datos de diversas investigaciones que muchas veces no son patentadas, que pueden ser enviados atreves de un correo electrónico. Un sistema DLP permite monitorizar el tráfico de red y cancelar flujos de datos que incluyan datos clasificados.

- Empresa de alimentos: Las empresas en este sector les interesa controlar las fórmulas que usan para la preparación y producción de determinados alimentos, siendo estas fórmulas datos críticos que les da ventaja sobre su competencia. Un sistema DLP permite monitorizar que se envía por la red, o lo que se envíen a dispositivos externos por distintos medios y generar alertas cuando algo no permitido suceda.

- Como se ve existen muchos escenarios para implementar un sistema DLP ya que siempre se desea monitorizar el tráfico de red como los sistemas de almacenamiento y procesamiento con el objetivo de que ningún dato se filtre sin ser detectado.

CAPÍTULO 2: METODOLOGÍA DE IMPLEMENTACIÓN

2.1 Clasificación de usuarios y propietarios de la Información.

Se debe tener presente que la información es un recurso que tiene gran valor, como el resto de activos que maneje la organización, y por ello esta debe estar protegida. Para ello primero se debe hablar de clasificación de la información, de esta manera se conoce la información con que cuenta la organización.

Según la norma NTC 27001, un propietario de activos de información es: "cualquier persona o entidad a la cual se le asigna la responsabilidad formal de custodiar y asegurar un activo de información o un conjunto de ellos".

La ISO/IEC 27001[3] recomienda establecer diferentes niveles para clasificar la información, por ejemplo, un sistema sencillo de clasificación podría contemplar los siguientes niveles:

- Información Pública: Esta información puede ser distribuida a todo el público en general a través de diferentes medios, que estén supervisadas por la Organización.

- Información Restringida: Dicha información está destinada al uso exclusivo de los empleados de la organización en el desarrollo de los procesos del negocio.

- Información de Uso interno: Esta información es para la divulgación interna segura, y no debe ser divulgada externamente.

[3] ISO/IEC 27001 estándar de la seguridad de la información, aprobado y publicado como estándar internacional en octubre de 2005 por *International Organization for Standardization* y por la comisión *International Electrotechnical Commission*.

- Información Confidencial: Información que al ser divulgada, podría violar la privacidad de personas o algún incumplimiento legal, disminuir la ventaja competitiva. Además podría causar un daño significativo a la organización y a su imagen.

Al clasificar la información se puede identificar las necesidades y prioridades de uso y así se puede establecer cuáles son los propietarios responsables de esta, por consiguiente se pueda brindar la protección que dicha información requiere.

Para poder establecer los propietarios de la información se deben identificar las áreas funcionales que están distribuidas en la organización, el tipo e interacción de información que se manejan y existen dentro de las diferentes áreas.

Los propietarios de la información son los responsables de dar mantenimiento y actualizar la información que se maneja dentro de las áreas funcionales. Además como función debe documentar y definir, sobre que usuarios tienen permiso de acceso y uso de la información de acuerdo a sus funciones, cargo o rol.

Un ejemplo de clasificación de usuarios y propietarios de la Información se puede observar en la siguiente tabla:

Área Funcional	Tipo de Información	Áreas de Interacción	Descripción del tipo de información	Propietario de la Información	Usuarios Autorizados

Tabla 1: Tabla de clasificación de usuarios y propietarios de la Información (Rendón Moisés).

Clasificando correctamente la información, los usuarios y propietarios de la información nos permitiría:

- Conocer la información que utiliza la organización.
- Asignar diferentes niveles de privacidad en función del tipo de información.
- Asignar permisos de acceso a la información según el propietario o usuario de esta.
- Brindar protección de la información en función de su nivel de privacidad.

2.2 Identificación de salidas de información.

La salida de información se puede definir como el proceso de transmitir información de un sistema, con una interacción de ordenador-usuario, de diversas maneras como: reportes, video, informes visualizados por pantalla, informes impresos en papel, etc.

2.2.1 Diagrama de red estándar basado en DLP.

A continuación, se presenta el diagrama red estándar basado en *host*, que explica como los dispositivos *End-Point* están conectados a la red de una organización.

Cada *End-Point* posee un agente que se ejecuta como un servicio del Sistema Operativo con una prioridad baja para que los usuarios no lo noten, y hay un estación que permite que se Administre el DLP que estará conectada a la misma red y estará monitorizando y supervisando la información sensible que se establezca dentro de la organización y se configure en el administrador.

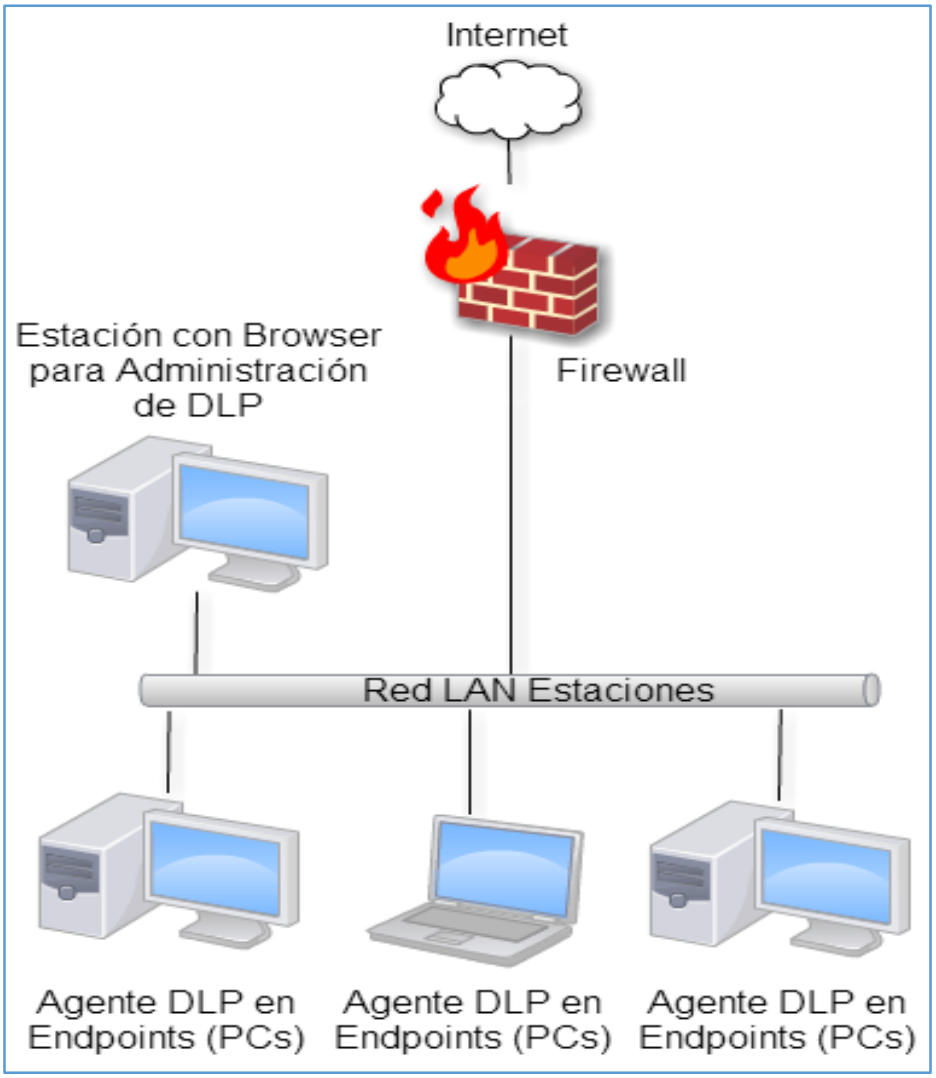

Figura 2: Diagrama de red estándar para implementar DLP en dispositivos Endpoints (Rendón Moisés).

En la actualidad en el mercado existen muchas herramientas DLP basados en host, pero para una demo demostrativa que se va a realizar más adelante, se va a emplear una herramienta *OpenSource*, basada en agentes y de gestión centralizada, puede identificar datos sensibles en cientos de máquinas de esta manera puede evitar en gran parte la pérdida de información crítica de las organizaciones.

A continuación se presenta un diagrama de red donde se ve como interactúa la herramienta *Open* con los agentes instalados dentro de cada *PCs* y la

aplicación web que esta de manera monitoreando y supervisando la información de una manera centralizada.

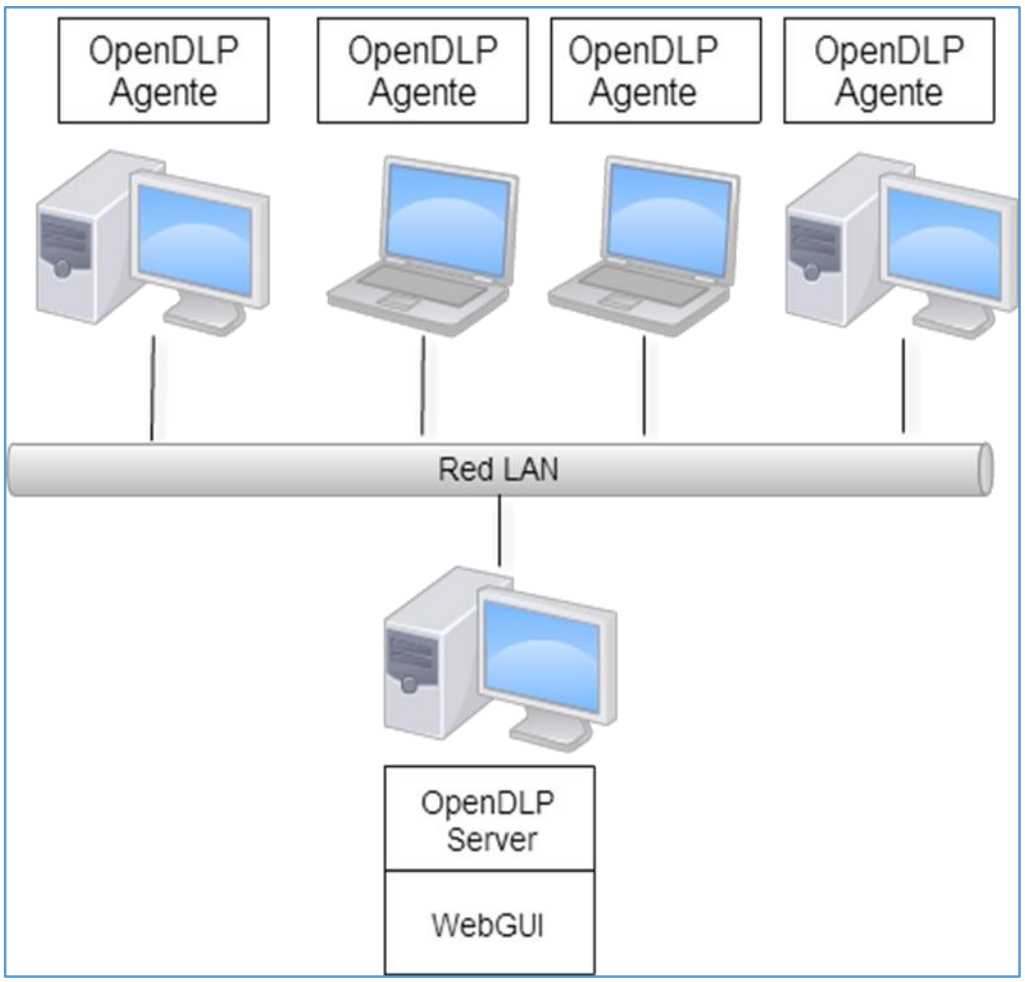

Figura 3: Diagrama de red estándar para implementar con herramienta Open (Rendón Moisés).

