UNIVERSIDAD INTERNACIONAL SEK

DIGITAL SCHOOL

Trabajo de fin de carrera titulado:

“PROPUESTA DE UN MODELO DE SEGURIDAD PARA LA PREVENCIÓN DE PÉRDIDA DE INFORMACIÓN SENSIBLE DIRIGIDO A LA ASAMBLEA NACIONAL”

Realizado por:

Edwar Rodolfo Chalá Ibarra

Director del proyecto:

Ing. Luis Fabián Hurtado, MGS

Como requisito para la obtención del título de Master en Ciberseguridad

Quito, septiembre de 2020

DECLARACIÓN JURAMENTADA

Yo, EDWAR RODOLFO CHALÁ IBARRA, con cédula de identidad 040165163-3, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

_____

EDWAR RODOLFO CHALÁ IBARRA

DECLARACIÓN DEL DIRECTOR DE TESIS

Declaro que el presente trabajo de investigación titulado:

"PROPUESTA DE UN MODELO DE SEGURIDAD PARA LA PREVENCIÓN DE PÉRDIDA DE INFORMACIÓN SENSIBLE DIRIGIDO A LA ASAMBLEA NACIONAL"

Realizado por:

EDWAR RODOLFO CHALÁ IBARRA

Como requisito para la obtención del Título de

MASTER EN CIBERSEGURIDAD

Ha sido dirigido por mi persona a través de reuniones periódicas con el estudiante y cumple con todas las disposiciones que rigen los trabajos de titulación.

_____

Ing. Luis Fabián Hurtado, MGS

DIRECTOR DEL PROYECTO

LOS PROFESORES INFORMANTES

Los profesores informantes:

Diego Riofrío Luzcando.

José Freire Rumazo.

Después de revisar el trabajo han calificado como apto para su defensa oral ante el tribunal examinador

_____ _____

Ing. Diego Riofrío Luzcando, PhD Ing. José Freire Rumazo, Msc.

Quito, septiembre de 2020

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.

EDWAR RODOLFO CHALÁ IBARRA

CI: 040165163-3

DEDICATORIA

A Dios, por permitirme llegar a este momento tan especial en mi vida. Por los triunfos y los momentos difíciles que me han enseñado a valorarlo cada día más, A mi madre María por ser la persona que me ha acompañado durante todo mi trayecto estudiantil y de vida, a mi padre Pedro quien con sus consejos ha sabido guiarme para culminar mi carrera profesional. A mis hijos Alessandro, Alejandra y Sherlyn que han sido los que me motivan y me dan fuerzas para superarme y salir adelante. También a mis hermanos, amigos y familiares, que hasta hoy seguimos siendo amigos. A mis profesores, gracias por su tiempo y dedicación, por transmitir ese conocimiento en las aulas.

AGRADECIMIENTO

En primer lugar, doy infinitamente gracias a Dios, por haberme dado fuerza y valor para culminar esta etapa de mi vida.

Agradezco especialmente a mis familiares y amigos quienes con su ayuda, cariño y comprensión han sido parte fundamental de mi vida.

Agradezco la confianza y el apoyo brindado por parte de mi madre María Ibarra, que sin duda alguna en todo este trayecto ha demostrado su amor y celebrando mis triunfos.

A mi padre Pedro Chalá, quien siempre está presente en el transcurso de mi vida y sé que está orgulloso de la persona en la cual me he convertido.

A mis hermanos por su apoyo y consejos, y por los buenos tiempos que hemos vivido, que siempre estarán en mis pensamientos.

Como olvidarme de la institución que me abrió las puertas a la educación superior la Universidad Internacional SEK.

En general a todas aquellas personas que, de una u otra forma, colaboraron o participaron en mi formación como profesional, hago extensivo mi más sincero agradecimiento.

RESUMEN

El presente trabajo de investigación propone la implementación de un DLP (Data Loss Prevention - Prevención de fuga de datos) por sus siglas en inglés, bajo la licencia GNU/Linux, el cual previene la fuga de información en la Asamblea Nacional, siendo uno de los recursos más importantes a nivel personal e institucional.

Las herramientas DLP han sido consideradas como una solución para incidentes de fuga de datos, estas herramientas están basadas en buenas prácticas y normas internacionales; la implementación del DLP utiliza métodos científicos y además está relacionada en su diseño a fin de dar cumplimiento a las leyes ecuatorianas, entre ella se puede mencionar: Código Orgánico Intregal Penal, Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Ley Orgánica de Telecomunicaciones entre otras, haciendo referencia a la privacidad de los datos en el Ecuador.

En este documento se explica qué es una solución DLP y de igual manera se propone un método de implementación dirigido a la Asamblea Nacional para que ayude a prevenir la pérdida de datos dentro de la misma. Este trabajo consta de cinco capítulos, donde se explica detalladamente el método a seguir para aplicar la solución DLP open source como lo son MyDLP y Opendlp.

Palabras Clave: DLP, Fuga de Información, Mydlp, Opendlp, fuga de datos.

ABSTRACT

This research work proposes the implementation of a DLP (Data Loss Prevention - Data Leak Prevention), under the GNU / Linux license, which prevents the leak of information in the National Assembly, being one of the most important personal and institutional resources.

DLP tools have been a solution for this type of data leakage incidents that are based on good practices and international standards, the implementation of this DLP technology uses scientific methods and is also related to Ecuadorian laws, including: Organic Integral Criminal Code, Electronic Commerce Law, Electronic Signatures and Data Messages, Organic Telecommunications Law, among others, referring to data privacy in Ecuador.

This document explains what a DLP solution is and also proposes an implementation method aimed at the National Assembly to help prevent data loss from it. This work consists of five chapters, where the method to follow to apply the open source DLP solution is explicitly explained, such as MyDLP and Opendlp.

Keywords: DLP, Information Leak, Mydlp, Opendlp, Data Leaks

ÍNDICE DE CONTENIDOS

RESUMEN ..... *vii*

ABSTRACT ..... *viii*

CAPÍTULO I *1*

El Problema de Investigación *1*

1.1. Planteamiento del Problema 1

1.2. Formulación del problema 2

1.3. Objetivo General 2

1.4. Objetivos Específicos 3

1.5. Justificaciones 3

1.6. Estado del Arte 4

CAPITULO II *8*

MARCO TEÓRICO 8

2.1. Seguridad informática 8

2.2. Tipos de seguridad 8

2.3. Seguridad Lógica 9

2.4. Seguridad de la información 9

2.5. Activo de Información 11

2.6. Prevención de fuga de información 11

2.7. Amenazas 12

2.8. Vulnerabilidades....13
2.9. Riesgo....13
2.10. Riesgo en la seguridad de la información....14
2.11. Políticas de Seguridad de la Información....14
2.12. Data Loss Prevention (DLP)....14
2.13. Características de DLP....16
2.14. Funciones de un DLP....17
2.15. Tipos de DLP....18
2.16. MyDLP....19
2.17. Opendlp....19
CAPÍTULO III....*21*
ANÁLISIS SITUACIONAL....21
3.1. Asamblea Nacional....21
3.2. Generalidades....21
3.3. Normativa Legal....22
3.4. Pérdida de datos....24
3.4.1. Ataque interno....25
3.4.2. Ataque externo....25
3.4.3. Pérdida accidental de los datos....25
3.5. Análisis y diseño del servidor....26
3.6. Resultados y discusión....27

CAPÍTULO IV *33*

PROPUESTA 33

4.1. Objetivo de la propuesta de implementación 33

4.2. Diseño de las políticas de seguridad 34

4.3. Reglas generales para la implementación en el DLP 35

4.4. Comparativa de herramientas DLP 37

4.5. MyDLP Appliance 41

4.5.1. Componentes de MyDLP 42

4.5.2. Requisitos de instalación 42

4.5.3. Tipos de implementación de MyDLP 42

4.6. Pruebas de concepto 49

CAPÍTULO V *55*

CONCLUSIONES Y TRABAJOS FUTUROS 55

5.1. Conclusiones 55

5.2. Trabajos futuros 56

BIBLIOGRAFÍA *58*

ANEXO 1 ..... *61*

ANEXO 2 ..... *62*

ÍNDICE DE FIGURAS

Figura 1: Triada de la seguridad de la información 10

Figura 2: Arquitectura DLP 15

Figura 3: DLP Implementación 16

Figura 4: Datos en movimiento 17

Figura 5: Datos en reposo 18

Figura 6: Diseño de arquitectura 27

Figura 7: Uso de correos institucionales 28

Figura 8: Almacenamiento de Información 30

Figura 9: Fuga de información 30

Figura 10: Traslado y almacenamiento 31

Figura 11: Políticas de trabajo 32

Figura 12:Diseño de políticas 35

Figura 13: Magic Quadrant 38

Figura 14: Tipos de implementación 43

Figura 20: Configuración proxy 45

Figura 21: Inicio de sesión en MyDLP 46

Figura 22: Instalación de Endpoint 47

Figura 23: Estructura de reglas 47

Figura 24: Crear regla de política para la web 49

Figura 25: Validación de regla contraseñas 52

Figura 26: Validación de la regla de traslado de información 53

Figura 27: Log de la herramienta 54

ÍNDICE DE TABLAS

Tabla 1: Población y muestra.....27

Tabla 2: DLP líderes a nivel mundial.....38

Tabla 3: Comparativa de herramientas DLP.....40

Tabla 4: Requerimientos de Sistema.....42

Tabla 5: Test de funcionalidad de canales de datos.....50

Tabla 6: Test de funcionalidad en sistemas operativos.....51

CAPÍTULO I

El Problema de Investigación

1.1. Planteamiento del Problema

La fuga de información privilegiada en el Ecuador es un hecho que se viene evidenciando desde años atrás. Como ejemplo de esta situación, se puede mencionar a uno de los casos más recientes que fue de conocimiento general: la filtración de datos de todos y cada uno de los ecuatorianos, los cuales se encontraban bajo la custodia del Registro Civil del Ecuador; en sus sistemas de información. Esta situación en particular va de la mano con lo dicho por Rendón (2014), en un estudio realizado en Colombia, quien señala que algunas instituciones no conocen cómo deben proteger los datos que manejan y la importancia que estos poseen. El autor llega a decir que dichas organizaciones no cuentan con métodos para manejar la información que poseen, ni buenas prácticas de seguridad, desencadenando un riesgo latente y como consecuencia la pérdida de información. En otras palabras, las instituciones no cuentan con políticas de seguridad que eviten convertirse en potenciales víctimas de fugas de información.

La pérdida de información confidencial es uno de los problemas más críticos que enfrenta toda institución, dichos datos son considerados como un activo muy valioso, el cual está propenso a ser filtrados por medio de correos electrónicos, mensajería instantánea, impresión o copia en dispositivos de almacenamiento (Rendón, 2014).

Este trabajo se desarrollará en la Asamblea Nacional, en cuya entidad se ha observado de manera directa e indirecta algunos inconvenientes relacionados al manejo de información. Entre los más preocupantes se puede mencionar: ataques de intrusos internos y externos, algunos funcionarios de la Asamblea utilizan los correos institucionales para fines personales

ajenos a lo laboral, las computadoras y portátiles (personales) no poseen controles basados en políticas de uso y son propensos a ser infectadas, no hay un control en la red de los equipos pertenecientes a los usuarios quienes no actualizan sus contraseñas en los tiempos establecidos, los usuarios no hacen uso del bloqueo de pantalla en sus respectivos equipos, significando esto que cualquier persona puede utilizar esos equipos y sustraer información. Actualmente, la Asamblea Nacional no cuenta con un mecanismo dedicado para el control, prevención y detección de fuga de información que asegure la confidencialidad y privacidad de la información (López, 2019).

Si se logra controlar los riesgos con mayor probabilidad de ocurrencia en la institución, se puede reconocer, analizar y responder a un incidente con mayor rapidez, esto va a limitar un daño potencial, de modo que se puedan minimizar los costos de reparación. Por lo tanto, con un método que logre proteger la información generada en la organización va a garantizar el correcto funcionamiento de la misma .

1.2. Formulación del problema

La Asamblea Nacional realiza procesos críticos y manejo de grandes volúmenes de datos sin un control adecuado de la información, lo que ha generado una serie de problemas en la gestión de la información sensible, lo cual compromete los principios de integridad, disponibilidad y confiabilidad de la información.

1.3. Objetivo General

Plantear un modelo de seguridad de la información basado en un DLP para la prevención de fuga de información dirigido a la Asamblea Nacional, que servirá como guía en la protección de los datos.

1.4. Objetivos Específicos

- Determinar las políticas de seguridad de la información que sean necesarias para la Asamblea Nacional mediante un estudio de las tecnologías que ayude a la prevención de fuga de información.
- Comparar las diversas herramientas de DLP aplicadas a la protección de pérdida de información para su futura implementación en la Asamblea Nacional.
- Recomendar mejores prácticas administrativas para la seguridad informática en la prevención de incidentes de fuga de información definiendo controles específicos.

1.5. Justificaciones

La información se ha convertido en uno de los recursos más importantes a nivel personal como a nivel institucional, la Asamblea Nacional como toda institución del Estado está obligada a implementar estándares y normas nacionales en mención de seguridad informática. En esta entidad estatal trabajan alrededor de 1.256 funcionarios y consta de varios departamentos, una gran cantidad de ellos desconocen de conceptos y mejores prácticas relacionadas a la seguridad de la información, he ahí donde algunas personas toman ventaja de este tipo de usuarios y las vulnerabilidades asociadas, para sustraer información que está bajo su responsabilidad.

La gestión de las redes de comunicación de la Asamblea Nacional debe cumplir con ciertas normas y una de ellas es el Esquema Gubernamental de la Seguridad de la Información (EGSI V2), que inicialmente fueron elaboradas para precautelar y cubrir este tipo de instituciones. Sin embargo, no existe un efectivo control e implementación de prevención de incidentes de fuga de la información.

El presente trabajo busca proponer la implementación de un sistema DLP, el cual permite la identificación, registro, categorización, priorización y solución a los eventos e incidentes de fuga de información. Dicho método tendrá un control total del flujo de información,

optimizando los procesos de seguridad de los activos de informacion de la Asamblea Nacional.

1.6. Estado del Arte

Hoy en día la sociedad pasa conectada a través de la red de Internet, en la cual existen amenazas contra sus usuarios, lo cual los convierte en objetivos de ataques. En el Ecuador se han visto múltiples incidentes a infraestructuras tecnológicas que han ocasionado problemas a su imagen o en el peor de los casos han generado considerables pérdidas económicas. En el 2019 a raíz de la salida de Julián Assange de la Embajada de Ecuador en Londres, el país sufrió una serie de ataques a instituciones del Estado como son el Servicios de Rentas Internas (SRI), Municipios y Cancillería. El Registro Civil del Ecuador también sufrió ataques no relacionados específicamente con lo sucedido con Julian Assange, pero este incidente, fue de controversia internacional debido a la magnitud de los sucedido; principalmente por que se filtraron los datos de ciudadanos ecuatorianos, lo que suponía información privada de prácticamente todo el país (VpnMentor, 2019).

Según Almeida & Herrera (2019) en su artículo "La ciberseguridad en el Ecuador, una propuesta de organización", mencionan que el uso de las tecnologías de la información es fundamental en todas las actividades que realizan los países y la sociedad en general. Esto ocasiona dependencia al Internet, lo que a su vez constituye una puerta para que se produzcan delitos ciberneticos. En este nuevo escenario no existen fronteras, actores, ni límites y estas nuevas amenazas pueden afectar la seguridad de una institución, organización o personas en general. Así, surge la necesidad de fomentar e implementar políticas y estrategias de protección de la información, por lo que el entorno digital en el que se desarrolla el mundo actual debe considerar los riesgos que se presentan en el uso del Internet y la información que ahí se genera.

León (2015), cita el estudio “Magic Quadrant for Content-Aware Data Loss Prevention” realizado por la consultora Gartner, en el año 2014. En este se indica que más del 50% de las empresas utilizó alguna característica en sus políticas de seguridad para la prevención de fuga de información (DLP) en sus datos, en conclusión, sólo el 30% de éstas dispuso de una herramienta o estrategia como es DLP.

Todas las herramientas DLP deben tener la funcionalidad de proteger de manera completa la información en reposo, en uso y en movimiento; las tecnologías esta en constante evolución y, en efecto, también la forma de protegerse en el mundo digital. El método a implementar es la herramienta DLP está se basa en su ciclo de vida de seis pasos que son aplicables a la organización: descubrir y aprender; evaluar el riesgo; afinamiento de políticas; aplicar controles; monitorizar y; aplicar; evaluar y prevenir. Con el cumplimiento de cada uno de los pasos del ciclo de vida se logrará tener más seguridad en el ámbito de la información en las empresas (León, 2015).

Hauer (2015), sostiene que existen cierto tipo de infracciones de datos que no son necesariamente intencionales; pueden darse por errores de los usuarios o por situaciones que se salen del control de todos. No obstante, siguen significando filtraciones de información privilegiada. Con el fin de obtener un mayor conocimiento sobre las violaciones reportadas por Digital Guardian (2015), se proponen criterios avanzados para organizar incidentes de fuga de datos. Se caracterizan a los ataques según su relevancia, así, se pueden establecer los instrumentos útiles para indicar la importancia de las medidas exitosas de Sistema de Información (SI) y revelar debilidades. El análisis de los incidentes de fuga de datos basados en estos criterios avanzados ilustra que el factor humano es clave y decisivo dentro del alcance del SI. Las organizaciones confían en la aceptación y la cooperación de sus empleados porque no existe un método infalible para evitar fugas.

Hauer (2015) señala que esto se debe al hecho de que estas soluciones dependen de ciertos volúmenes de la seguridad de la información que se establecerán en la reducción del riesgo de violaciones de datos basados en la tecnología. Por lo tanto, este trabajo introduce un concepto coherente que consta de varios elementos para establecer DLP e ILP dentro del alcance de seguridad de la Información.

Según Purohit & Singh (2013) mencionan que:

> *Se puede equilibrar la seguridad de los datos y la comodidad del usuario. También se puede sugerir la forma de prevenirlo apostando por la tecnología DLP. Se ha demostrado los detalles de implementación de esta tecnología como parte del experimento. Sin embargo, es mucho más fácil implementar la tecnología DLP que tratará la seguridad de la nube.*
>
> *La pérdida de datos se ha convertido en el mayor inconveniente en las organizaciones actuales, donde estas tienen la responsabilidad de superar este problema. Se produce un incidente de seguridad cuando la confidencialidad de la información se ha visto comprometida. Se refiere a una transmisión no autorizada de datos dentro de una organización a un destino externo (p.3).*

Por su parte, López, Richardson, & Carvajal (2015) argumentan lo siguiente:

> *Con el pasar del tiempo la fuga de información se agrava cada vez más y las industrias pierden uno de los activos más importantes de hoy en día los datos. La pregunta es: ¿Las compañías deben confiar al 100% en sus empleados?, sin establecer políticas de seguridad de datos o usar herramientas que protejan los datos de posibles fugas de información ya sea relevante o no, en el mundo real todo es diferente, los funcionarios cometen errores (p.2).*

En consecuencia, López, et.al (2015) consideraron que la fuga de datos es un problema visible y se debe investigar algún tipo de tecnología para la prevención de pérdida de datos (DLP), esto ayudará a las organizaciones a aumentar el cumplimiento de las políticas de seguridad de la información y mantener la seguridad de sus datos de empleados o del personal mal intencionado que desea sustraer la información de la organización.

En el caso de Ecuador, el cual compete a este trabajo de investigación, los DLP están basados en los criterios de la información confidencial. En Ecuador no existe específicamente una ley de protección de datos, la única guía significativa sobre el tema en la ley ecuatoriana, es el artículo 66 de la Constitución de la República del Ecuador. Este artículo garantiza que las personas tengan derecho a que sus datos personales se protejan, refiriéndose al derecho a decidir con quién comparten su información y cómo esta puede ser utilizada.

En este trabajo se propone la posibilidad de probar la metodología contra software de código libre y el software comercial para analizar si el método a implementar y la tecnología DLP, son efectivos en el funcionamiento de la organización. Esto con la finalidad de precautelar su activo más importante, que es la información generada dentro de la institución; por lo que se utilizará la tecnología DLP con el fin de dar a conocer el potencial de esta solución e implementar en la Asamblea Nacional del Ecuador, se lo hará entre otros puntos, como señalan López et al. (2015).

CAPITULO II

MARCO TEÓRICO

2.1. Seguridad informática

La seguridad informática se encarga de salvaguardar los recursos informáticos, según varios autores esta disciplina obedece a elaborar técnicas, métodos, procedimientos y normas para hacer de un sistema de información robusto, seguro y confiable (López, 2010). Vieites (2011), afirma que principalmente este tipo de sistemas se basan en nuevas tecnologías, por tanto, la seguridad informática protegerá los datos que están disponibles en el sistema, de tal manera que sólo tendrán acceso usuarios autorizados.

Los objetivos de la seguridad informática son:

- Proteger los activos de información mediante los principios de seguridad.
- Administrar los posibles riesgos para mantenerlos en niveles aceptables.
- Concientizar y capacitar al personal que esté involucrado con la institución a fin de salvaguardar los activos de información que están en su poder.
- La alta gerencia se encarga de limitar y monitorear mediante el uso de herramientas, además de planificar las auditorías internas.
- Cumplir con la normativa legal estipulada e implementar acciones correctivas y mejoras en la seguridad de la información.

2.2. Tipos de seguridad

López (2010), menciona que: *lo que no está permitido debe de ser prohibido* (p.9), para ello se debe realizar periódicamente, revisiones y actualizaciones de las medidas de seguridad informática y estas constan de dos tipos:

- **Activa. -** Conjunto de herramientas o medidas que su objetivo principal es evitar o reducir que se produzca un riesgo que amenace al sistema.
- **Pasiva. -** Este tipo de seguridad está destinada a minimizar su repercusión y facilitar la recuperación inmediata del sistema.

2.3. Seguridad Lógica

Son los mecanismos y las herramientas que ayudan a la seguridad lógica y tienen como objetivo principal proteger digitalmente la información de forma directa. Cabe indicar que para subsanar la seguridad lógica se puede implementar una serie de conjuntos de soluciones y métodos que ayudan a los administradores y funcionarios que están a cargo de la seguridad de las organizaciones (López, 2010).

2.4. Seguridad de la información

Bertolín (2008) menciona que la seguridad de la información es una ciencia en continua evolución. La información es la parte más relevante de las organizaciones. La meta de la seguridad permite que una organización cumpla con todo su objetivo, implementando sistemas que tengan prevención de riesgos relacionados con la TIC, los objetivos de la seguridad de la información son:

Figura 1: Triada de la seguridad de la información
Fuente: Bertolin (2008)

- **Accesibilidad y Disponibilidad.** Este sería un requisito indispensable para garantizar la seguridad de la información y la protección de los sistemas.
- **Integridad.** Garantiza que la información no sea modificada o adulterada por personas sin autorización, además de la integridad de los datos y los sistemas.
- **Confidencialidad de la información.** Asegurar la confidencialidad de los datos almacenados mientras se transmiten. Para algunos sistemas con generadores de códigos de verificación de dos pasos es clave mantener la confidencialidad.
- **Responsabilidad**. Es un requisito de política para las instituciones y soporta directamente el no repudio, la disuasión, aislamiento de fallo, prevención y detección de intrusiones y acción de recuperación.
- **Confiabilidad**. Garantiza que los cuatro objetivos anteriores se cumplan con total normalidad, asegurando las medidas operacionales, técnicas y funcional de los sistemas.

Para que funcione un sistema perfectamente debe cumplir al menos cuatro de estos objetivos, la confianza es fundamental para que los mecanismos de seguridad cumplan el rol establecido en los sistemas.

2.5. Activo de Información

Asegurar los activos es fundamental para precautelar la confiabilidad, disponibilidad e integridad, la información relevante de los activos pueden ser de aspectos físicos (bases de datos, archivos e impresos), de aspectos técnicos (servidores y equipos informáticos), de aspectos financieros (voucher, estados de cuentas) y aspectos de desempeño (Sola & Crespo, 2016).

Hay que diseñar y asegurar controles que protejan adecuadamente estos activos por su valiosa información o contribución para la continuidad del negocio y proporcionen confidencialidad a las instituciones (Piattini Velthuis, 2015).

2.6. Prevención de fuga de información

León (2015) señala que la herramienta de prevención de fuga de información DLP, nos permite el control de información confidencial mediante la auditoría y bloqueo de dicha información ya que es susceptible en aplicaciones, en dispositivos físicos y protocolos de red.