2.2.2 Definición de políticas de uso aceptable de las herramientas tecnológicas.

Existen muchas definiciones de política de Seguridad, el autor Álvaro Gómez Vieites lo define como: “Una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran”[4]; es decir las políticas de seguridad son herramientas que definen los activos que la organización desea proteger.

[4] (Vieites, 2007) Enciclopedia de la Seguridad Informática "Amenazas a la Seguridad Informática".

Se debe tener en consideración que una política de seguridad puede ser prohibitiva o permisiva dependiendo de cómo se exprese, es decir, es prohibitiva si todo lo que no está expresamente permitido esta denegado, o permisiva si todo lo que no está expresamente prohibido está permitido.

Se pueden definir políticas tan granular como se desee, además dependerá mucho del tipo de negocio que sea.

A continuación se presentan políticas estándares que se pueden aplicar a una organización que desee implementar un DLP para que trabaje conjuntamente con este; esto no quiere decir que la organización debe apegarse a todas estas políticas descritas, ya que puede crear sus propias políticas ajustándolas al marco legal, orientación del negocio, entorno social de donde se encuentre esta.

- Solo se puede usar el equipo autorizado por la organización para trabajar (portátiles, equipo de escritorio, dispositivo de almacenamiento externo, dispositivos móviles, entre otros).
- El equipo autorizado, ya antes mencionado, no debe ser para el uso personal; debe ser exclusivo para realizar las tareas y labores referentes a su puesto de trabajo.
- Almacenar la información en dispositivos que sean autorizados para su uso.
- Almacenar solo la información relacionada con la organización en los medios de almacenamientos autorizados.
- Se debe emplear el correo electrónico de la organización solo para uso de trabajo, no para emplearlo de manera social, personal o político.
- Asegurar la correcta dirección a la que se envía la información.
- Cada usuario es el único autorizado para leer su correo.
- Generar perfiles de usuario de acuerdo al área funcional para cada empleado, estableciendo permiso y restricciones para las diferentes actividades.
- Realizar bitácoras donde se almacenen los intentos de acceso y terminación de la conexión que existen en el tráfico de la red.
- Cada área funcional deberá clasificar la información que manejan para señalar su sensibilidad y criticidad.
- No permitir la transferencia de información confidencial o sensible a través de aplicaciones IM (*Google Talk, MSN, Skype*, etc).no se puede trasmitir ningún

tipo de información sensible o confidencial sin la debida autorización o por petición de un ente de control.

- Restringir el acceso a la información, llevando un registro del personal autorizado para utilizar la información, para evitar el acceso no autorizado.
- Restringir la instalación y uso de programas no autorizados por la organización, además de aplicaciones que permitan compartir archivos vía web.

Se debe aclarar, que si se incumple con algunas de las políticas antes mencionadas, o políticas que la organización crea pertinente ajustar o crear, se aplicaran las sanciones que estén establecidas por parte de la organización.

Se debe siempre mantener las políticas actualizadas, siempre vigentes además que deben ser difundidas periódicamente a todo el personal y si es necesario instruirlos, para que de esta manera tengan un conocimiento de estas políticas.

2.2.3 Clasificación de la información de acuerdo a su criticidad

Una vez que hemos clasificado a los usuarios, propietarios de la Información, se debe proceder a valorar la información que estos manejan, de acuerdo a su criticidad, evaluar el valor que posee dentro de la organización y la importancia que esta tiene.

Para poder establecer un valor de criticidad a la información, se debe analizar el impacto que puede generar un activo a la organización si este resulta dañado en cuanto a su disponibilidad, integridad y confidencialidad (CID[5]).

La valoración se la hará empleando una escala, esta puede ser cuantitativa o cualitativa, si los activos se puede valorar económicamente, se empleara la escala

[5] Dentro de la Seguridad de la Información se puede definir de una manera simple como:
Confidencialidad: Que nadie más vea la información, solo el usuario autorizado.
Integridad: Que nadie altere la información procesada.
Disponibilidad: Que la información siempre esté disponible cuando se la requiera.

cuantitativa; aunque la mayoría de los casos no es posible o va a suponer diferentes tipos de opinión y con ello conllevar a un esfuerzo excesivo, por lo que es mejor y recomendable emplear las escalas cualitativas como por ejemplo criterios como: bajo, medio, alto; o bien un rango numérico como: rangos del 0 al 10.

A continuación se presenta parámetros definidos para valorar los criterios de criticidad de los activos en cuanto a la integridad, confidencialidad y disponibilidad; con la intención de conocer que información se debe controlar, ya que no se puede monitorear toda la información que genere una organización sino solo la considerada critica, sensible o confidencial.

Se empleara criterios como: alto, medio, bajo, muy bajo.

Disponibilidad:

Criterio	Descripción	Explicación
A	Alto	Debe estar disponible al menos el 99% del tiempo.
M	Medio	Debe estar disponible al menos el 50% del tiempo.
B	Bajo	Debe estar disponible al menos el 10% del tiempo.
MB	Muy Bajo	No aplica / No es relevante.

Tabla 2: Tabla de clasificación de la información de acuerdo a su criticidad en base a la Disponibilidad (Rendón Moisés).

Integridad:

Criterio	Descripción	Explicación
A	Alto	Tiene que estar correcto y completo al menos en un 95%.
M	Medio	Tiene que estar correcto y completo al menos en un 50%.

B	Bajo	No son relevante los errores que tenga o la información que falte.
MB	Muy Bajo	No aplica / No es relevante.

Tabla 3: Tabla de clasificación de la información de acuerdo a su criticidad en base a la Integridad (Rendón Moisés).

Confidencialidad:

Criterio	Descripción	Explicación
A	Alto	Los daños serían catastróficos, la reputación y la imagen de la organización se verían comprometidas.
M	Medio	Serían relevantes, el incidente implicaría a otras áreas.
B	Bajo	Daños muy bajos, el incidente no trascendería del área afectada.
MB	Muy Bajo	No aplica / No es relevante.

Tabla 4: Tabla de clasificación de la información de acuerdo a su criticidad en base a la Confidencialidad (Rendón Moisés).

A continuación se establece la importancia total de cada activo de la información, de acuerdo a la valoración de cada una de las propiedades CID (Confidencialidad, Integridad y Disponibilidad), ya antes establecidas.

Disponibilidad	Integridad	Confidencialidad	Valor de Criticidad
Alto	Alto	Alto	Alta
Alto	Medio	Bajo	Alta
Muy Bajo	Medio	Bajo	Media
Muy Bajo	Medio	Medio	Media
Muy Bajo	Bajo	Bajo	Baja

Tabla 5: Tabla de Valor de Criticidad de cada activo, de acuerdo a la valoración de cada una de las propiedades CID (Rendón Moisés).

Como se aprecia en la Tabla 5, el valor de criticidad de cada activo será el criterio más alto que este establecida de cada una de las propiedades CID.

2.3 Configuración de parámetros de control de salidas de información.

Después de haber establecido los valores de criticidad y el nivel de clasificación de la información (publica, restringida, etc.), se debe establecer los parámetros de control de salida de la información que se maneja dentro de la organización, que actúen según las políticas que se estableció anteriormente, dependiendo del tipo de información que se maneje se puede: alertar, bloquear, monitorea, notifica, almacena evidencias.

Esto depende mucho del alcance que posea la herramienta, las funcionalidades que tenga, pero a continuación se presenta parámetros generales que se pueden establecer conjuntamente con las políticas que se establecieron en capítulos anteriores.

2.4 Alertamiento y bloqueo de salida de información de acuerdo a su criticidad.

A continuación se procede a enumerar varios parámetros generales que pueden ser tenidas en cuenta para un sistema DLP u otros controles con herramientas diferentes.

- Validar que los archivos con información sensible o confidencial generados por un usuario solo los pueda ser leídos por un grupo determinado de usuarios autorizados.
- Verificar que un archivo con información sensible o confidencial pueda ser leído por una persona autorizada, pero no pueda ser modificado.
- Bloquear, notificar, alertar y almacenar evidencia de transferencia de archivos adjuntos con datos confidenciales desde el correo interno. y correo externo
- Bloquear la transferencia de archivos adjuntos con datos confidenciales desde el correo externo.

- Bloquear, notificar y almacenar evidencia de copiado de archivos con información confidencial en medios extraíbles (CD, USB, discos duros, etc.).
- Bloquear, notificar la transferencia de información y datos confidenciales a través aplicaciones web no permitidas como: redes sociales, blogs, aplicaciones de mensajería etc.
- Bloquear, alertar y almacenar evidencia de la transferencia de información y datos confidenciales a través de aplicaciones: HTTP, FTP, NFS, etc.
- Bloquear, monitorear, almacenar evidencia que una porción tanto del archivo como de una base de datos determinado no pueda ser impreso ni transferido.
- Alertar, monitorear y almacenar evidencia de impresión de archivos que sean de nivel: confidencial, restringido o de uso interno.
- Alertar la impresión de pantalla de la información Clasificada.

2.5 Estabilización y mantenimiento, mejora continua.

Como en toda implementación sea este algún sistema, procedimiento, etc. se necesitara de un tiempo de maduración para que se estabilice para que de esta manera ingrese a un ciclo de mejora continua, que en general busca ser la base para asegurar la estabilización del proceso y la posibilidad de mejora del DLP en una organización y prevenir la fuga de información, es por ello que dentro de esta etapa se debe realizar un monitoreo una vez implementada la metodología y herramienta.

La mejora continua requiere que exista un apoyo en la gestión por parte del área administrativa y de los empleados, una retroalimentación (*Feedback*), como resultado de la revisión de los pasos de cada proceso realizado, ya que este es un ejercicio práctico que ayudará a:

- Detectar errores.
- Identificar las fallas de seguridad.
- Controlar que las actividades de seguridad se realicen de acuerdo a lo establecido.
- Definir las acciones a implementar para corregir errores y fallas.

La norma ISO 27001:2005 estipula las siguientes actividades orientadas al monitoreo y revisión:

- Evaluar la efectividad de las acciones ejecutadas para resolver los incidentes de seguridad.
- Establecimiento de criterios de medición de la efectividad de los controles.
- Revisión de los riesgos residuales y los riesgos aceptables
- Auditorías internas y externas a la configuración de la herramienta y metodología.