El método que se recomienda para implementar la solucion DLP se basa en 6 pasos que son:

- **Descubrir y Aprender:** En esta etapa se efectúa el monitoreo de la información asociada con los diferentes departamentos.
- **Evaluar el Riesgo:** La evaluación está vinculada a los datos de los perfiles asociados a la herramienta.
- **Afinamiento de Política**: La personalización de políticas a base de DLP con información examinada por parte de los usuarios.

- **Aplicar Controles**: La creación de grupos de usuarios a los cuales se aplicarán las políticas, asociación de las diferentes políticas a los grupos de usuarios y replicación de la política definida para las diferentes jefaturas en ambiente de producción.
- **Monitorear, Reportar y Evaluar**: Monitorización de los diferentes eventos asociados por la herramienta en el Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés) y la evaluación de los resultados de áreas o procesos implicados y delimitando los planes de ejecución.
- **Prevenir:** Implementar medidas de prevención para los departamentos definidos en los planes de mitigación.

2.7. Amenazas

Se entiende por amenaza a la presencia de factores que pueden aprovechar las vulnerabilidades que se presentan ya sea un sistema de información, personas o procesos. Hay diferentes tipos de amenazas de las que se debe proteger los sistemas como son: fallas eléctricas, fallos de software, errores intencionados y fallas humanas. Las amenazas se clasifican en: Interrupción, interceptación, modificación, fabricación, accidentales e intencionados (López, 2010).

Las amenazas están relacionadas con el peligro de que se materialicen y estas pueden ser de procedencia natural, tecnológico o error humano, por ende, puede manifestarse en un lugar y momento específico. Técnicamente, se manifiesta como la probabilidad de rebasar el nivel de ocurrencia de un evento con un nivel de severidad en un lugar específico y durante un período de tiempo (Cardona, 1993).

2.8. Vulnerabilidades

López (2010) dice que las vulnerabilidades son una debilidad de un software o hardware, resultado probable de ocurrencia que una amenaza se materialice en contra de los equipos informáticos. No todos los sistemas o equipos informáticos son vulnerables. Al realizar un análisis de riesgos se debe tener en cuenta la vulnerabilidad de cada uno de ellos, estas fragilidades son aprovechadas por los atacantes para realizar su cometido y explotarlas.

Solarte y Benavides (2015), indican que las vulnerabilidades son cualquier evento, independientemente del tipo de origen que pueda afectar a los activos, datos o información sensible ante un eventual ataque, por parte de usuarios internos o externos a una organización.

Las diferentes vulnerabilidades que pueden asociarse al nivel informático son: vulnerabilidad en la gestión de los recursos, vulnerabilidad de directorio, vulnerabilidades del hardware, vulnerabilidades del software o de configuración, vulnerabilidad en privilegios y control de acceso, vulnerabilidad humana y vulnerabilidad en las comunicaciones.

2.9. Riesgo

El riesgo es el resultado del análisis de las vulnerabilidades y amenazas de que se materialicen y estos suelen categorizarse por su impacto bajo, medio y alto, y por su clasificación pueden ser: de integridad, de relación, de acceso, de utilidad e infraestructura. (Sánchez & Ignoto, 1991).

Solarte y Benavides (2015) mencionan que son un problema potencial, estos pueden afectar a los sistemas de información. Si estos no cuentan con medidas adecuadas para proteger los datos y la información, potencialmente se convierte en un problema latente, dichos riesgos dejan en evidencia las posibles amenazas y vulnerabilidades en cualquier momento.

2.10. Riesgo en la seguridad de la información

Riesgo latente de que una amenaza tome ventaja y explote ciertas vulnerabilidades que se evidencie en los activos de información de una entidad u organización (Castrillón & Lezcano, 2013).

2.11. Políticas de Seguridad de la Información

Las políticas de seguridad de la información son las disposiciones de alto nivel que determinan el nivel de seguridad a implementar dependiendo de las necesidades. Esto lineamientos delimitan las responsabilidades de las interpretaciones técnicas y organizacionales que se requieren en un sistema u otro (Vieites, 2011)..

Sin políticas no se distingue entre los datos confidenciales y públicos. Las políticas se basan en las especificaciones propias de cada institución, pero también de entornos que están fuera del ambiente laboral, como son los sistemas de seguridad digital o las interconexiones de componentes intermedios (Acosta, 2015).

2.12. Data Loss Prevention (DLP)

Tahboub & Saleh (2014) mencionan que es la solución para detectar una potencial brecha de la seguridad, esta se encarga de monitorear el tráfico en tiempo real y detectar la fuga de grandes volúmenes de información. El DLP es considerado una estrategia para la protección de la información, este método es utilizado en ciertos tipos de información como son la financiera, personal e institucional de carácter reservado. Exponer estos datos fuera de una institución conlleva a consecuencias perjudiciales para la misma. Las soluciones DLP se distinguen entre tres fases de datos que son: datos en reposo (DAR), datos en movimiento (DIM) y datos en uso (DIU).

El DLP es una solución para encontrar, monitorear y proteger la información confidencial que está almacenada a través de la red y los discos de almacenamiento. Las soluciones DLP se utilizan para prevenir el problema de perder los datos confidenciales.

Los componentes de la solución están diseñados de la siguiente manera:

- Detección de los datos confidenciales almacenados.
- Monitorear para que se utilizan los datos.
- Proteger los datos para evitar su pérdida.

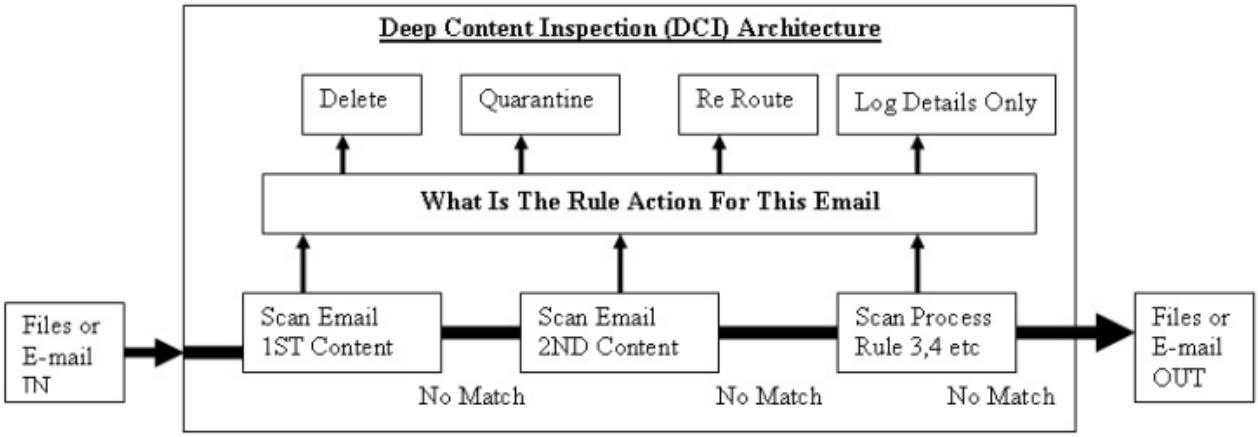


Figura 2: Arquitectura DLP
Fuente: Radwan (2015)

Se trata de un sistema con un conjunto de herramientas tecnológicas para la prevención de fugas de información, sin embargo, la pérdida de la información es una de las incidencias más comunes en materia de seguridad en las instituciones y a nivel personal (Andrade, 2015).

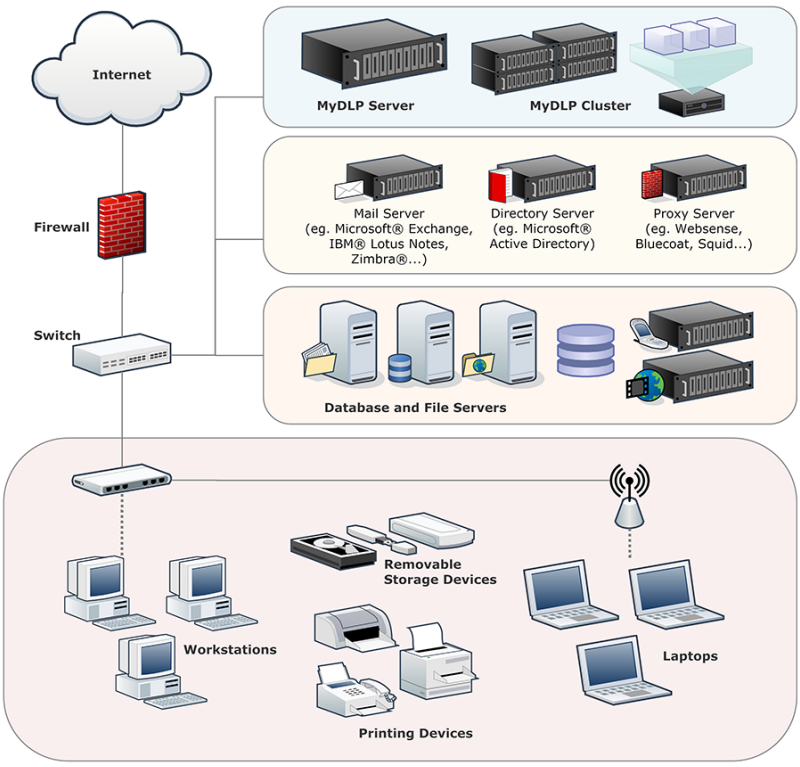


Figura 3: DLP Implementación

Fuente: Purohit & Singh (2013)

2.13. Características de DLP

Torres (2015) afirma que las soluciones DLP están orientadas al monitoreo, administración, protección y detección de la información clasificada como sensible dentro de una organización y se caracteriza por:

- Supervisar dónde y cuándo es utilizada la información considerada sensible por parte de los usuarios de la organización.
- Detectar dónde se encuentra la información sensible y genera un inventario de los datos y propietarios con el fin de administrar la información.
- Proteger la información con aplicaciones y políticas de seguridad con el fin de prevenir la fuga de dicha información.
- Administrar las políticas de pérdida de datos, identificar los incidentes de seguridad y elaborar informes por medio de la plataforma unificada.

2.14. Funciones de un DLP

Torres (2015) afirma que la principal función de un DLP es la protección de la información, la herraminta se basa en un catálogo de los procesos para examinar los datos sensibles:

- Datos en uso: Son los datos usados en tiempo real por los usuarios, estos son monitoreados revisando cada acción que realizan los usuarios finales en sus computadores para protegerlos por medio de agentes instalados en los computadores de los funcionarios. Estas aplicaciones bloquean el traslado de información.
- Datos en movimiento: Estos se trasmiten a través de una red y su protección se da en la red, analizando fragmentos en busca de patrones que verifiquen que los datos tengan autorización de su movimiento, la herramienta DLP debe ser capaz de monitorear el tráfico de forma pasiva y así determinar si los paquetes que están en la red no infringen alguna regla que esté debidamente configurada en el DLP.

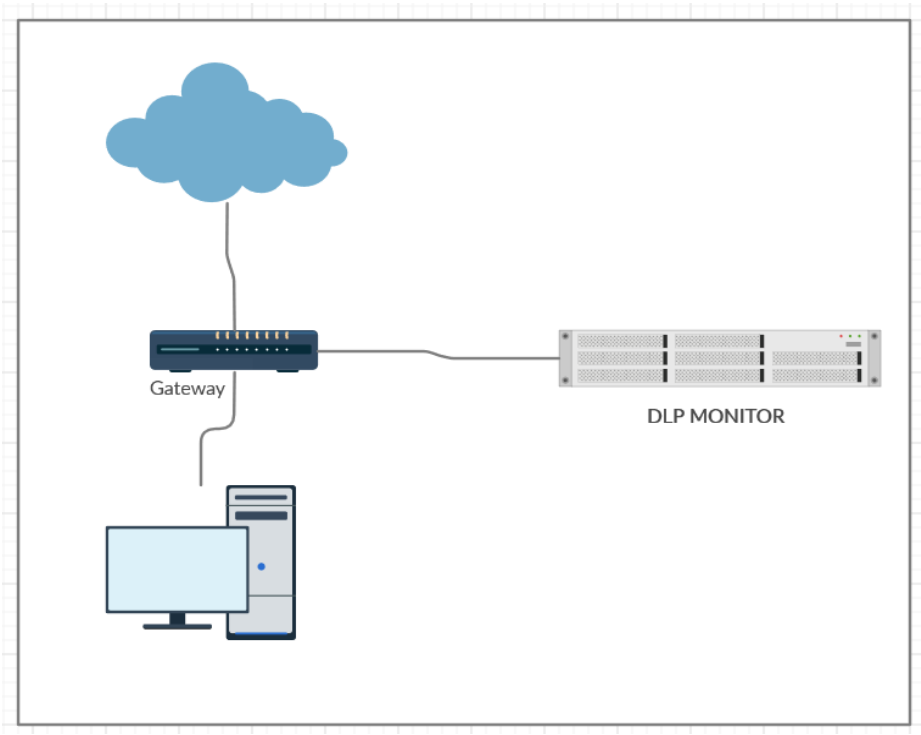


Figura 4: Datos en movimiento
Fuente: Torres (2015)

- Datos almacenados: Una funcionalidad de la herramienta DLP es la de rastrear tipos de información y localizar en dónde se almacenan en la organización. Estos se encuentran en algún medio de almacenamiento en el organismo una vez encontrados los datos, la herramienta DLP debe escanear su contenido en busca de datos sensibles para su protección.

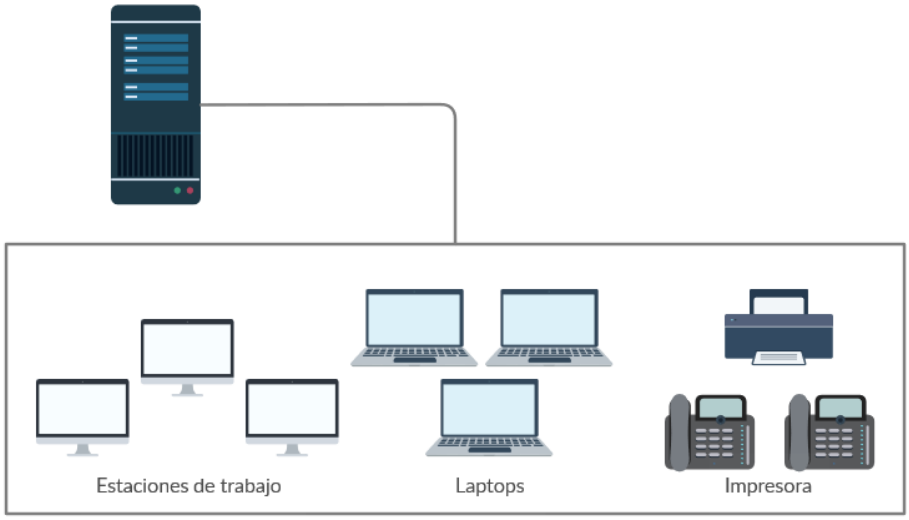


Figura 5: Datos en reposo
Fuente: Torres (2015)

2.15. Tipos de DLP

López (2015) argumenta que la tecnología DLP se centra en sus tres principales funciones y estas son: datos en reposo, en movimiento y almacenados, los datos en movimiento pueden ser filtrados por los puertos FTP, P2P, SSH, SMTP, HTTP, HTTPS, entre otros. Para contrarrestar esto se dispone dos tipos de DLP, uno es un span que estará en modo promiscuo revisando todo el tráfico de la red. La otra arquitectura que soporta un DLP es en línea, esto quiere decir que todo el tráfico que se genere dentro de la red deberá pasar físicamente por el DLP, la diferencia entre estas dos arquitecturas es que span solo puede detectar, pero no bloquear, por el contrario en línea detecta, bloquea y notifica.

Para los datos que se encuentran almacenados en los servidores y otros sistemas, siendo su contenido vulnerable debido al acceso de funcionarios y clientes, las herramientas DLP ayudarán buscando información sensible y negando el acceso al personal no autorizado.

Los datos en almacenamiento en los puntos finales siempre corresponden a los portátiles, computadores o dispositivos móviles, esta es la parte más crítica, ya que en la mayoría de los casos es donde se guarda la información, es aquí donde hay que instalar los agentes de control para hacer cumplir las políticas implementadas en el servidor DLP.

2.16. MyDLP

La aplicación open source es una multiplataforma fácil de configurar y funciona en red. MyDLP es un proyecto GNU (Código abierto) que es capaz de monitorear, inspeccionar y prevenir la fuga de información en la red. Este utiliza políticas y un gran rendimiento para los administradores de TI que a su vez pueden combatir la fuga de información (Purohit & Singh, 2013).

También, Torsteinbo (2012) manifiesta que MyDLP es open source y viene en dos versiones MyDLP Enterprise Edition y MyDLP Community esta última es la versión gratuita y viene en una imagen ISO precargada con todos las configuraciones.

2.17. Opendlp

Permite detectar y prevenir que los datos sean transferidos en la red o memoria USB, desde computadores o portátiles, definiendo políticas que deben cumplir para evitar la fuga de información (Rendón, 2014).

Raj, Cherian, & Abraham (2013) afirman que Opendlp es una suite de prevención de pérdida de datos, esta tiene una interfaz web centralizada que permite administrar los escaneos en el sistema de archivos del agente en Windows, bases de datos y sistema de archivos de Windows y UNIX, que identifican datos confidenciales en reposo. Se pueden

buscar varios elementos de texto, como las direcciones de correo electrónico y nombre de una persona utilizando expresiones regulares.

Opendlp no es capaz de identificar el texto cifrado, esto evidencia una debilidad para esta herramienta. Dado que el cifrado convierte el texto sin formato en una forma ilegible, el escaneo de expresiones regulares se vuelve inútil para este caso en particular (Silowash & King, 2013).

CAPÍTULO III

ANÁLISIS SITUACIONAL

3.1. Asamblea Nacional

En la Constitución de la República del Ecuador (2008), en el artículo 118 indica lo siguiente:

> *La Función Legislativa se ejerce por la Asamblea Nacional, que se integrará por asambleístas elegidos para un periodo de cuatro años. La Asamblea Nacional es unicameral y tendrá su sede en Quito. Excepcionalmente podrá reunirse en cualquier parte del territorio nacional. La Asamblea Nacional se integrará por: 1. Quince asambleístas elegidos en circunscripción nacional. 2. Dos asambleístas elegidos por cada provincia, y uno más por cada doscientos mil habitantes o fracción que supere los cientos cincuenta mil, de acuerdo al último censo nacional de la población. 3. La ley determinará la elección de asambleístas de regiones, de distritos metropolitanos, y de la circunscripción del exterior.(p.75)*

3.2. Generalidades

En este documento se diseñará una propuesta para implementar una solución de prevención de fuga de datos (DLP) la cual será de gran ayuda para la detección, supervisión y protección de la información sensible que está almacenada o en uso en la institución. “La herramienta propone una cobertura total para la información sensible en todo el tramo de la red y en el sistema de almacenamiento interno” (Purohit & Singh, 2013, p.3).

En el Ecuador en el Decreto Ejecutivo número 1014 de (2008), en el artículo 1 se refiere a lo siguiente: “Establecer como política pública para las entidades de la Administración Pública Central la utilización de software libre en sus sistemas y equipamientos informáticos”.

En el Decreto Ejecutivo número 1014 (2008), en el artículo 2 se refiere a lo siguiente:

> *Se entiende por software libre.- A los programas de computación que se pueden utilizar y distribuir sin restricción alguna, que permitan su acceso a los códigos fuentes y que sus aplicaciones puedan ser mejoradas. Estos programas de computación tienen las siguientes libertades: a) Utilización del programa con cualquier propósito de uso común; b) Distribución de copias sin restricción alguna; c) Estudio y modificación del programa (Requisito: código fuente disponible); y, d) Publicación del programa mejorado (Requisito: código fuente disponible).(p.3)*

3.3. Normativa Legal

La Asamblea Nacional es una entidad pública la cual está obligada a respetar, cumplir y hacer cumplir las normas establecidas, en el Código Orgánico Integral Penal COIP (Registro Oficial No. 180, 2017), en el Artículo 233 se refiere a lo siguiente:

> *Delitos contra la información pública reservada legalmente. - La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años.*

Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad.(p.37)

En la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Registro Oficial No. 557, 2002), en el Artículo 9 se refiere a la:

Protección de datos.- Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de estos, quien podrá seleccionar la información a compartirse con terceros. La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente. No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran apersonas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato. El consentimiento a que se refiere este artículo podrá ser revocado a criterio

> *del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo.(p.2)*

En la Ley Orgánica De Telecomunicaciones (Registro Oficial No. 439, 2015), en el Artículo 76 se refiere a:

> *Las medidas técnicas de seguridad e invulnerabilidad.- Las y los prestadores de servicios ya sea que usen red propia o la de un tercero, deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios y la invulnerabilidad de la red y garantizar el secreto de las comunicaciones y de la información transmitida por sus redes. Dichas medidas garantizarán un nivel de seguridad adecuado al riesgo existente. En caso de que exista un riesgo particular de violación de la seguridad de la red, el prestador de servicios de telecomunicaciones deberá informar a sus abonados, clientes o usuarios sobre dicho riesgo y, si las medidas para atenuar o eliminar ese riesgo no están bajo su control, sobre las posibles soluciones.(p.22)*

3.4. Pérdida de datos

Koutsourelis (2014) establece que el extravio de datos es un mal que aqueja a todas las instituciones, para ello hay que conocer quiénes son los más propensos a generar este tipo de incidentes, la pérdida de datos se clasifica en tres, estos son:

- Ataques Internos
- Ataques Externos
- Pérdida accidental de datos

3.4.1. Ataque interno

Acosta (2015) señala que este tipo de ataque es el más común, en lo que general casi siempre viene de un funcionario que conoce la arquitectura de red, o las vulnerabilidades de los sistemas como lo son los administradores de servicios o funcionarios expertos en este tipo de materia de seguridad, de acuerdo a datos tomados del FBI en el 2012 se refiere que los incidentes registrados en las instituciones por lo general el 80% viene de ataque internos.

La mayoría del tiempo, los trabajadores tienen acceso a distintas funcionalidades electrónicas (modificar, eliminar, leer) a ellos se suma que una gran mayoría son custodios de la información.

3.4.2. Ataque externo

Por lo general este tipo de ataque tiene por objetivo apoderase de la información que está en la institución, estos pueden ser piratas informáticos que violentando la seguridad informática de las instituciones obtienen su cometido, cuando estos logran realizar su objetivos casi siempre la recompensa es económica (Acosta, 2015).

3.4.3. Pérdida accidental de los datos

Los principales responsables de la pérdida de datos son aquellos funcionarios que desconocen las políticas de seguridad de las instituciones o hacen caso omiso de ellas. No son conscientes del valor de la información, por lo general, guardan documentos sensibles en almacenamiento remoto sin cifrado, por lo tanto, una de las fortalezas de la herramienta DLP es combatir la pérdida accidental de datos.

Si se implementan políticas sólidas se detendrá con gran facilidad las fugas accidentales de las instituciones. Una vez implementada la herramienta DLP de forma correcta se garantizará

que la información de la institución viaje por canales seguros y protegidos (Koutsourelis, 2014).

La clasificación de los datos confidenciales o sensibles deberán ser cifrados para garantizar una cultura de no datos perdidos.