Además se recomienda definir un área responsable de monitorear y validar la seguridad de la información en la organización, la cual será responsable de:

- Validar que las actividades de seguridad sean ejecutadas de acuerdo a las políticas de seguridad de la información.
- Detectar actividades no autorizadas.
- Identificar brechas e incidentes de seguridad, y comprobar si las acciones tomadas para resolver incidentes de seguridad han sido eficaces.
- Medir la eficacia de los controles.
- Revisar regularmente la evaluación de riesgos: influencian los cambios en la organización, tecnología, procesos y objetivos de negocio, amenazas, eficacia de los controles o el entorno.

La asignación de las responsabilidades se debe realizar de acuerdo a las políticas de seguridad de la información establecidas por la organización.

Se recomienda realizar bitácoras (*logs*) en los cuales se lleve el registro de las fallas ocurridas en la organización y presentarlas en una reunión semanal, donde se analizara todas actividades registradas en las bitácoras.

Se debe mantener las políticas actualizadas, además que deben ser difundidas periódicamente a todo el personal dentro de procesos formales de capacitación o procedimientos informativos, para que de esta manera tengan un conocimiento actualizado permanente de las políticas de seguridad de la información institucional.

Además a continuación se sugiere herramientas que se debe tener en cuenta cualquier organización, como mínimo, para así contar con un esquema de seguridad que sirva como línea base para salvaguardar su información.

A continuación se presenta las herramientas brevemente detalladas:

- Antivirus: El objetivo primordial de cualquier antivirus es detectar amenazas informáticas que puedan afectar *PCs* de la organización y bloquearlas antes de que la misma pueda infectar un equipo, o poder eliminarla tras la infección.

Es conveniente disponer de una licencia activa de antivirus, vigente y actualizada así pueda estar preparado para nuevas amenazas.

En la actualidad la mayoría de antivirus vienen integrados con *anti-spam* y *anti-spyware,* en la mayoría de los casos hasta con *firewall*, y manejan dos módulos que son:

Módulo de Control, que se encarga de:

- Protección preventiva del sistema.
- Detección de códigos maliciosos.
- Configuración del funcionamiento del programa antivirus.

Módulo de Respuesta encargado de:

- Registro de incidencias y generación de alarmas.
- Bloqueo de programas sospechosos.
- Desinfección de programas y archivos infectados.

Los virus ocasionan muchos daños desde ocultar la información creando accesos directos hasta la pérdida de información.

- *Firewall*: El *firewall* puede ser un dispositivo o software que permite el filtrado de paquete de datos a partir de reglas que son definidas por el administrador de red, permite o denega el acceso a Internet de manera selectiva, así consiguiendo que el trafico pueda ser filtrado de esta manera obligando a los usuarios cumplir con las restricciones que se hayan definido con anterioridad. Ayudan a las organizaciones a detectar y responder ante intrusiones no deseadas o ataques maliciosos.

  Algunos de los servicios que el *Firewall* ofrece son:

  - Bloqueo del Tráfico no autorizado, se bloquea y se restringe determinadas direcciones de equipos o de ciertas páginas web que se deseen.
  - Se Puede ocultar equipos internos así evitar posibles ataques del exterior.
  - Redirige el trafico entrante de la organización hacia zonas que están restringidas que están vigiladas permitiéndonos monitorear el tráfico.
  - Permite registrar todo el tráfico de la red de la organización, sea este tráfico entrante o saliente.

- *Gateway*: Dispositivo que permite interconectar redes de protocolos y arquitecturas diferentes, el propósito principal es traducir la información del protocolo utilizado en una red inicial al protocolo usado en la red de destino.

Esta herramienta permite analizar los paquetes de datos de un servicio o aplicación según las reglas del protocolo en cuestión y no solo os datos de los paquetes individuales.

- Filtro de correo *anti-spam*: Sistema que sólo permite recibir e-mails de quien tenga autorización. De esta manera únicamente le llegarán los correos de los remitentes a los que usted haya querido dar permiso, evitando el correo basura.

Restringe ciertos contenidos en la red, controlando su acceso. Pueden combinar varias técnicas para tratar de determinar si un determina mensaje de correo se podría considerar como malicioso como:

- Análisis de la estructura y la cabecera del mensaje del correo para así determinar la dirección IP del que envía el mensaje.
- Uso de listas negras, incluye las direcciones IP de servidores que se deseen bloquear.
- Uso de listas blancas, solo permiten el paso de correo de servidores que estén autorizados en la lista.
- Filtros de contenido que eliminan los mensajes que contienen palabras prohibidas, directamente, existe un filtro conocido como: Filtro Bayesiano que empleando una lista de palabras prohibidas y del contexto calcula la probabilidad de que el mensaje sea un correo basura.

Hay que recordar siempre, que se debe capacitar de las políticas de la organización, las herramientas que se está usando, a cada empleado nuevo, y capacitar periódicamente a empleados antiguos.

Los incidentes pueden ocurrir dentro de la organización tarde o temprano, así que como se mencionó con anterioridad, se debe contar con bitácoras y registros que nos permitirá identificar a los responsables de los incidentes, además de contar con

evidencias y los más importante contar con una retroalimentación para así poder aprender de los errores para no volverlos a cometer.

Así que se puede concluir, que se recomienda manejar procedimientos que permitan validar cada herramienta de seguridad así se puede conocer el estado de salud de cada una y si están cumpliendo los objetivos para los que fueron implementadas, ajustándose a la orientación y necesidad de la organización.

CAPÍTULO 3: PRUEBA DE CONCEPTOS, IMPLEMENTACIÓN HERRAMIENTA OPENSOURCE

En este capítulo se presenta una prueba de conceptos, realizada con la herramienta "MyDLP", la cual es una solución para la prevención de fuga de datos, está disponible bajo licencia GPL, la comunidad y la versión empresarial de la solución se encuentran en: http://www.mydlp.com/products

Con "MyDLP" se puede monitorear los datos que se encuentran almacenados dentro de la organización y controlar los flujos de datos, ya que permite detectar y evitar datos salientes no autorizados o clasificados de la red de la organización.

3.1. Partes de "MyDLP"

- Protección y Administración de Servidor con "MyDLP Network Server". Funciona como centro de administración, es un software independiente que se ejecuta en un Servidor Ubuntu.

  Está desarrollado en el lenguaje Erlang[6], debido a su rendimiento en las operaciones de red simultáneas.

- Protección con "MyDLP Endpoint".
  Permite detectar y evitar que los datos se transfieran a dispositivos extraíbles, como memorias USB, desde estaciones de trabajo u ordenadores portátiles, hace cumplir las políticas que se han definido sobre los datos que están almacenados. Está escrito en C++, C#.

- "MyDLP Web UI"
  Está escrito en PHP y Adobe Flex, usa "MySql" para almacenar las configuraciones del usuario.

[6] Lenguaje de programación orientado a la concurrencia.

3.2. Instalación de “MyDLP Network Server”.

Para instalar “MyDLP Network Server” se recomienda descargar la imagen de disco llamada “MyDLP Appliance” de la siguiente dirección http: //www.mydlp.com/getting-started/, este servidor requiere de la instalación previa de un sistema “Ubuntu Server 12.04”.

Para la Prueba de conceptos el servidor se lo instalara en una máquina virtual, emplearemos VMware Workstation.

1. Cargamos la imagen “MyDLP Appliance”, en el dispositivo CDROM / DVD-ROM del menú de arranque de la máquina.

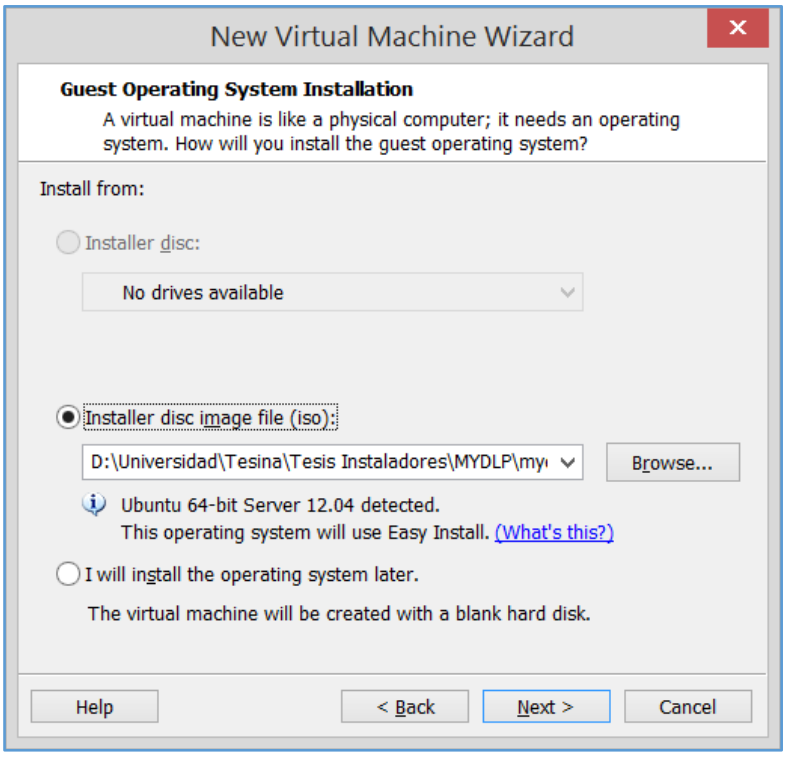

Figura 4: Carga de la imagen “MyDLP Appliance” (Rendón Moisés).

2. Seleccionar idioma de instalación.

Figura 5: Selección de Idioma (Rendón Moisés).

3. Seleccione Instalar MyDLP Appliance.

Figura 6: Selección de opción “Install MyDLP Appliance” (Rendón Moisés).

4. Seleccione Idioma del Sistema Operativo.

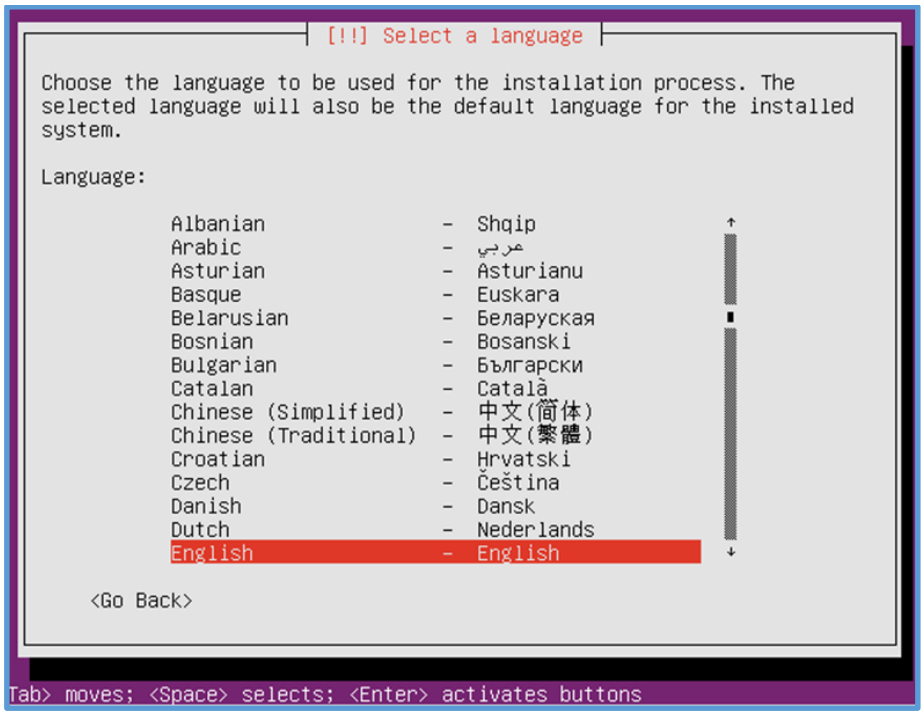

Figura 7: Selección del idioma del Servidor (Rendón Moisés).