3.5. Análisis y diseño del servidor

Koutsourelis (2014), asegura que:

> *El objetivo de DLP es proteger los datos durante todo el ciclo de vida ininterrumpidamente. Existen tres tipos básicos de protección en los sistemas DLP, relacionados con los estados principales de información: datos en reposo, datos en movimiento y datos en uso. Un sistema DLP completo debe combinar e implementar las tres tecnologías de protección de datos de la manera más eficiente. Los componentes básicos de un sistema DLP son: Agentes de control, son aplicaciones que se instala en la parte de los clientes o funcionarios de las instituciones y se encarga del análisis y seguimiento de los datos almacenados, el DLP de red que casi siempre está entre las redes LAN y WAN, este funciona como un proxy y monitorea todo el tráfico en la red y el servidor DLP o consola de administración central, está administra los dos componentes anteriores y es el responsable de verificar el cumplimiento de la política. La infraestructura de dicho sistema DLP se presenta en la Figura 6, donde se puede ver el tipo y componentes básicos de protección de datos de un sistema DLP (p.36).*

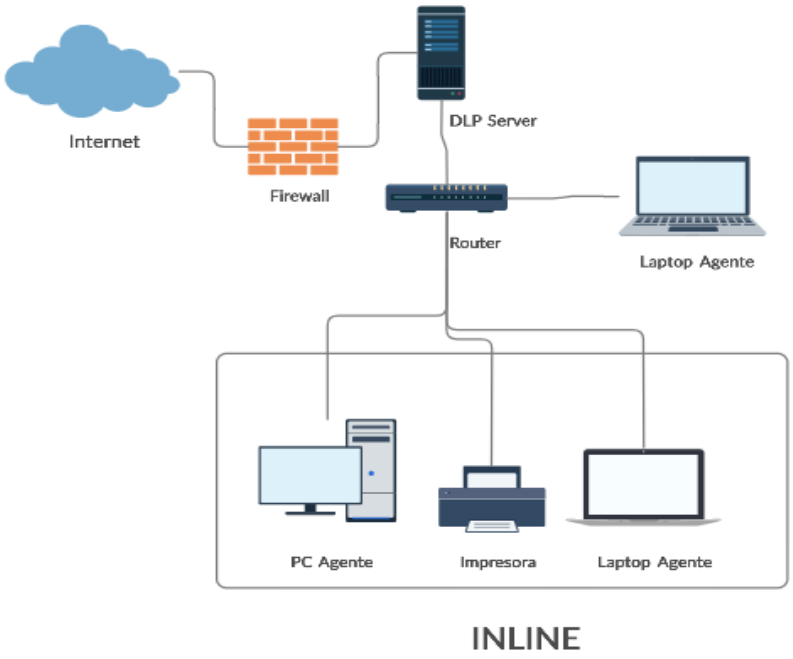


Figura 6: Diseño de arquitectura

3.6. Resultados y discusión

Entre noviembre 2019 a marzo 2020 se realizó una investigación en la Asamblea Nacional del Ecuador con un alcance a nivel nacional, esta cuenta con 1.256 funcionarios, para ello, se establecen algunas preguntas relacionadas con la fuga de información, con el fin de determinar el grado de participación y causas por los que los funcionarios incurrieron en este tipo de incidentes.

Tabla 1

Población y muestra

Detalles	Total
Funcionarios Públicos	1255
Líder de seguridad	1
Total	1256

Elaborado por: El autor de la investigación
Fuente: Asamblea Nacional (2020)

$$n = \frac{k^2 pqN}{e^2(N-1) + k^2 \text{pq}}$$

$$n = \frac{1{,}96^2 * 0{,}5 * 0{,}5 * 1256}{5^2(1256-1) + 1{,}96^2 * 0{,}5 * 0{,}5} = 294$$

N = tamaño de la población, k = nivel de confianza, p = probabilidad de éxito, o proporción esperada, q = probabilidad de fracaso y e = precisión (Error máximo admisible en términos de proporción) hay que usar cuando sea necesario y comprender bien los principios del cálculo (García, Redingl, & López, 2013).

Se realizó la muestra por que la población sobrepasa las 500 personas, por ellos, se debe aplicar la formula por la amplitud de la personal, en la Asamblea laboran 1.256 funcionarios y sobrepasa el tamaño permitido por la estadística, de este grupo de funcionarios se tomará en cuenta el margen de error de 6, una variación de 0.5 el resultado obtenido da un total de 294 funcionarios a encuestar.

Al líder de seguridad se le realizó una entrevista por el motivo de recabar información detallada de cómo se maneja internamente los procesos.

a. ¿ Utiliza frecuentemente el correo institucional?

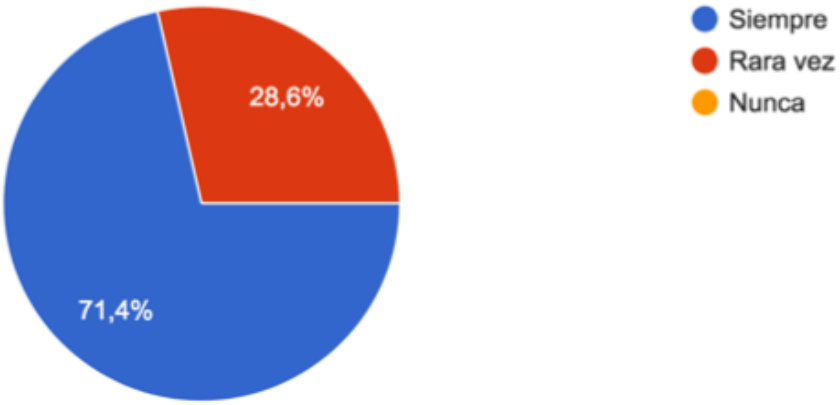


Figura 7: Gráfico de cuadro de datos
Fuente: Elaborada por autor de la investigación

En el gráfico anterior se indica que en Asamblea Nacional alrededor del 71,4% los funcionarios utilizan frecuentemente el correo institucional o corporativo, sin embargo, hay un 28,6% que no hace uso de ese correo institucional y prefiere utilizar correos tradicionales como pueden ser Gmail, Hotmail, Yahoo! entre otros.

b. ¿Donde se almacena la información generada en la institución?

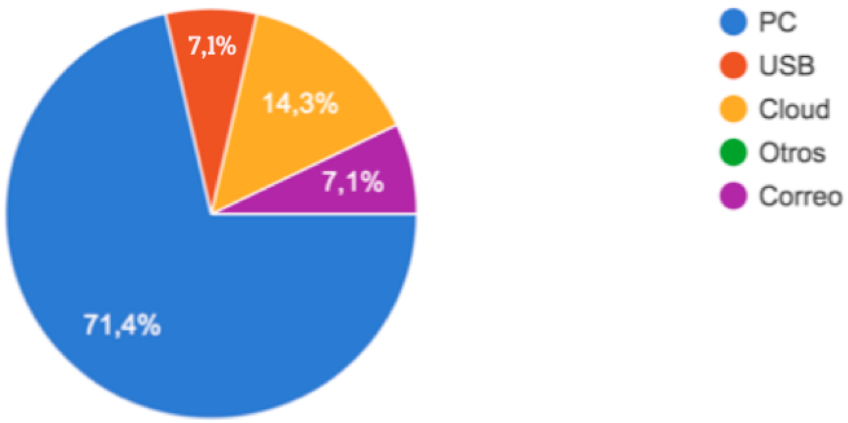


Figura 8: Almacenamiento de Información

Fuente: Elaborada por autor de la investigación

Mediante la investigación se determinó que el 71,4% de la información es almacenada en la PC asignada por la institución, mientras un 14,3% es almacenada en la nube (Cloud) y una gran minoría lo hace con el 7,1% en USB y otros medios no tradicionales.

c. ¿ Qué pasa si no termina su trabajo en la oficina, continúa en casa?

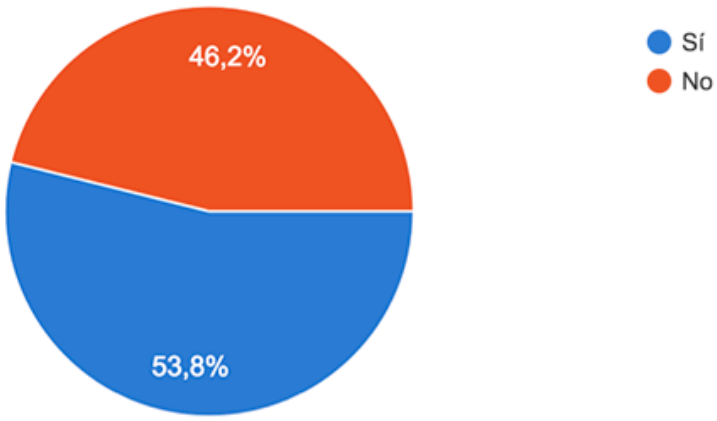


Figura 9: Fuga de información

Fuente: Elaborada por autor de la investigación

El 53,8% de los funcionarios de la Asamblea Nacional cuando no logran terminar sus tareas en los horarios de trabajo continúan en casa frente al 42,2% de los funcionarios que deja para el siguiente día. Queda en evidencia que la información es transportada y almacenada en los PC que no pertenecen a la institución donde laboran produciendo la fuga de información.

d. ¿ Qué medio electrónico utiliza para movilizar la información?

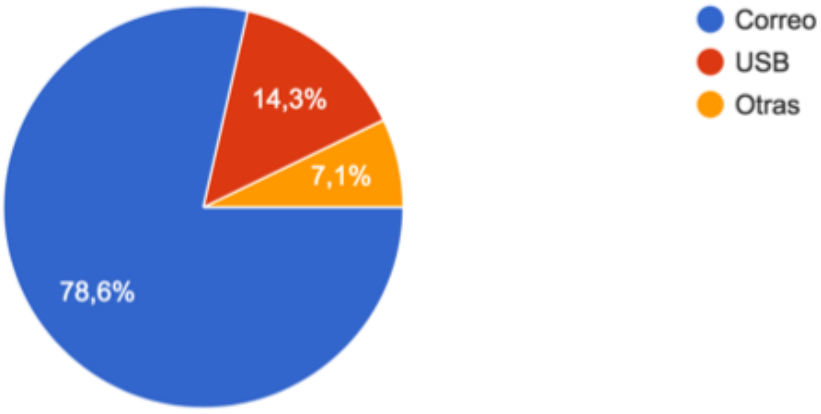


Figura 10: Traslado y almacenamiento
Fuente: Elaborada por autor de la investigación

En esta investigación también se determinó que la información que se genera en la institución es transportada mayormente en correo electrónico por un 78,6%, mientras que el 14,3% utiliza USB y un 7,1% utiliza otras opciones como medio de trasporte de la información que desean movilizar.

e. ¿ Conoce Ud. las políticas y normas de la Asamblea Nacional?

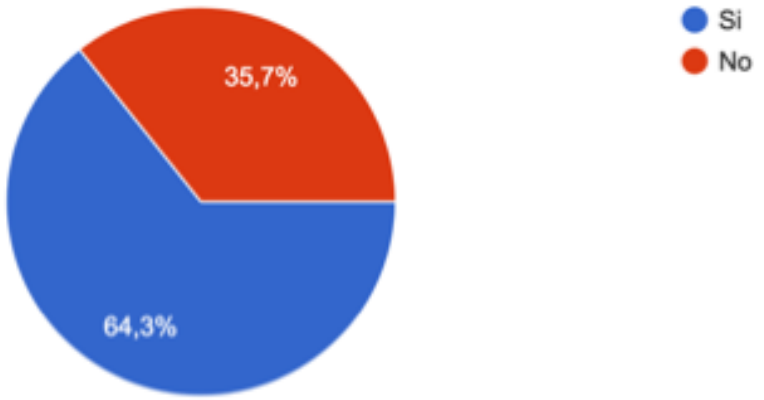


Figura 11: Políticas de trabajo
Fuente: Elaborada por autor de la investigación

En esta investigación también se determinó que el 64,3% de los funcionarios de la institución conocen las normas y políticas de la misma, mientras que el 35,7% desconocen y se genera una gran confusión a la hora de proteger la información.

Después de haber realizado las encuestas se determinó que en la institución hay un porcentaje notable de salida de información ya sea sensible o no, cabe indicar que el departamento de seguridad de la información debe clasificar la información sensible para que en el futuro la herramienta DLP realice el bloqueo de la misma.

CAPÍTULO IV

PROPUESTA DE IMPLEMENTACIÓN DE UN SISTEMA DE PREVENCIÓN DE PÉRDIDA DE DATOS.

4.1. Objetivo de la propuesta de implementación

Para la realización de este trabajo y de acuerdo a los objetivos planteados, se diseñó una propuesta para implementar una herramienta Data Loss Prevention (DLP), siendo esta un mecanismo para la detección, supervisión y protección de la información sensible donde quiera que esta se almacene o se utilice. Actualmente la Asamblea Nacional del Ecuador no cuenta con un mecanismo similar, por lo que están expuestos a acciones tan sencillas como que algún funcionario copie datos confidenciales en un Flash Memory. En este apartado se expone la propuesta que se plantea para prevenir la fuga de datos de la Asamblea Nacional; entre las principales bondades del sistema se pueden describir:

- Prevenir la fuga o pérdida de activos de información; especialmente datos privilegiados.
- Datos sensible en el tramo final de la red; aún si los usuarios no están conectados en una red institucional.
- Se toman las herramientas de software libre más robustas que existen actualmente en el mercado; explicadas a profundidad más adelante.

En el mercado tecnológico, los DLP son aquellas tecnologías o herramientas que tienen como función prevenir la pérdida de datos basados en la inspección de contenidos con un análisis textual de los datos. Por ejemplo: en reposo, datos en la nube, datos en movimiento en la red y en dispositivos (Gartner, 2017). También, Reed (2017) señala que los productos DLP integrados ofrecen un conjunto de características como son: pasarelas web, pasarelas de

correo electrónico, firewalls de redes, IDS, cifrado de correos electrónicos, gestión de contenidos, herramientas de clasificación de datos, herramientas de descubrimiento de datos y agentes de seguridad de acceso en la nube. La propuesta de Reed (2017) sostiene que DLP integrado se basa en el cumplimiento de la normativa y casos de uso de la propiedad intelectual de los datos. Es a través de estos principios de cumplimiento de normativas que se quiere ofrecer el proyecto DLP a la Asamblea Nacional.

4.2. Diseño de las políticas de seguridad

Según Castrillón & Lezcano (2013), las políticas se deberían establecer en la herramienta Data Loss Prevención (DLP) para realizar una correcta detección del movimiento de la información confidencial en las instituciones. Estas guías o políticas, son más claramente establecidas por Rendón (2014), quien señala que hay distintos tipos de políticas y están clasificadas en 8 clases de reglas establecidas de acuerdo a la información que desea proteger. Es en los lineamientos de este autor que el proyecto DLP de este proyecto se pretende basar para ofrecer servicios de primer nivel a la Asamblea Nacional del Ecuador:

- Políticas para web: este tipo de políticas se encargan de monitorizar el tráfico en la web para determinar la información que viaja por esos protocolos.
- Políticas para correos electrónicos: Este tipo de políticas trabajan sobre los protocolos POP3, SMTP e IMAP para ver qué información cruza por dichos protocolos.
- Políticas de almacenamiento extraíbles: Este tipo de políticas trabaja sobre los datos que son transferidos a los dispositivos extraíbles como USB y discos duros.
- Políticas de almacenamiento encriptado: Este tipo de políticas trabajan sobre los datos encriptados que son transferidos a los dispositivos extraíbles como USB y discos duros.

- Políticas de almacenamiento en entradas extraíbles: Este tipo de políticas se utilizan para el control de la información que es copiada a dispositivos extraíbles.
- Políticas de impresoras: Este tipo de políticas controlan que la información no sea impresa sin la autorización correspondiente.
- Políticas para captura de pantallas: Este tipo de políticas controlan el uso de las capturas de pantalla cuando se esté usando con alguna información sensible en primer plano.
- Política API: Esta regla es una característica única de la herramienta MyDLP.

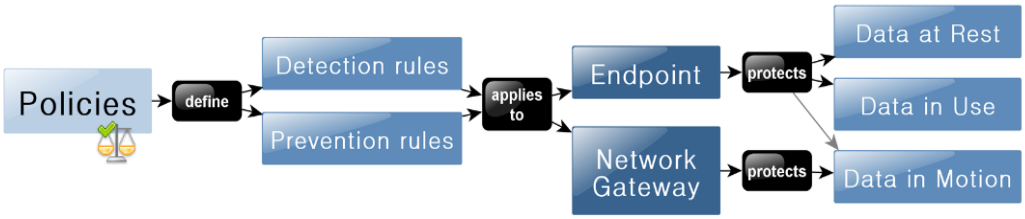


Figura 12:Diseño de políticas
Fuente: Castrillón & Lezcano (2013).

4.3. Reglas generales para la implementación en el DLP

Al momento de llevar a cabo la implementación del proyecto DLP del presente trabajo, es necesario seguir ciertas reglas establecidas para el mismo. A continuación, se describen:

- Restringir el uso de equipos y medios de almacenamiento no autorizados por la institución.
- Generar y almacenar la información de la institución en los equipos que están debidamente autorizados.
- No guardar información ajena a la institución en los equipos y medios de almacenamiento pertenecientes a la misma.

- El correo electrónico debe ser utilizado para uso exclusivo de trabajo de la institución.
- Determinar la información sensible de la institución por cada departamento o custodio de la misma.
- Bloquear y notificar la transferencia en archivos adjuntos que contenga información sensible por correo electrónico.
- Bloquear y notificar la transferencia en archivos adjuntos comprimidos que contengan información sensible por correo electrónico.
- Bloquear y notificar la transferencia de información sensible que esté en el cuerpo del mensaje del correo electrónico.
- Bloquear y notificar la transferencia de fragmentos de información sensible en el cuerpo del mensaje del correo electrónico.
- Bloquear y notificar la transferencia de fragmentos de información sensible que contenga la cabecera del mensaje en correo electrónico.
- Bloquear y notificar la transferencia de información sensible por medios de almacenamiento extraíbles como DVD, CD, HDD, USB entre otros.
- Bloquear y notificar la transferencia de fragmentos de información sensible por medios de almacenamiento extraíbles como DVD, CD, HDD, USB, entre otros.
- Bloquear y notificar la transferencia de información sensible por medios de protocolos: HTTP, FTP, NFS, etc.
- Bloquear y notificar la transferencia de fragmentos de información sensible por medios de protocolos: HTTP, FTP, NFS, etc.
- Bloquear y notificar la transferencia de información sensible por medio de mensajería instantánea como Skype, Google Talk, etc.

- Configurar para que el generador y su grupo de trabajo puedan leer la información de carácter sensible.
- Bloquear y notificar la transferencia de información sensible por VPN en la red.
- Bloquear y notificar la impresión de información sensible.
- Bloquear y notificar la captura de pantalla de la información sensible.
- Restringir la transferencia de la información sensible sin la autorización por parte de un ente rector.
- Restringir que la información sensible generada en la institución sea cifrada.
- Almacenar y conservar los eventos (logs) para futuros análisis forenses.
- Restringir la instalación y desinstalación de los agentes de control de los equipos informáticos de la institución.
- Definir los perfiles de cada usuario y su área de trabajo para cada funcionario, estableciendo permiso y restricciones de actividades.

4.4. Comparativa de herramientas DLP

Gartner (2017) define que los DLP pueden ejecutar desde simples notificaciones hasta bloqueo de activos. Las tecnologías DLP pueden dividirse en dos categorías: a.- Los DLP Empresariales, los cuales incorporan técnicas de detección sofisticadas para ayudar a prevenir la fuga de datos críticos, con la ayuda de agentes y servidores en dispositivos virtuales o físicos y monitoreo del tráfico de la red. b.- por otro lado están los DLP Integrados los cuales ofrecen un conjunto limitado de funciones para ello se debe combinar con otros productos de seguridad y a la vez formar un conjunto de herramientas de protección de los datos entre ellas pudeen ser: sistema de prevención y detección de intrusos (IDPS), puerta de enlace de correo seguro (SEG) y firewalls de redes empresriales (ENFW). El cuadrante mágico resalta las diferencias de las empresas fabricantes y las herramientas líderes DLP que están en el mercado.

Figura 13: Magic Quadrant
Fuente: Gartner (2017)

En la figura No. 13 se muestran las herramientas de pago, más no las de código abierto, a continuación, se realizará una comparación de las herramientas líderes DLP libres y de pago.

Tabla 2:

DLP líderes a nivel mundial

Herramienta	Open Source	Paid	Observación
Opendlp	x		Es una herramienta libre, está no dispone de soporte y es compleja a la hora de instalar y configurar.
MyDLP	x	x	Es una herramienta DLP consta

		de dos versiones, la versión empresarial y la otra versión de la comunidad libre.
Sycmatec	x	Esta herramienta está orientada para grandes empresas, y proporciona servicios útiles para prevención de fuga.
Forcepoint	x	La Herramienta DLP Forcepoint para empresas multiplataforma funciona para Mac, Linux y Windows, además esta aplicación tiene un módulo de análisis de imágenes.
Digital Guardian	x	Es una poderosa herramienta difícil de configurar, esta herramienta DLP es para grandes empresas y es multiplataforma, funciona tanto para Windows, Mac y Linux.
Intel Security	x	Está herramienta se puede adaptar fácilmente a la empresa, a diferencia de las demás ésta tiene más enfoque en el análisis forense.

Elaborado por: El autor de la investigación

Koutsourelis (2014) establece que Opendlp y MyDLP son las dos herramientas libres más completas para detectar la fuga de información, siempre hay margen de mejora, pero el sistema propuesto puede proporcionar un nivel de protección satisfactorio al implementar las

polítas correctas en la herramienta, sin costo alguno. A continuación se presenta un párrafo mostrando las bondades y limitaciones de cada una:

Tabla 3

Tabla de comparativa de las herramientas DLP

	Opendlp	MyDLP Enterprise	MyDLP Comunity
Open source	x		x
Multiplataforma: en Windows, Mac y Linux, con soporte para impresoras, servidores de terminales y escritorios virtuales.	x	x	x
Es un producto DLP con una consola de administración intuitiva y fácil de usar.		x	x
Controla la trasferencia de archivos en medios extraíbles (USB, Discos Duros).	x	x	x
Controla el envió de archivos sensibles por correo electrónico.	x	x	x
Acciones de cuarentena y archivo.		x	
Soporte y servicio al cliente.		x	
Controla la impresión de archivos sensibles.	x	x	x
Integración con directorio activo.		x	x

Registrar y controlar el cifrado de la información sensible almacenada.		x	x
Plataformas web.	x	x	x
Integración de bases de datos.	x	x	
Integración de almacenamiento remoto (CIFS, SMB, NFS, FTP).		x	
Documentos hash.		x	x
Detalles de coincidencia de texto, destinatario del correo y archivo de correo.	x	x	x
Revisión de políticas	x	x	x

Elaborado por: El autor de la investigación
Fuente: Koutsourelis (2014)

Cómo se mencionó anteriormente, OpenDLP es derrotado cuando se enfrenta a datos cifrados y la automatización de MyDLP, debido a la arquitectura de su consola web. Los servidores Linux no admiten una interfaz gráfica todo se realiza bajo comando UNIX.

4.5. MyDLP Appliance

MyDLP es de código abierto a nivel servidor, es una aplicación para monitorear información confidencial tanto en el host como en el tráfico de la red. Esta aplicación ayuda a prevenir que la información de las organizaciones que la utilicen pueda perderse, fugarse o robarse de cualquier manera. El proyecto de desarrollo MyDLP ha hecho que su código fuente esté disponible bajo la licencia GNU (General Public Licence). MyDLP soporta la prevención de pérdida de datos en red, en uso y reposo (Koutsourelis, 2014).

4.5.1. Componentes de MyDLP

Para Rendón (2014) esta herramienta consta de tres componentes:

- MyDLP Network Server, este funciona como el centro de administración de la herramienta, su instalación se realiza de preferencia en la distribución Ubuntu/Linux.
- MyDLP Endopoint, es el agente de control el que permite detectar y evitar que la información de las organizaciones sea trasladada en cualquier medio existente, se encarga del cumplimiento de las políticas implementadas para erradicar la fuga de información.
- MyDLP Web UI, desde este aplicativo web se configura las políticas, agentes de control y todo el proceso para erradicar la fuga de información.

4.5.2. Requisitos de instalación

Tabla 4

Requerimientos de Sistema

	Servidor	**Cliente**
Procesador	Core i5 3GHz 64 bits	Core i3 1,6GHz
Memoria RAM	8GB	2GB
Sistema operativo	Ubuntu	Linux, Windows y Mac
Almacenamiento	256GB o más	50GB
Red	100/1000 Mb/s	10/100/1000 Mb/s

Elaborado por: El autor de la investigación

4.5.3. Tipos de implementación de MyDLP

Hay dos maneras de implementar una herramienta DLP, una de ellas es el modo span, este es un sniffer en modo promiscuo que revisa el tráfico que pasa por la red. El otro modo es inline, todo el tráfico pasa de forma física por la herramienta DLP; a diferencia del modo

span que sólo detecta, pero no bloquea la pérdida de información, el modo inline por su implementación este será capaz de detener y bloquear la fuga de información (López et al., 2015).