5. Seleccione su país.

6. Seleccione país, modo de distribución de teclado, zona horaria, según desee.

7. Introduzca el nombre de usuario y contraseña que servirá como ingreso al sistema operativo, la contraseña deberá ser robusta.

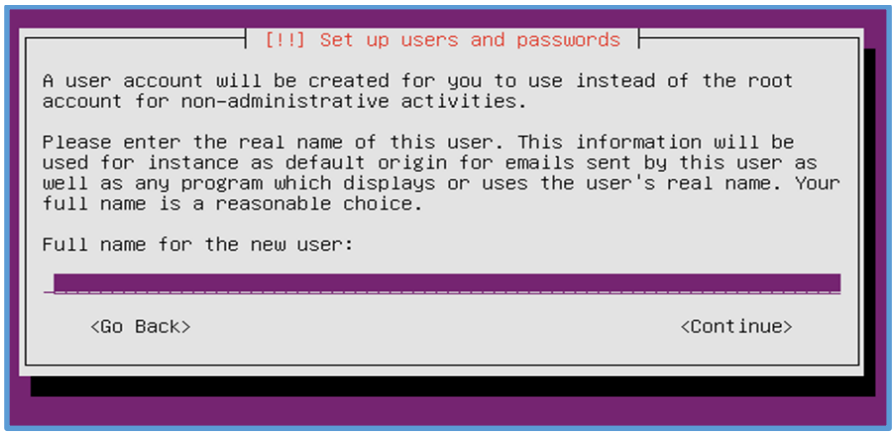

Figura 8: Establecer nombre de Usuario (Rendón Moisés).

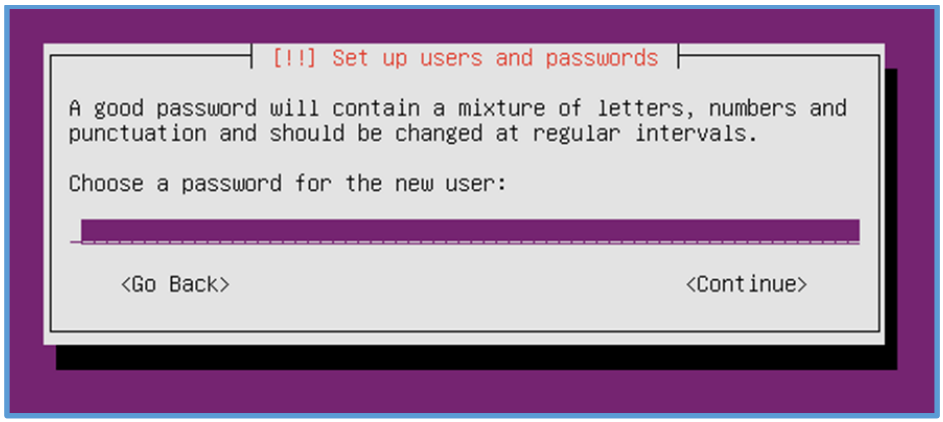

Figura 9: Establecer contraseña (Rendón Moisés).

8. Espere a pasos de instalación automática para terminar.

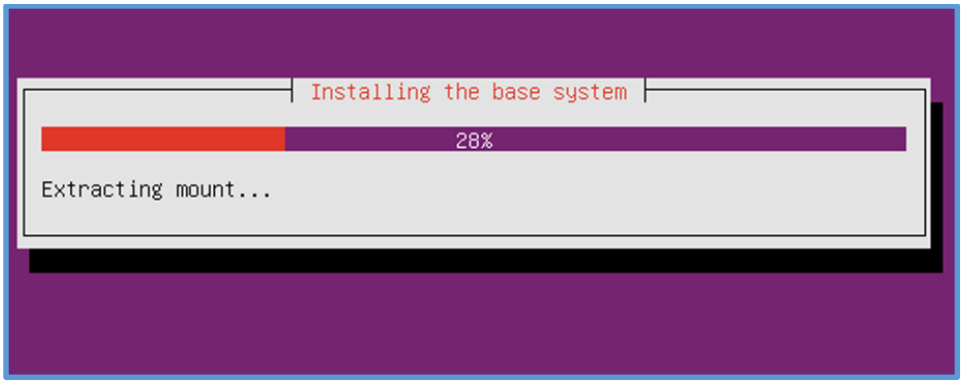

Figura 10: Instalación del Sistema (Rendón Moisés).

Luego de terminar la instalación, ingresamos a la consola de administración con el nombre de usuario y la contraseña que establecimos anteriormente.

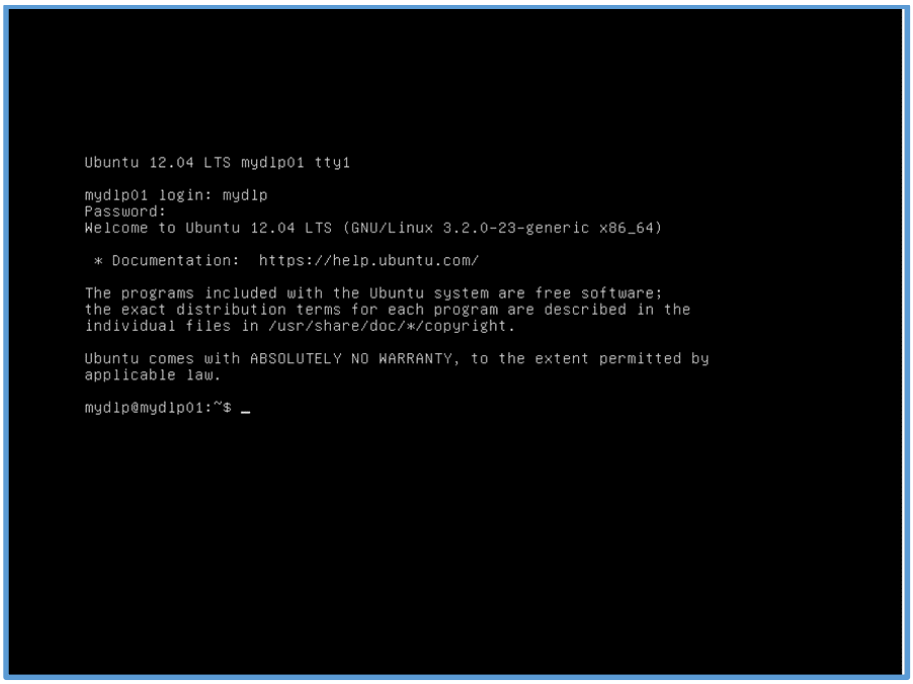

Figura 11: Consola del Servidor (Rendón Moisés).

Para la configuración inicial de “MyDLP Network Server” usaremos el comando: sudo pico –t /etc/network/interfaces
Agregamos las siguientes líneas de acuerdo a la configuración de la red establecida. Por ejemplo:

iface eth0 inet static
address 192.168.1.100
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1

La siguiente imagen muestra cómo debería quedar:

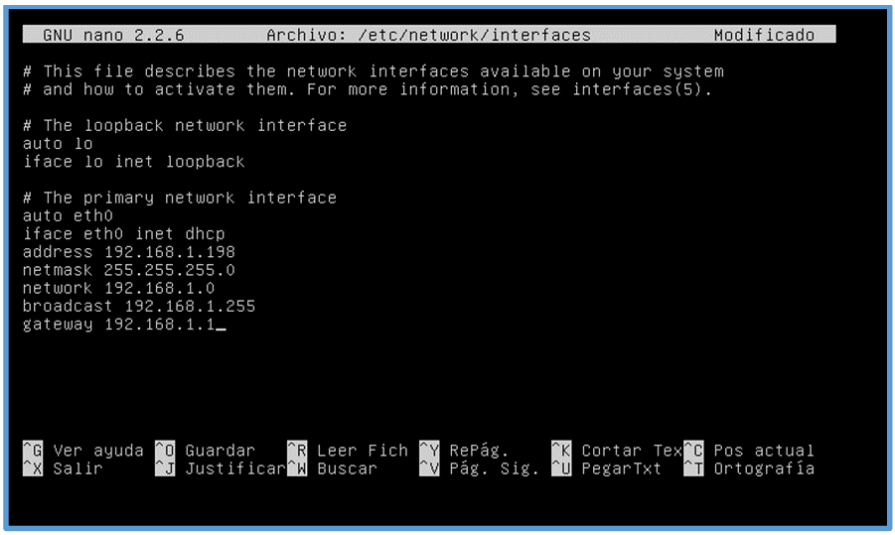

Figura 12: Configuración de red del servidor (Rendón Moisés).

Reiniciamos el servicio de redes con el comando:

sudo /etc/init.d/networking restart

Para ingresar al servidor lo haremos desde un explorador web, para ello debemos configurar en las Opciones de Internet.

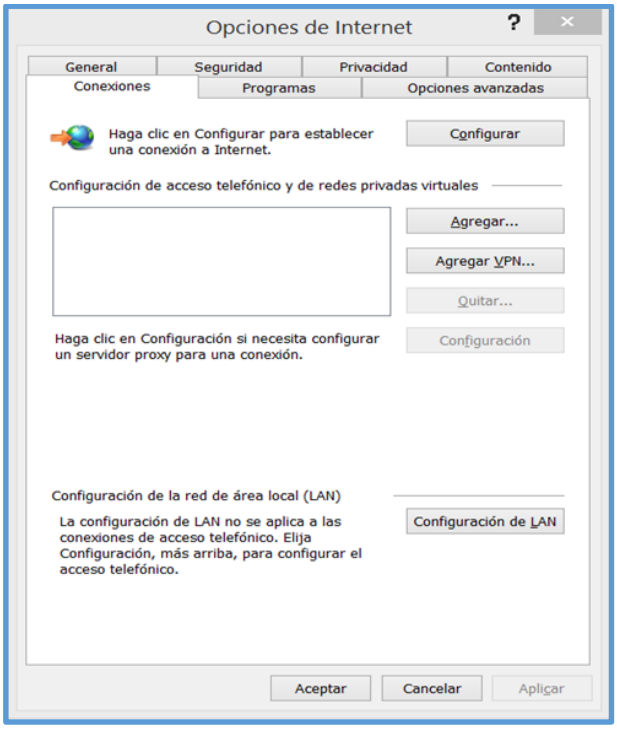

Figura 13: Ventana de Opciones de Internet (Rendón Moisés).