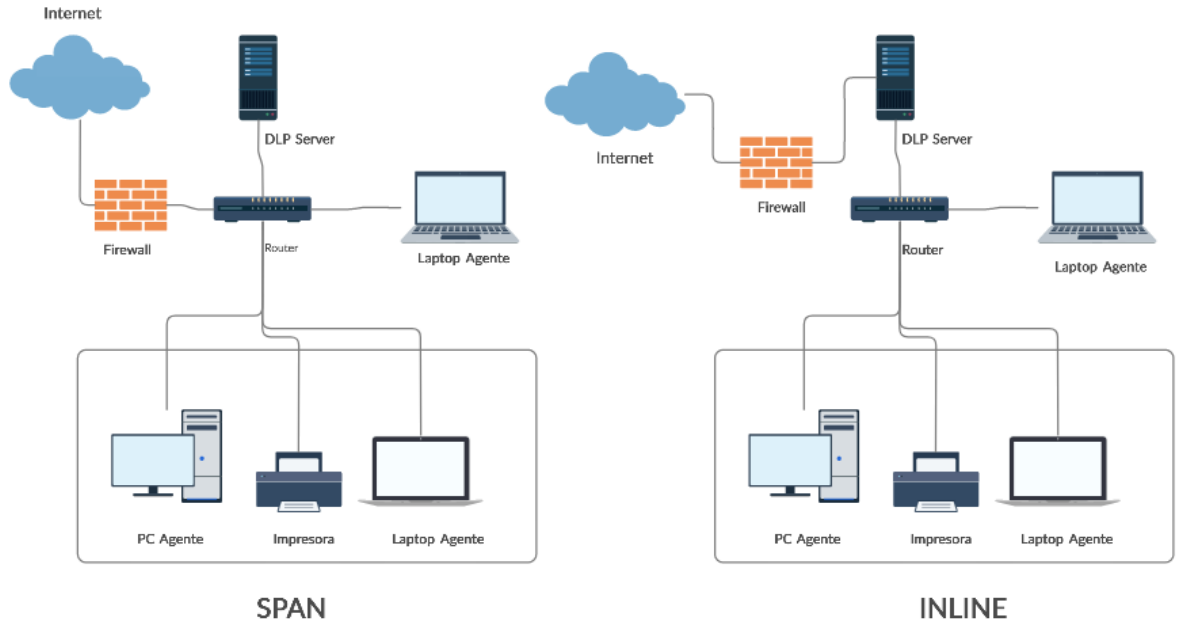


Figura 14: Tipos de implementación

Fuente: López & Carvajal (2015)

4.5.4. Instalación

Para la instalación de la herramienta MyDLP se puede descargar la ISO desde la página oficial https://download.comodo.com/mydlp/iso/latest.html, hay que tener en cuenta las características mencionadas anteriormente ya sea en máquina virtual o física. Para instalación en una máquina virtual se debe crear un virtual host vacía e iniciar por medio de una unidad extraíble, se procede a instalar MyDLP, en idioma escoger inglés, la configuración del teclado también tiene que estar en idioma inglés. Lo que se refiere a la zona horaria dejar por defecto del sistema.

Para empezar la instalación dirigirse al anexo 2 de este documento.

4.5.5. Configuración

Para realizar la configuración inicial de MyDlp se debe ingresar al terminal y digitar el siguiente comando sudo pico –t /etc/network/interfaces, se modifica la configuración que viene por defecto y se añaden nuevas configuraciones a la interfaz de red del servidor de acuerdo a la configuración de la misma.

Iface enss3 intec estatic
Address 192.168.0.136
Netmask 255.255.255.0
Network 192.168.1.0
Broadcast 192.168.1.255
Gateway 192.168.1.1

A continuación se procede a reiniciar el servicio de red con el siguiente comando: sudo /etc/init.d/network restart, con lo cual se establecerán los ajustes de nuestra red.

El acceso al servidor debe hacérselo desde otra PC por medio del navegador este puede ser Internet Explorer, Mozilla Firefox o Google Chrome el usuario se dirige a ajustes y configurar el servicio proxy e insertar la IP del servidor 192.168.0.136 con el puerto 3128 para establecer la configuración.

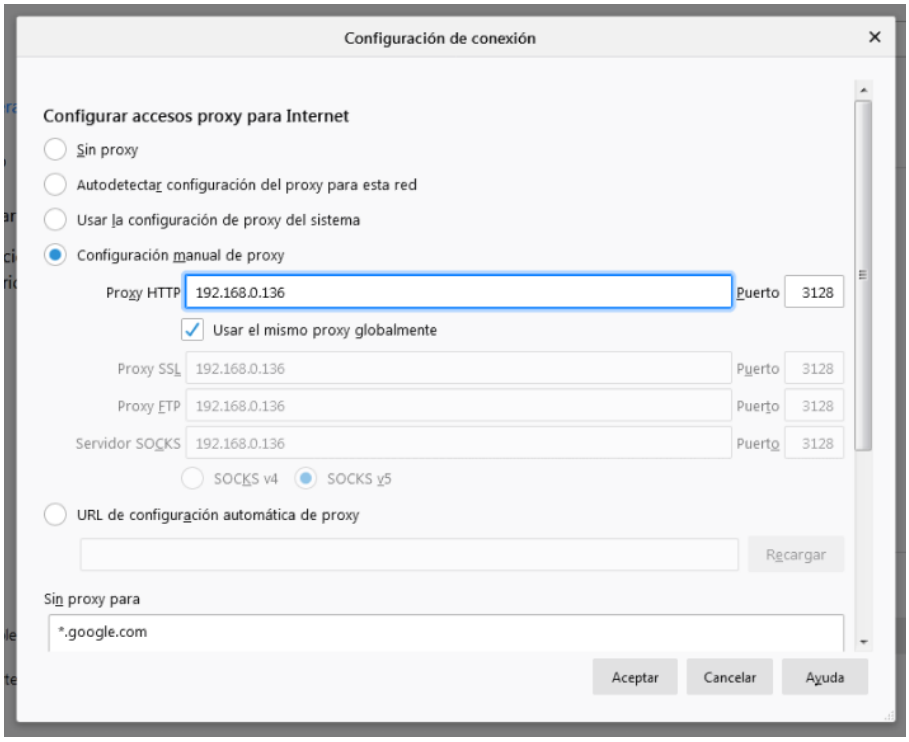


Figura 15: Configuración proxy
Fuente: Elaborada por autor de la investigación

Continuando con la configuración se debe ingresar al navegador web y en la parte de la URL digitar lo siguiente https://192.168.0.136, esta será la dirección IP con la cual trabajará el servidor de MyDLP luego aparecerá la pantalla principal de la aplicación.

Una vez que ya se ingresó al navegador aparecerá una pantalla con un formulario de ingreso y ahí se debe digitar la clave y usuario que se configuró en la instalación del servidor MyDLP y luego ingresar al sistema.

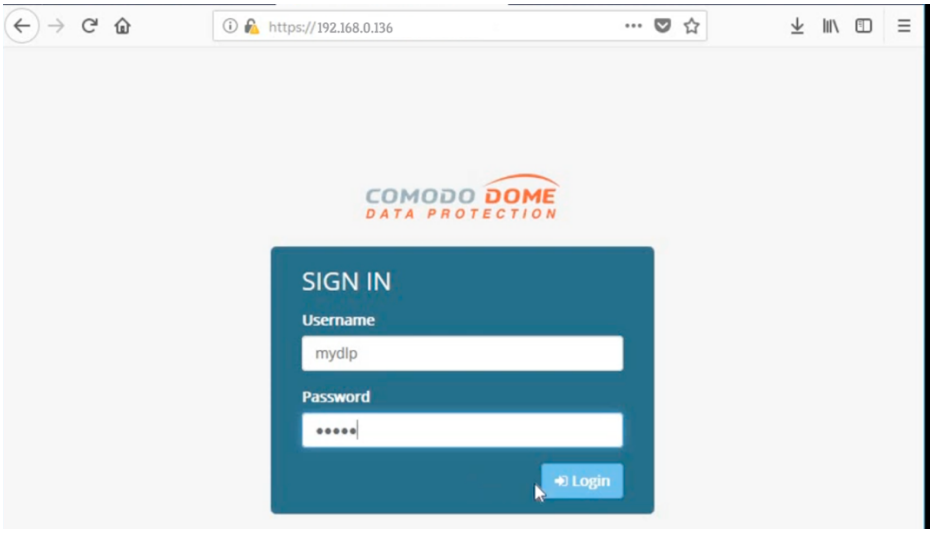


Figura 16: Inicio de sesión en MyDLP
Fuente: Elaborada por autor de la investigación

Al realizar esta prueba de concepto y verificar el funcionamiento de la herramienta de prevención de fuga de información se deben comprender algunos puntos cómo el levantamiento de la información clasificada de manera sensible, y priorizar las políticas que entrarán en funcionamiento.

4.5.6. Instalación de Endpoint MyDLP

La instalación del agente de MyDLP en los puntos finales de la red o en los tramos fuera de la misma que se desea monitorear y tener el control de la información que viaja a través de esta. Se puede instalar el agente uno por uno en cada máquina, también se puede sincronizar con el Active Directory.

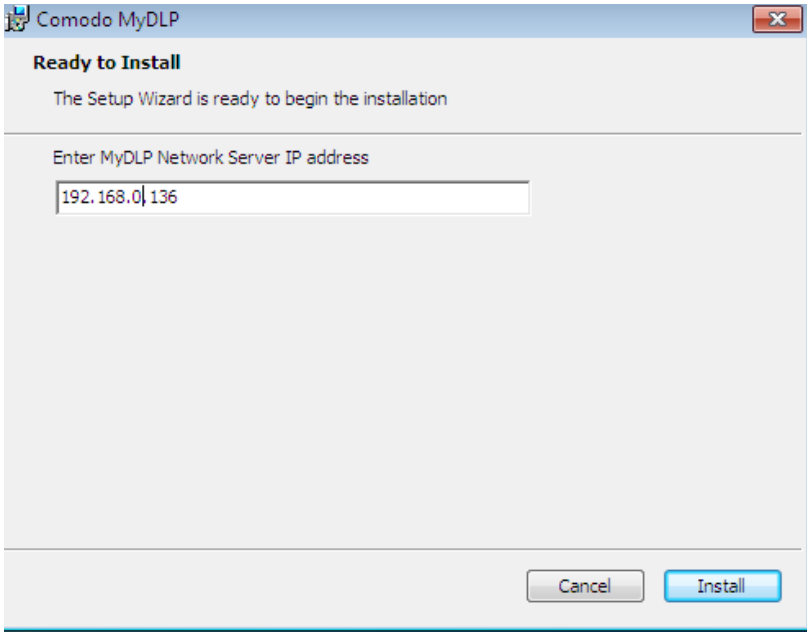


Figura 17: Instalación de Endpoint
Fuente: Elaborada por autor de la investigación

4.5.7. Estructuras de las reglas

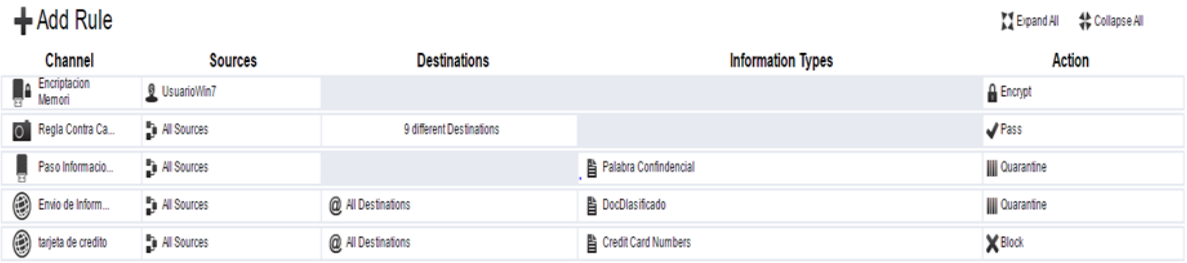


Figura 18: Estructura de reglas
Fuente: Elaborada por autor de la investigación

En la figura No. 18 se puede observar la estructura para el registro de reglas e ítems que se deben llenar con el fin de prevenir la fuga de información, entre ellas se detallan las siguientes:

- **Canal**: Es el sitio donde se escoge la vía de transmisión de información que se debe controlar, estos pueden ser: vía web, USB, captura de pantalla, entre otros.
- **Fuente**: En este recuadro se debe priorizar a que tipos de usuarios, grupos de usuarios o direcciones IP va dirigido esta regla.

- **Destino**: Puede dirigirse a dominios, grupos o aplicaciones.
- **Tipos de Información**: Para esta regla se debe seleccionar qué tipo de información será bloqueada, o puesta en cuarentena.
- **Acción:** Se debe escoger que acción se puede tomar en el momento que se genere un incidente al infringir dicha regla y se pueden seleccionar las siguientes acciones:

  Pasar: Esta acción permite el libre tránsito de la información por los canales sin ninguna restricción.

  Bloquear: Esta acción no permite que la información circule por los canales, con ella se bloquea todo el tráfico de la información y genera un registro de los eventos, con la excepción en los medios extraíbles.