Hacemos *Click* en Configuración de LAN

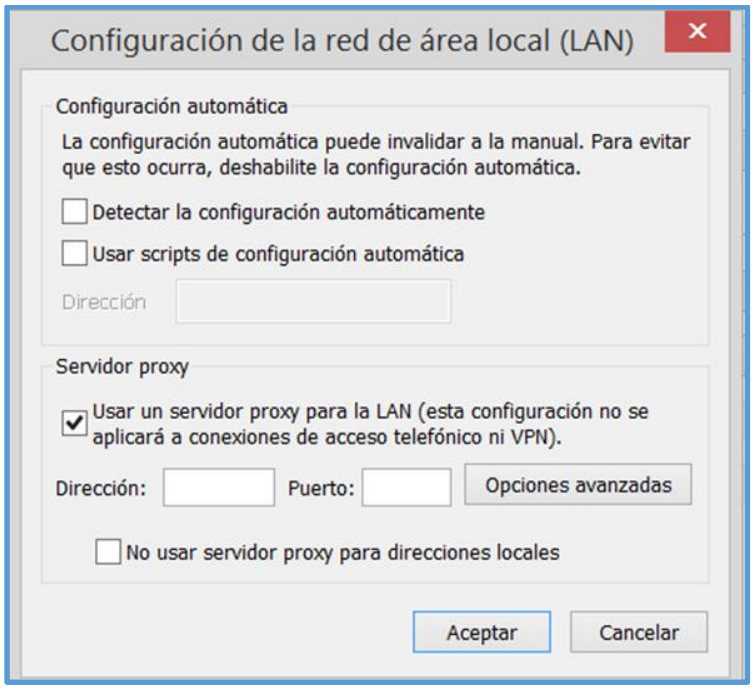

Figura 14: Configuración de red de área Local (Rendón Moisés).

Ingresamos la dirección Ip que configuramos previamente, y en puerto se establece 3128 y aceptamos. Luego ingresamos en la barra de direcciones la Ip del servidor y nos presentara la siguiente página.

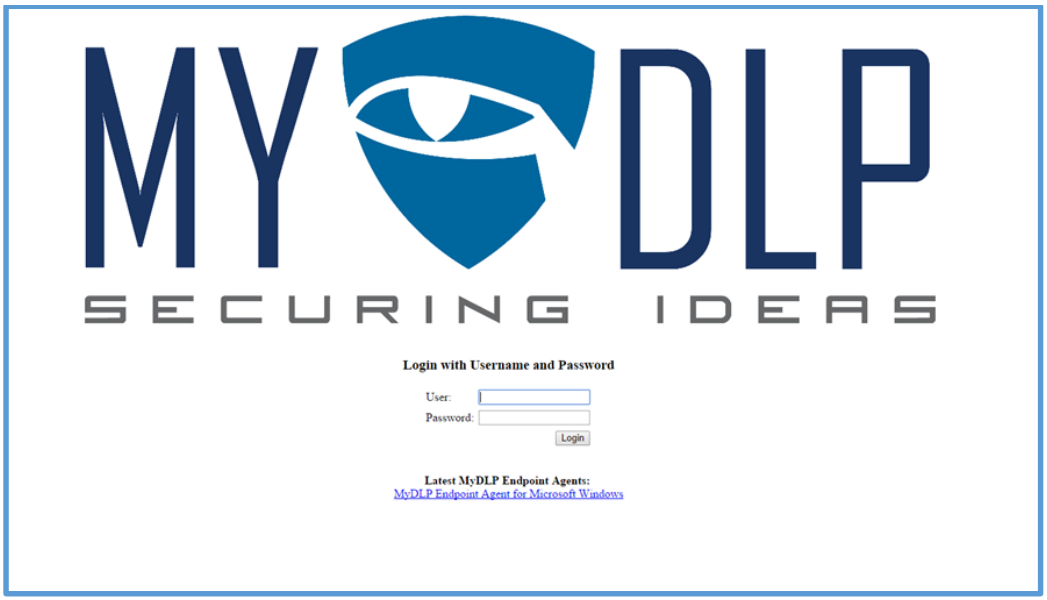

Figura 15: Pantalla de inicio de “MyDLP” (Rendón Moisés).

Ingresamos el usuario y contraseña que establecimos en la instalación previa para acceder a la página principal de “MyDLP”.

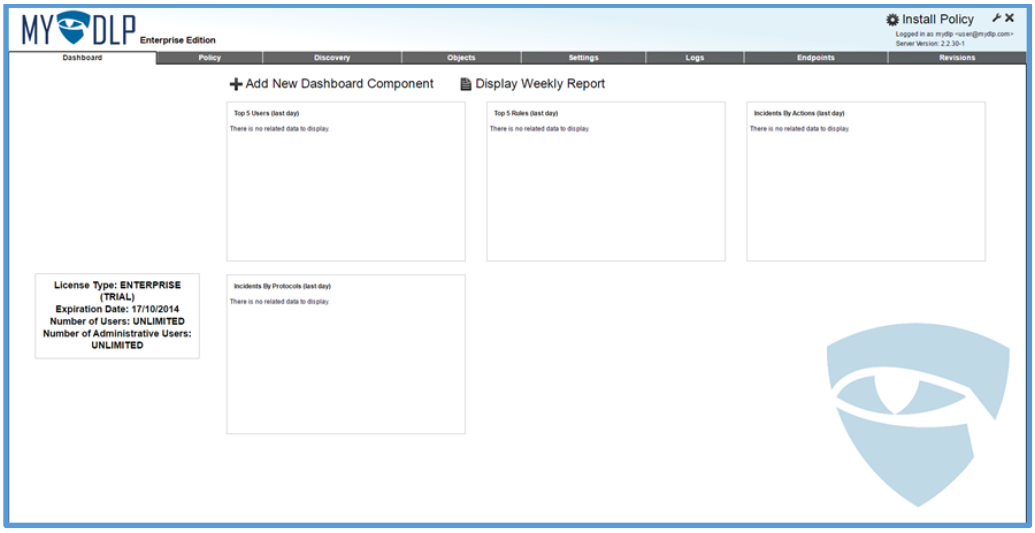

Figura 16: Pantalla Principal de “MyDLP” (Rendón Moisés).

Para comprender de mejor manera la prueba de conceptos, que se realizara en la sustentación de este documento, se presentara algunos conceptos a tener en cuenta.
Para introducir una política se tienen:

- Tabla de Reglas:
  La tabla de reglas contiene las reglas del DLP que se han definido, van en orden de prioridad de importancia.

- Tipos de reglas:
  Hay ocho tipos de reglas diferentes y se clasifican de acuerdo al tipo de información a ser inspeccionada.

Cada tipo de regla es efectiva sólo en el canal de flujo de datos relacionados, a continuación se explican las reglas disponibles:

- Regla de Web: Se utiliza para monitorizar y controlar el tráfico de Internet.
- Regla de correo: Se utiliza para supervisar y controlar los e-mails.
- Regla de almacenamiento extraíble: se utiliza para controlar los datos transferidos a los dispositivos de almacenamiento, como memorias USB, discos duros extraíbles, etc.
- Regla de almacenamiento Encriptado: Permite encriptar los dispositivos de memoria extraíbles, como la memoria USB palos, discos duros extraíbles.
- Regla de almacenamiento de entrada Extraíble: Se utiliza para controlar el copiado de archivos en los dispositivos de memoria extraíbles.
- Regla de impresora: Se utiliza para controlar la impresión de documentos.
- Regla Captura de pantalla: Evita que la función de impresión de pantalla se ejecute mientras que una aplicación sensible se está ejecutando.
- Regla API: es una característica única de MyDLP, permite integrar las aplicaciones que empleen con MyDLP.

3.3. Estructura de la Regla.

Figura 17: Estructura de una Regla (Rendón Moisés).

La primera parte es el tipo de canal y el nombre de la regla. El tipo de la regla determina el canal de datos para ser inspeccionado, La segunda parte es la restricción de las fuentes que restringe la regla en un determinado usuario o un grupo de usuarios puede ser definido por dirección IP, red, elemento de Active Directory o una dirección de correo electrónico dependiendo del tipo de regla, Se requiere la columna Fuentes para todo tipo de reglas.

La tercera parte es los Destinos, puede variar dependiendo por el tipo de regla, puede ser dirigido hacia un dominio, directorios o nombres de aplicaciones.

La cuarta parte es el tipo de información que se debe buscar en el canal de datos relacionados durante la inspección. La última parte es la acción que se desea tomar cuando la regla se ejecute, las acciones disponibles son: “Pass”, “Block”, “Log”, “Quarantine” y “Archive”.

- Pass: Permite que la información pase a través del canal de datos libremente.
- Block: Evita que la información pase a través del canal de datos y genera registro de eventos.
- Log: Permite que la información pase a través del canal de datos, pero genera un log.
- Quarantine: Impide que la información pase, genera registro de eventos y archivos de una copia de la información.

- Archive: Permite que la información pase a través del canal de datos, genera evento registro y archivos de la copia de la información.

3.4. Prueba de Concepto

Para la prueba de concepto se simulo una red que contiene dos máquinas conectadas al servidor Ubuntu donde está instalada previamente “MyDLP”. Una maquina tiene el SO Windows 8.1 y la otra Windows 7, las dos máquinas están instaladas previamente la aplicación “MyDLP Endpoint”.

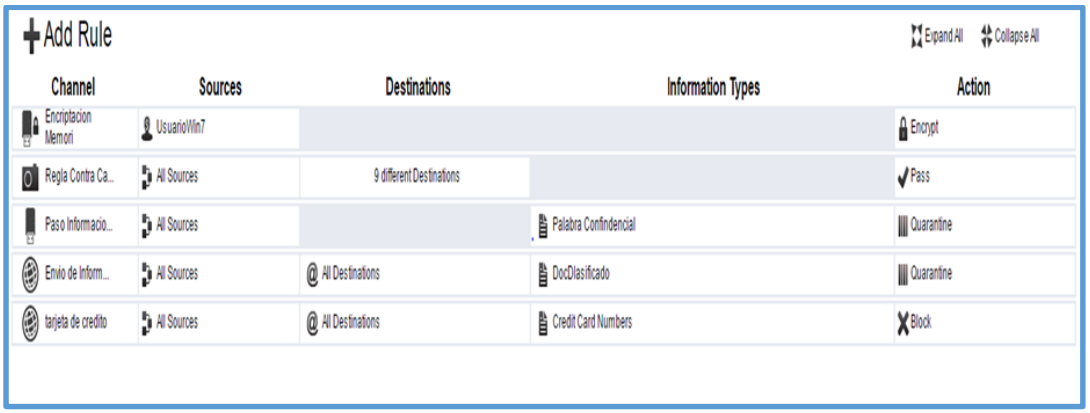

Figura 18: Reglas implementadas en la Prueba de conceptos (Moisés Rendón).

Como se ve en la Figura 18, se ha implementado cinco reglas que a continuación se detallara.

- Regla de Protección de envió de patrón de número de tarjetas de crédito, vía Mail.

  Esta regla bloquea él envió de mail, cada vez que detecta algún patrón de modelo de un número de tarjeta de crédito, que se encuentra en el cuerpo del correo electrónico.

Figura 19: Correo no enviado si se detecta un patrón de número de tarjeta de crédito (Moisés Rendón).

Como se observa cada vez que se detecta un patrón de número de tarjeta de crédito, envía un mensaje que existió un error y no envió el mensaje, en este caso dentro de un mensaje de texto se envió un patrón de número de tarjeta de crédito 4111 1111 1111 1111, por lo tanto no envía el mensaje.

- Regla de Protección de envió de información clasificada vía Mail.
  Esta regla, si detecta que se está adjuntando un documento que ha sido clasificado previamente, bloquea que este documento pueda ser adjuntado en un correo electrónico, para evitar así que pueda ser enviado.

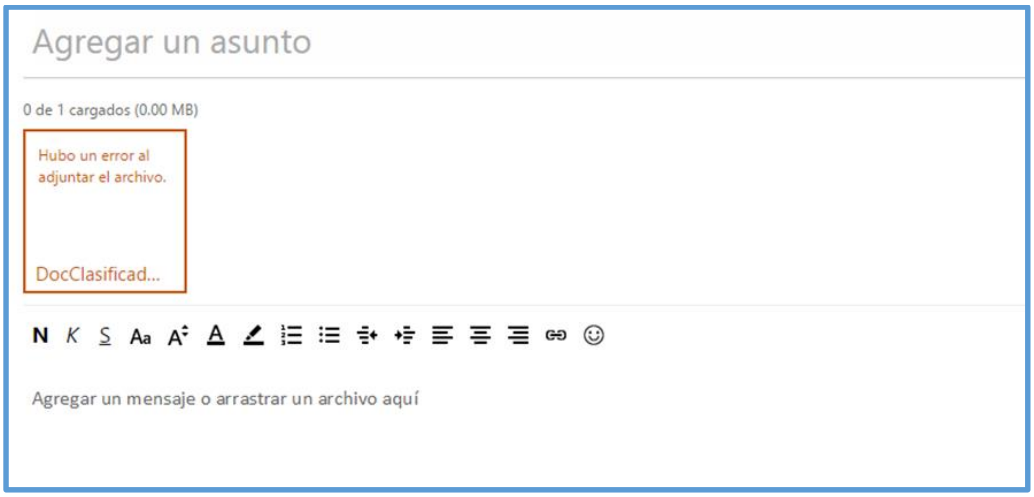

Figura 20: Error al adjuntar un Documento Clasificado (Moisés Rendón).

Como se puede observar en la Figura 20, evita que se pueda adjuntar un archivo clasificado, para ello indicando que hubo un error al adjuntarlo.

- Regla de Protección de envió de información clasificada hacia Memoria Usb. Brinda un gran apoyo para proteger documentos clasificados, asignándoles palabras restringidas, bloqueando su paso a una memoria extraíble cuando encuentra una de estas palabras, genera un log donde se podrá observar la hora, fecha y quien violo la regla.

A continuación restringimos la palabra “Clasificado” así que cuando deseamos pasar algún documento que contenga esta palabra no permitirá su paso hacia

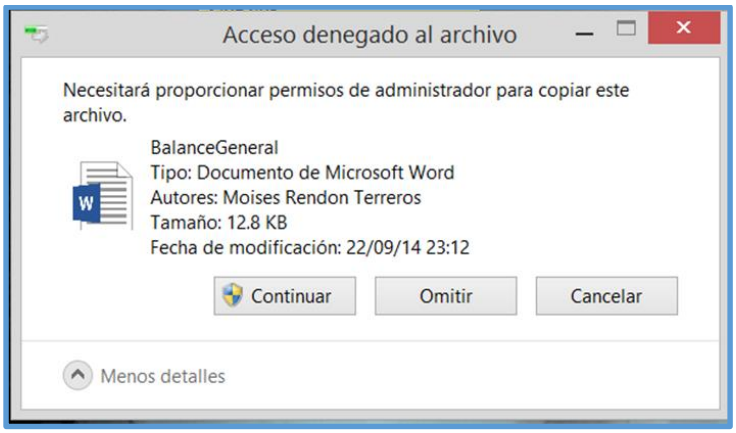

Figura 21: Acceso denegado para copiar información clasificada (Moisés Rendón).

Cabe mencionar que se pueden generar una lista de palabras clasificadas.

- Regla de bloqueo de Captura de pantalla.

Esta regla nos permite bloquear las capturas de pantalla que se puede realizar con la abreviatura de teclado FN- PRTSC, las bloquea automáticamente

dependiendo de la fuente al que le asignemos, en este caso está contemplado para todos los “endpoints” que estén en la red, no genera informes en los log.

Así que cada vez que intentemos hacer una captura de pantalla no se lo podrá hacer ya que esa función está bloqueada.

- Regla, Encriptación y formateo de Memoria Usb extraíble.

Esta regla permite que cada vez que se ingrese una memoria USB extraíble se deba formatear para su uso dentro de las fuente que este configurada, al formatearlo lo encripta para que no pueda ser usado fuera de la fuente que no tenga permiso, para esta prueba se asignó a la computadora con Windows 7 como fuente que encripta la memoria a continuación veremos que cada vez que se conecta una memoria Usb a la PC Windows 7 pide formatear para su uso, esta regla no genera log.

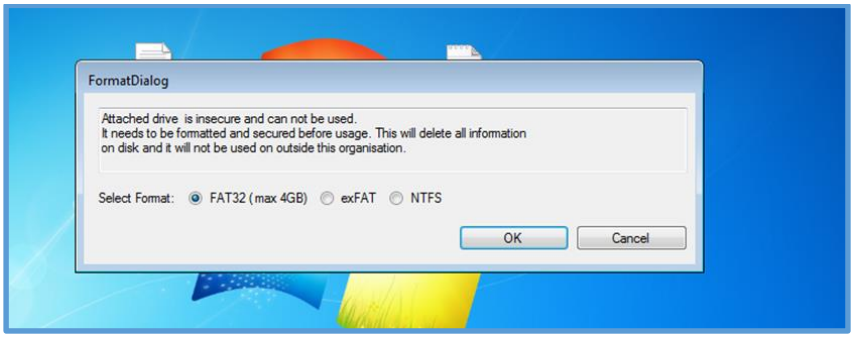

Figura 22: Petición de “MyDLP” para formatear la Memoria Usb para así encriptarlo que pueda usado (Moisés Rendón).

Al conectarlo en otra máquina que no tenga permiso de uso, nos pedirá formatearlo, de esta manera protegiendo la información que este contenga.

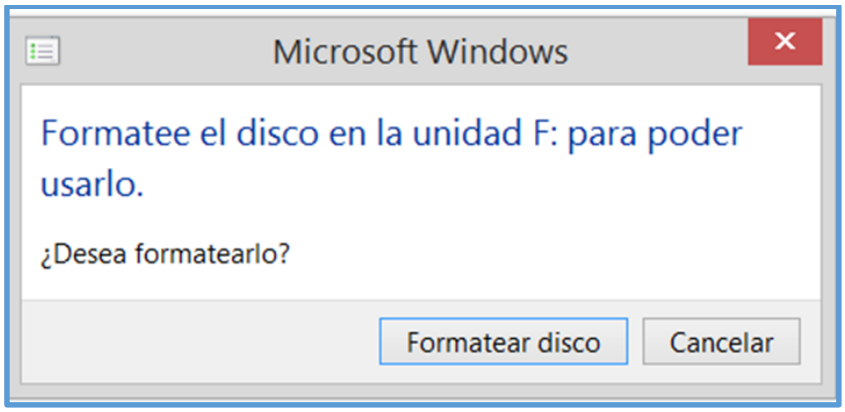

Figura 23: Mensaje que explica que la Memoria Usb no se puede usar y se tiene que Formatear (Moisés Rendón).

Cada vez que se incumple una regla generada, si lo configuramos con acciones de “Log”, “Quarantine” y “Archive”, se generara un log que almacena: la fecha, hora, fuente, acción, canal y regla que fue violada.

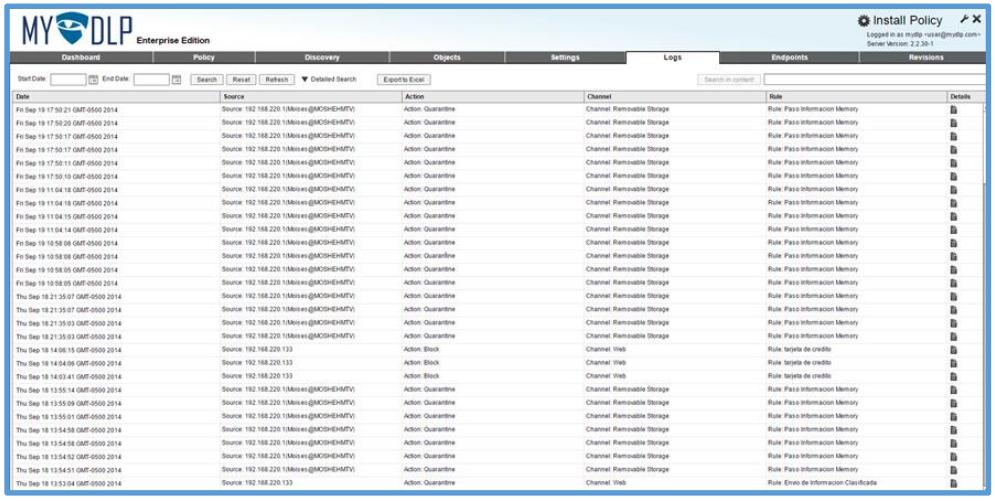

Figura 24: Logs que se generan cuando se incumple una Regla, si se configura para que se generen (Moisés Rendón).

CAPÍTULO 4 CONCLUSIONES Y RECOMENDACIONES.

Conclusiones.

Con el desarrollo de este trabajo investigativo se denota la importancia que tiene la protección y prevención de fuga de información en cualquier organización, y que existen herramientas que nos pueden ayudar a conseguir este objetivo.

Con el trabajo investigativo realizado se ha conseguido adquirir y actualizar los conocimientos sobre mejores prácticas, medidas y herramientas que nos ayuden a garantizar la debida gestión de la información y su debido trato a nivel de confidencialidad.

Se logró desarrollar una guía de implementación estándar que puede ser aplicada en cualquier organización.

Con la prueba de conceptos se puso en práctica el conocimiento adquirido a lo largo del desarrollo de este trabajo investigativo, comprobando la importancia de contar con una herramienta de DLP como una medida proactiva y básica para garantizar la confidencialidad de la información de una empresa.

Este documento en un futuro puede servir como fuente bibliográfica para futuros trabajos académicos o se pueda llevar a cabo una implementación de DLP en alguna organización.

Recomendaciones.

Se recomienda siempre mantener actualizados las políticas de la organización, sobre todo las que están vinculadas con el manejo de la información, además de tener una revisión constante de buenas prácticas, estándares de seguridad como la norma ISO/IEC 27001, para así tener un mejor manejo y protección de la información confidencial,

Además de revisar las políticas y la metodología de implementación, se debe revisar el sistema DLP a implementar, según las necesidades de la organización, la herramienta Open-Source “MyDLP” es una herramienta muy amigable, y luego de la prueba de conceptos se recomienda su implementación.

Las organizaciones deben manejar un sistema de capacitación periódica a los empleados, nuevos y antiguos, sobre las políticas, metodología y herramientas que

esta implementado; ya que con usuarios capacitados se puede reducir fugas de información.

Cuando se inicie un plan de implementación de un sistema DLP, se deben tener presente los principales, riesgos, amenazas y vulnerabilidades a las que se están expuestas y como se beneficiará, cuando se culmine la implementación.

Bibliografía

ALIDE. (2013). ¿Cómo gestionar activos de la información. *ALIDE*, 1-5.

Berciano, J. (s.f.). *redseguridad*. Obtenido de http://www.redseguridad.com/opinion/articulos/la-importancia-y-la-necesidad-de-proteger-la-informacion-sensible

Cardozo González, L. F., & García Severiche, B. (09 de Mayo de 2013). *Slideshare*. Obtenido de http://www.slideshare.net/bgarcias18/prevencin-de-perdida-de-datos-data-loss-prevention

Diario, E. (28 de Marzo de 2013). *El Diario*. Obtenido de http://www.eldiario.ec/noticias-manabi-ecuador/257319-denuncian-fuga-de-informacion-en-la-fiscalia-de-chone/

iso27000. (22 de 06 de 2014). *iso27000*. Obtenido de http://www.iso27000.es/download/doc_iso27000_all.pdf

Kanagasingham, P. (15 de Agosto de 2008). *Sans Institute*. Obtenido de http://www.sans.org/reading-room/whitepapers/dlp/data-loss-prevention-32883

Mercurio, E. (12 de Junio de 2012). *El Mercurio*. Obtenido de http://www.elmercurio.com.ec/336414-carvajal-ordena-investigar-posible-fuga-de-informacion/#.VBDgl_l5Oos

Mogull, R. (03 de April de 2008). *Websense, Inc*. Obtenido de http://www.websense.com/content/understanding-selecting-dlp-reg.aspx

Neira, A. L., & Ruiz Spohr, J. (22 de 05 de 2005). *iso27000*. Obtenido de http://www.iso27000.es/

Pepper, C. (19 de Junio de 2012). *Securosis*. Obtenido de https://securosis.com/assets/library/reports/Implementing_and_Managing_DLP.v.1.pdf

Vieites, A. G. (2007). Enciclopedia de la seguridad informatica "Amenazas a la seguridad informatica". En A. G. Vieites, *Enciclopedia de la seguridad informatica "Amenazas a la seguridad informatica"* (págs. 25-26). Madrid: Alfaomega.

DOCTOR ROMEL MACHADO CLAVIJO,

SECRETARIO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACION

DE LA UNIVERSIDAD DEL AZUAY,

C E R T I F I C A:

Que, el H, Consejo de Facultad de Ciencias de la Administración en sesión del 27 de junio de 2014, conoció la petición del señor **MOISES RENDON TERREROS (47600),** que denuncia su trabajo de titulación denominado: **"PREVENCION Y MINIMIZACION DE FUGA DE INFORMACION IMPLEMENTANDO DLP (DATA LOST PREVENTION)",** presentado como requisito previo a la obtención del Grado de Ingeniero de Sistemas y Telemática. El Consejo acoge el informe de la Junta Académica y aprueba la denuncia. Designa como Director de dicho trabajo al ingeniero Fernando Aguilar Ochoa y como miembro del Tribunal Examinador al ingeniero Paúl Ochoa Arévalo. De conformidad a las disposiciones reglamentarias el denunciante deberá presentar su trabajo de monografía en un plazo máximo de **TRES MESES** contados a partir de la fecha de aprobación, esto es hasta el 27 de septiembre de 2014.

Cuenca, junio 27 de 2014

UNIVERSIDAD DEL AZUAY
FACULTAD DE ADMINISTRACION
SECRETARIA

CONVOCATORIA

Por disposición de la Junta Académica de Ingeniería de Sistemas, se convoca a los Miembros del Tribunal Examinador, a la sustentación del Protocolo del Trabajo de Titulación "PREVENCION Y MINIMIZACION DE FUGA DE INFORMACION, IMPLEMENTANDO DLP (DATA LOSS PREVENTION)", presentado por el estudiante Moisés Rendón Terreros con código 47600, previa a la obtención del grado de Ingeniero de Sistemas y Telemática, para el día **JUEVES 22 DE MAYO DE 2014 A LAS 08h30.**

Cuenca, 14 de mayo de 2014

Dra. Jenny Ríos Coello
Secretaria de la Facultad

Ing. Fernando Aguilar Ochoa X

I
ng. Paúl Ochoa Arévalo .....

comunicado

Oficio Nro. 046-2014-DIST-UDA

Cuenca, 07 de Mayo de 2014

Señor Ingeniero
Xavier Ortega Vázquez
DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMNISTRACIÓN
Presente.-

De nuestras consideraciones:

La Junta Académica de la Escuela de Ingeniería de Sistemas y Telemática, reunida el día 07 de Mayo del 2014, revisó el proyecto de monografía titulado "Prevención y Minimización de Fuga de Información, Implementando DLP(Data Lost Prevention)", presentada por el estudiante Moisés Rendón, estudiante de la Escuela de Ingeniería de Sistemas y Telemática, previo a la obtención del título de Ingeniero de Sistemas y Telemática.

La Junta considera que el diseño de trabajo de titulación cumple con los requisitos normados en la "Guía de Elaboración y Presentación de la Denuncia/Protocolo de Trabajo de Titulación", razón por la cual solicita, por su digno intermedio, notificar al tribunal designado y determinar lugar, fecha y hora de sustentación.

Por lo expuesto, y de conformidad con el Reglamento de Graduación de la Facultad, recomienda como director y responsable de aplicar cualquier modificación al diseño del trabajo de graduación posterior al Ing. Fernando Aguilar Ochoa (Docente del Curso de Graduación), y como miembro del Tribunal al Ing. Paúl Ochoa Arévalo.

07/05/2014
Autorizado.
Por favor notifique lo solicitado.
Gracias
May 7 2014

Atentamente,

Ing. Marcos Orellana Cordero
Director Escuela de Ingeniería de Sistemas y Telemática
Universidad del Azuay

Cuenca, 11 de Junio del 2014

Ing. Xavier Ortega

Decano de la Facultad de Ciencias de la Administración

Ciudad

De mi consideración:

Suscribo e informo a Usted que he procedido a revisar el trabajo de diseño de investigación de tercer nivel intitulado: **"Prevención de fuga de información, implementando DLP (Data Loss Prevention)"** presentado por el estudiante Moisés Rendón Terreros egresado de la Escuela de Sistemas y Telemática, como requisito previo a la obtención del Título de Ingeniero en Sistemas y Telemática, cumpliendo de esta forma con los cambios sugeridos por el tribunal académico. Finalmente informo a usted Sr. Decano que autorizo el desarrollo del mismo.

Sin más por el momento me despido de usted.

Atentamente

Ing. Fernando Aguilar Ochoa

UNIVERSIDAD DEL AZUAY

Cuenca, 8 de Mayo del 2014

Ing. Xavier Ortega

Decano de la Facultad de Ciencias de la Administración

Ciudad

De mis consideraciones:

YO, MOISES RENDON TERREROS con código 47600, estudiante de la Escuela de Sistemas y Telemática, solicito a usted de la manera más respetuosa y por su intermedio al Honorable Consejo de Facultad, se sirvan revisar mi diseño de tesis titulado: **"Prevención y Minimización de fuga de Información, implementando DLP (Data Loss Prevention)"**, previo a la obtención del título de Ingeniero en Sistemas y Telemática.

Me permito sugerir el nombre del Ing. Fernando Aguilar Ochoa como director, el cual fue docente de la catedra de "Seguridad Web" en el curso de graduación, además me ha asesorado en la elaboración del presente esquema y además cuento con su aceptación.

Por la favorable acogida que se sirva a la presente, suscribo a usted.

Atentamente

Moisés Rendón Terreros

0105947824

Edición autorizada de 20.000 ejemplares
Del 618.501 al 638.500
Nº 0629955

Universidad del Azuay

Facultad de Ciencias de la Administración

Escuela de Sistemas y Telemática

Diseño de Monografía Final

Autor: Moisés Rendón Terreros

Cuenca, Ecuador

2014

DATOS GENERALES

Nombre del estudiante: Moisés Rendón Terreros.
Código: 47600

Contacto:
Teléfono: 2819522.
Celular: 0992635963.
Correo electrónico: moshehmtv@hotmail.com

Director sugerido:
Fernando Aguilar Ochoa, **Ing. MAE**, Ingeniero en Sistemas, Magister en Administración de Empresas

Contacto
Teléfono: 2832500 ext. 1434
Celular: 0989618013
Correo electrónico: faguilar@baustro.fin.ec

Co-director sugerido:
Esteban Crespo, **Ing.**

Contacto
Teléfono: 4091000
Celular: 0996804562
Correo electrónico: ecrespo@uazuay.edu.ec

Tribunal Designado
Ing. Paúl Ochoa Arévalo

Código UNESCO:
Línea: 1203 Informática de computadores
Programa: 1203.99 Sistemas de Seguridad de la Información

Tipo de trabajo:
Proyecto de investigación formativa.

Área de estudio:
Seguridad de la Información

Título propuesto:
"Prevención de fuga de información, implementando DLP (Data Loss Prevention)".

Estado del proyecto:
El trabajo es nuevo, orientado a la seguridad de la información.

CONTENIDO

Motivación de la investigación:

La presente investigación surgió por la necesidad de prevenir fugas de información que existen muchas veces en las empresas, organizaciones, instituciones etc. Hoy en día la información es el activo más importante que posee cualquier organización, la mayoría de veces permite generar ventaja a quien la posee, es por esto que el éxito de una organización o empresa no solo depende del manejo de sus recursos materiales como el capital, también depende de cómo se aprovechen sus activos intangibles, en este caso la información que ellos generan.

A medida que la tecnología crece y evoluciona, hace que salvaguardar la información, necesite de procedimientos más complejos y eficientes para prevenir robos y el mal manejo de la información.

Problemática:

Durante el año 2010 se dio un caso de fuga de información muy discutido denominado el caso “Wikileaks”, pero lo importante a enfatizar es que esta problemática no es nueva dentro del campo de la seguridad de la Información, sin embargo la evolución tecnológica y empresarial ha ido dando mayor relevancia a la gestión efectiva de la información, llegando a convertirse en la actualidad en el principal activo de toda empresa.

Las Organizaciones hoy en día no disponen de un esquema de buenas prácticas que garantice el correcto manejo de la información, esto pone en un riesgo muy alto la información confidencial. Los diferentes dispositivos portátiles y de almacenaje extraíbles, también representa una amenaza muy grande, y las organizaciones no cuentan con políticas ni implementaciones que permitan evitar que estas se convierten en víctimas de fugas de información, así evitándoles gastos muy altos que muchas veces se representan en pérdidas de clientes o indemnizaciones sin dejar de lado el coste de recuperar la confianza de una empresa cuya información ha sido robada o falsificada. Esto abarca lo referente a riesgo operativo, riesgo legal y riesgo reputacional.

Pregunta de investigación:

¿Se puede prevenir y minimizar la fuga de información, implementando un DLP (Data Loss Prevention - Prevención de perdida de información)?

Resumen:

Lo que se pretende es investigar buenas prácticas, estándares y herramientas que permitan implementar un DLP y nos permitan construir una guía de implementación estándar que pueda acoplarse a cualquier empresa, con la intención de minimizar o prevenir fugas de información. Como ya se mencionó con anterioridad, muchas organizaciones no saben cómo proteger sus datos, ni la importancia de los mismos, por lo tanto no tiene políticas para salvaguardar su información.

Estado del Arte y marco teórico:

Un DLP (Data Loss Prevention) se encarga de prevenir el robo, acceso o salida de datos de una empresa, ya sea accidental o de manera consciente. En la actualidad se ha vuelto una necesidad de las grandes y medianas empresas por la gran cantidad de información sensible que gestionan día a día.
DLP es un término que se emplea en el área de seguridad de la información que hace referencia a los sistemas que identifican, supervisan y protegen los datos que se procesan, transmiten o almacenan. Los sistemas están diseñados para detectar y prevenir el uso no autorizado y la transmisión de información privada, sensible y confidencial principalmente acorde a la clasificación de la información de cada entidad.

La fuga de información no es tan reciente, desde el año 2007 se han denunciado el robo y vulneración de cuentas de usuarios de diversas empresas como “Monster”, “Tuenti”, entre otros. En el Ecuador por ejemplo: la Fiscalía de Chone denuncio que existió fuga de información y aseguro que nadie conocía la existencia de este incidente.

Existen varios escenarios en los cuales se puede implementar DLP como: hospitales, sector financiero, alimenticio, jurídico, político, entre otros.

Existen diferentes mecanismos de clasificación entre los que podemos encontrar:

- Clasificación en varios niveles: resguarda tanto la información contextual como el contenido.
- Registro de documentos: incluye diferentes tipos de acceso biométricas de información a medida que cambia.
- Clasificación de archivos: identifica el tipo de contenido independientemente de la extensión del archivo o del tipo de compresión en el que este.

EL DLP con cualquier herramienta empleada deben ser minuciosamente configuradas, para lo cual se solicita conocer el valor de la información, y este se obtiene realizando un estudio de evaluación/inventario de activos de información y clasificación de la información. Así se pueden conocer el valor de los activos, información, que se desean proteger.

Mientras mayor sea el número de personas que comparten información de forma digital, mayor es el riesgo de que alguien de manera involuntaria o intencionada envíe información confidencial a una persona no autorizada y ponga en riesgo los datos de la empresa. Existiendo varios medios como por ejemplo: a través del correo electrónico, la Web, FTP, etc.

Algunos mensajes o transacciones están autorizados, pero deben cifrarse para garantizar la privacidad de los datos. Otros tipos de comunicaciones simplemente no son aceptables en ningún momento y deben bloquearse. La implementación de las directivas adecuadas en el momento justo es esencial para garantizar la seguridad de los datos, el cumplimiento de las normativas y la protección de la propiedad intelectual.

Cualquier implementación de un sistema de este tipo, puede salir muy costoso tanto a nivel de licencias como a nivel de la propia implementación.
En resume, la fuga de información se puede dar de manera espontánea, sea esta por error, omisión, o de una manera voluntaria. Proteger la información de la organización es crucial ya que se correlaciona con el valor monetario de la misma. DLP, no solo previene la fuga de información sino que además la protege, no debe tomarse como una opción, sino como una iniciativa crítica para proteger el activo más importante de una organización: La información.

Objetivo general:

Prevenir la fuga de información de una empresa, con la implementación de una Herramienta de DLP (Data Loss Prevention - Prevención de perdida de información).

Objetivos específicos:

- Explicar que es una DLP y sus principales funcionalidades.
- Proponer una guía estándar de implementación de DLP, que pueda ser acogida por cualquier empresa.
- Realizar una prueba de concepto, con la aplicación DLP “OpenDLP”.

2.9 Metodología:

La presente investigación se realizara a través de diferentes consultas de documentos como: libros, libros digitales, revistas etc. Se empleará todos estos documentos para recolectar información y de esta manera proceder a seleccionar, analizar y presentar un documento de información que sirva en un futuro como fuente bibliográfica y sea de ayuda a las personas que lo consulten.

La investigación es co-relacional ya que persigue medir el grado de relación existente entre el nivel de implementación de DLP de una organización y el nivel de confiabilidad, integridad y disponibilidad de la información de dicha organización.

Alcances y resultados esperados:

Lo que se espera es poder cumplir cada uno de los objetivos mencionados y de esta manera documentarlos, la información procesada, para que en un futuro pueda servir como fuente bibliográfica para futuros trabajos académicos o se pueda llevar a cabo una implementación de DLP en alguna organización.

Supuestos y riesgos:

El principal riesgo es que no se pueda encontrar información sobre organizaciones que hayan podido con éxito implementar un DLP o que no se tenga un amplio acceso a esta información, ya que muchas veces nos encontramos que esta información está clasificada por no tener una costumbre de compartir información, y que esta área de seguridad es desconocida en nuestro país.

2.12 Presupuesto: debe incluir una tabla de presupuesto que contenga:

Rubro-Denominación	Costo USD (detalle)	Justificación ¿para qué?
Hojas	$10,00	Impresión de diseño, tesis.
Copias	$ 5,00	Recolección de Información.
Empastado de tesis	$ 30,00	Presentación de trabajo final.
Carpetas	$ 2,00	Presentación de avances.
Útiles de oficina	$ 3,00	Desarrollo del trabajo.
Hojas Membretadas	$5,00	Hojas para impresión de solicitudes
TOTAL	$55,00	

Financiamiento

El proyecto será autofinanciado es decir que los recursos económicos serán propios.

Esquema tentativo:

Introducción.
Descripción de la Problemática.
Justificación.

Capítulo 1 Conceptos Generales:
1.1 ¿Qué es un DLP?
1.2 Función del DLP.
1.3 Características de un DLP.
1.4 Prevención de Fuga de Información.
1.5 Causas y Factores principales para que exista perdida de datos en las empresas.
1.6 Necesidad de proteger el negocio
1.7 Escenarios de implementación de DLP.

Capítulo 2 Metodología de Implementación:

2.1 Clasificación de usuarios y propietarios de la Información.
2.2 Identificación de salidas de información.

2.2.1 Diagrama de red estándar
2.2.2 Definición de políticas de uso aceptable de las herramientas tecnológicas
2.2.3 Clasificación de la información de acuerdo a su criticidad
2.3 Configuración de parámetros de control de salidas de información.
2.4 Alertamiento y bloqueo de salida de información de acuerdo a su criticidad.
2.5 Estabilización y mantenimiento, mejora continua.

Capítulo 3: Prueba de conceptos, implementación demo de "OpenDLP".

Capítulo 4: Conclusiones y Recomendaciones
-Conclusiones
-Recomendaciones
-Bibliografía

Cronograma:

Objetivo Específico	Actividad	Resultado esperado	Tiempo (semanas)
Explicar que es una DLP y sus principales funcionalidades	• Recolección de información.	**Reunir una gran cantidad de información, sean estas de artículos, revistas, libros, sitios web, etc.**	1
Proponer una guía estándar de implementación de DLP, que pueda ser acogida por cualquier empresa.	• Revisar recolectar y analizar información sobre DLP y de su implementación.	**Procesar la información con guía del director de tesis, para que este enfocada a nuestro proyecto. Y de esta manera proponer una guía estándar de implementación que pueda ser de utilidad a cualquier empresa.**	3

Realizar una prueba de concepto, con la aplicación DLP "OpenDLP".Analizar una aplicación DLP específica para realizar un demo demostrativo de este.	• Generar y Preparar Demo demostrativo que forme parte del proyecto	**Presentar un ejemplo de una aplicación DLP.**	4
Conclusiones y recomendaciones	• Documentación de Conclusiones y futuras recomendaciones para implementar una DLP.	**Presentar conclusiones que se han desarrollado a lo largo del desarrollo del proyecto.**	2
	• Revisión final. • Empastado. • Presentación.	**Revisión, sugerencias del director de la tesis y posteriormente del tribunal.** **Empastado o anillado de la documentación del proyecto.** **Explosión del proyecto.**	2

Referencias

AVELLANEDA, J. C. (25 de Junio de 2008). *http://seguridad-de-la-informacion.blogspot.com/*. Obtenido de http://seguridad-de-la-informacion.blogspot.com/2008/06/tecnologa-dlp.html

Booth, N. (09 de Diciembre de 2013). *Searchdatacenter*. Obtenido de http://searchdatacenter.techtarget.com/es/opinion/Como-mantener-la-confidencialidad-en-la-nube

Cano, F. (10 de Marzo de 2011). *Seinhe*. Obtenido de http://www.seinhe.com/blog/14-introduccion-a-la-tecnologia-data-loss-prevention-dlp

Costales, J. R. (18 de Octubre de 2011). *Canal Tecnologico*. Obtenido de http://www.canal-tecnologico.com/index.php?option=com_content&view=article&id=1219:la-fuga-de-informacion-un-problema-tecnologico-y-humano&catid=25&Itemid=123

Cruz, A. d. (19 de Octubre de 2011). *Symantec Corporation* . Obtenido de http://www.symantec.com/es/es/about/news/release/article.jsp?prid=20111019_01

Diario, E. (28 de Marzo de 2013). *El Diario*. Obtenido de http://www.eldiario.ec/noticias-manabi-ecuador/257319-denuncian-fuga-de-informacion-en-la-fiscalia-de-chone/

Editor. (23 de Diciembre de 2010). *Eset*. Obtenido de http://www.welivesecurity.com/la-es/2010/12/23/sobre-la-fuga-de-informacion/

Mogull, R. (13 de Diciembre de 2013). *Searchdatacenter*. Obtenido de http://searchdatacenter.techtarget.com/es/consejo/Como-evitar-errores-de-implementacion-de-DLP

Telecinco. (13 de 03 de 2014). *Telecinco*. Obtenido de http://www.telecinco.es/informativos/internacional/Intento-fuga-frustrado-Penitenciaria-Nacional_0_1762950670.html

Tiempo, E. (01 de Febreo de 2013). *El tiempo*. Obtenido de http://www.eltiempo.com.ec/noticias-cuenca/112851-robo-de-informacion-se-registro-en-2012/

Torres, A. (16 de Enero de 2012). *El Comercio*. Obtenido de http://www.elcomercio.com.ec/seguridad/Fuga-datos-secretos-UAF-impune_0_628137278.html

Firma de responsabilidad

Moisés Rendón Terreros
0105947824

Firma de responsabilidad

Ing. Fernando Aguilar Ochoa
Director Sugerido

Fecha de entrega: 11 de junio de 2014