  Registro: Crea un registro de los datos que pasan por el canal, esta acción es incompatible con la captura de pantalla y regla de disquete.

  Cuarentena: No permite que la información pase y a su vez se crea un registro, este se almacena en el servidor MyDLP, con eso el administrador puede descargar y revisar qué información fue afectada. Esta acción no está disponible para las siguientes reglas; Almacenamiento extraíble, captura de pantalla, USB, CD-DVD y disquete.

  Archivo: Esta acción permite que pase la información, se crea un registro y se almacena una copia en el servidor MyDLP, esta acción no está disponible para las siguientes reglas; Almacenamiento extraíble, captura de pantalla, USB, CD-DVD y Disquete.

  Encriptación: Se aplica a los dispositivos extraíbles encriptando la información, esta acción solo está permitida para la regla de almacenamiento extraíble.

Solo lectura: La acción de solo lectura está disponible solo para las reglas de CD-DVD y disquete.

4.6. Pruebas de concepto

La prueba de concepto se realizó en un ambiente controlado en redes virtuales con máquinas virtuales, como servidor Ubuntu 12.04 donde está preinstalada la herramienta MyDLP, para los agentes de control (MyDLP Endpoint) se instaló en máquinas Windows 7 y en Ubuntu 16.04.

Para esto se comenzará con la configuración y activación de las políticas de acuerdo a los requerimientos de la institución, para ello se puede realizar las reglas de transferencia o de descubrimiento de datos todo depende de la necesidad de la organización, para crear una regla de transferencia de datos, haga clic en 'Políticas', luego 'Add Rule' a la izquierda en la sección 'Política'.

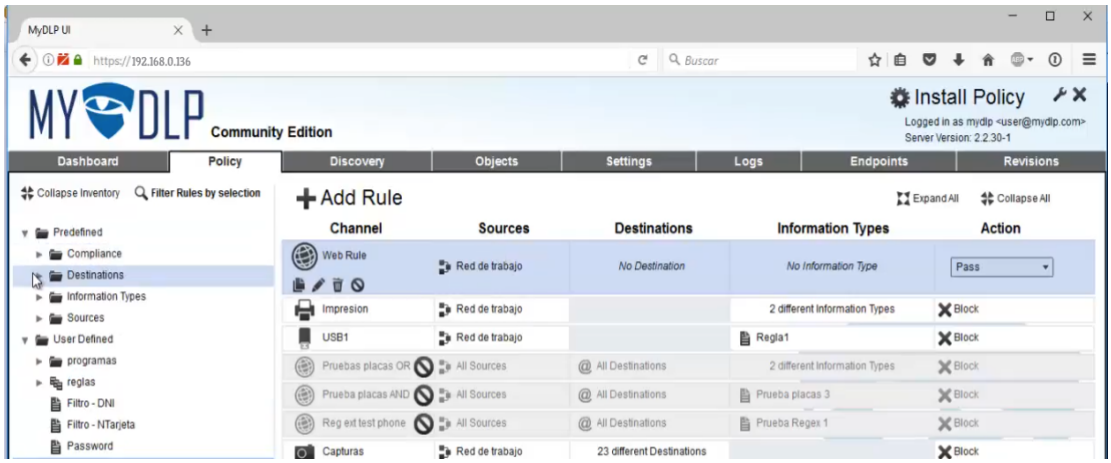


Figura 19: Crear regla de política para la web
Fuente: Elaborada por autor de la investigación

Para la realización de la prueba de funcionalidad con los formatos y los canales de transmisión en el punto final de la red, se utiizaron los datos más comunes con los que se trabaja en la Asamblea Nacional, los cuales se enlistan más adelante. En la siguiente tabla se detallarán algunos formatos con los cuales se trabajó para realizar la prueba de concepto.

Tabla 5

Test de funcionalidad de canales de datos

Formato	**Canales**					
	Impresión	**Email**	**HTTP/s**	**FTP**	**SSH**	**CD/DVD**
*.txt	x	x	x	x	x	x
*.pdf	x	x	x	x	x	x
*.doc	x	x	x	x	x	x
*.docx	x	x	x	x	x	x
*.ppt	x	x	x	x	x	x
*.pptx	x	x	x	x	x	x
*.xls	x	x	x	x	x	x
*.xlsx	x	x	x	x	x	x
*.odt	x	x	x	x	x	x
*.odg	x	x	x	x	x	x
*.odp	x	x	x	x	x	x
*.rft	x	x	x	x	x	x
*.ods	x	x	x	x	x	x
*.png	x	x	x	x	x	x
*.jpg	x	x	x	x	x	x
*.bmp	x	x	x	x	x	x
*.iso			x	x	x	x
*.tar		x	x	x	x	x
*.zip		x	x	x	x	x
*.gz		x	x	x	x	x
*.7z		x	x	x	x	x

*.tar.gz	x	x	x	x	x
*.rar	x	x	x	x	x
*.zip_pass	x	x	x	x	x
*.sha-512	x	x	x	x	x
*.Backup	x	x	x	x	x

Elaborado por: El autor de la investigación
Fuente: López, Richardson, & Carvajal (2015)

También se especifica la funcionalidad de cada formato de los datos versus los canales para los sistemas operativos que se mencionó en la descripción de arriba mediante los canales de archivos.

Tabla 6

Test de funcionalidad en sistemas operativos

Formato	**Windows**		**Linux**	
	Con Agente	**Sin Agente**	**Con Agente**	**Sin Agente**
*.txt	x	x	x	
*.pdf	x	x	x	x
*.doc	x		x	
*.docx	x		x	
*.ppt	x		x	
*.pptx	x		x	
*.xls	x		x	
*.xlsx	x		x	
*.odt			x	
*.odg			x	x
*.odp			x	x
*.rft			x	x
*.ods			x	x
*.png	x		x	
*.jpg	x		x	
*.bmp	x		x	

*.iso	x	x
*.tar		x
*.zip	x	x
*.gz		x
*.7z		x
*.tar.gz		x
*.rar	x	x
*.zip_pass	x	x
*.sha-512	x	x
*.Backup	x	x

Elaborado por: El autor de la investigación
Fuente: López, Richardson, & Carvajal (2015)

Se han implementado algunas reglas, una de ellas es la política para la web donde se impedirá que los funcionarios puedan enviar claves o contraseñas por medio de correos electrónicos u otros aplicativos web.

Esta regla detecta algún patrón de contraseñas, claves o número de tarjetas entre otros, bloqueando así el envió de correos electrónicos.

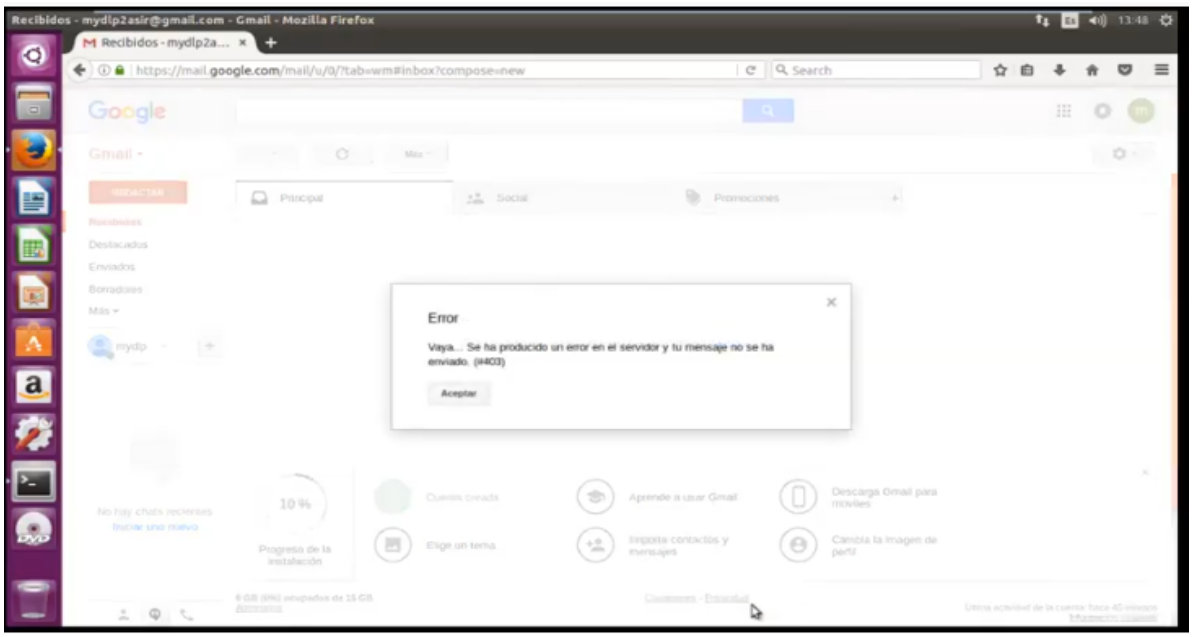


Figura 20: Validación de regla contraseñas
Fuente: Elaborada por autor de la investigación

Cada vez que la herramienta detecta un patrón de contraseñas, número de tarjetas de créditos o débito, la solución bloquea el envió del correo generando un mensaje de error y notificando al funcionario que el correo no puede ser enviado, en este caso como ejemplo se utilizó la plataforma de correos de Gmail y se trató de enviar “la contraseña: mydlp”.

Otra de las reglas que se implementó en este servidor es la regla de política de discos extraíbles, ésta ayuda a evitar que los documentos que contengan información clasificada como sensible sea trasladada a un disco extraíble sea este una USB u otro dispositivo.

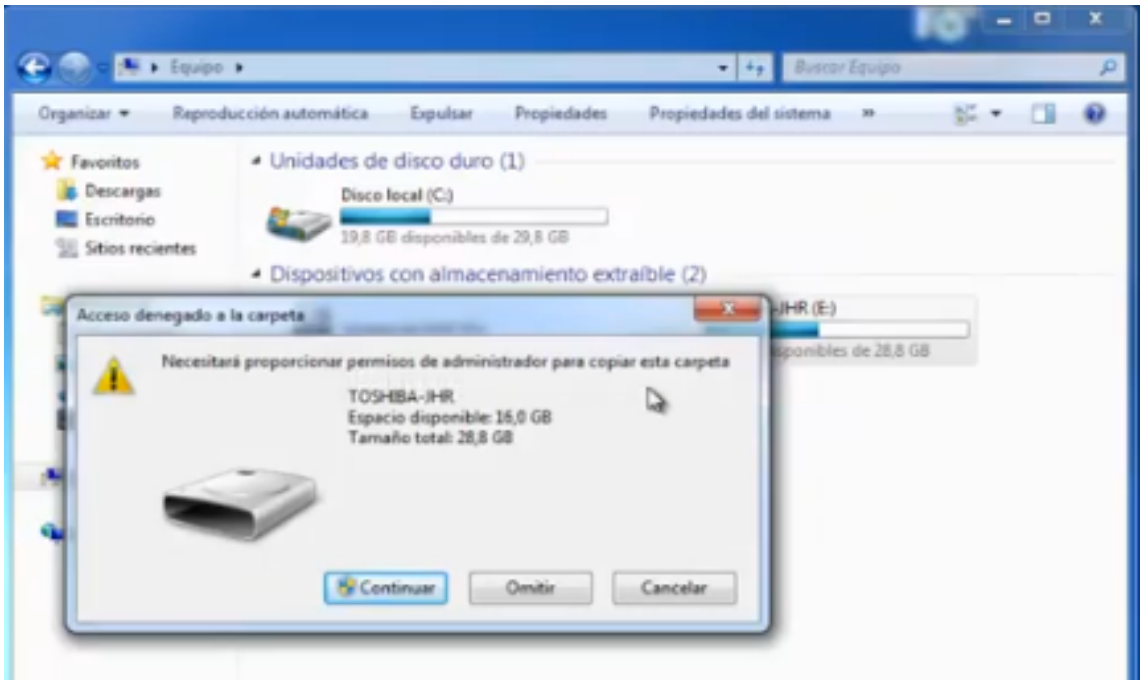


Figura 21: Validación de la regla de traslado de información
Fuente: Elaborada por autor de la investigación

La imagen anterior muestra como la herramienta bloquea el traslado del documento que contiene información sensible, este ejemplo se creó con la información susceptible que se configuró para que la herramienta detecte los patrones de la información y así evitar que el archivo sea transportado en un disco extraíble.

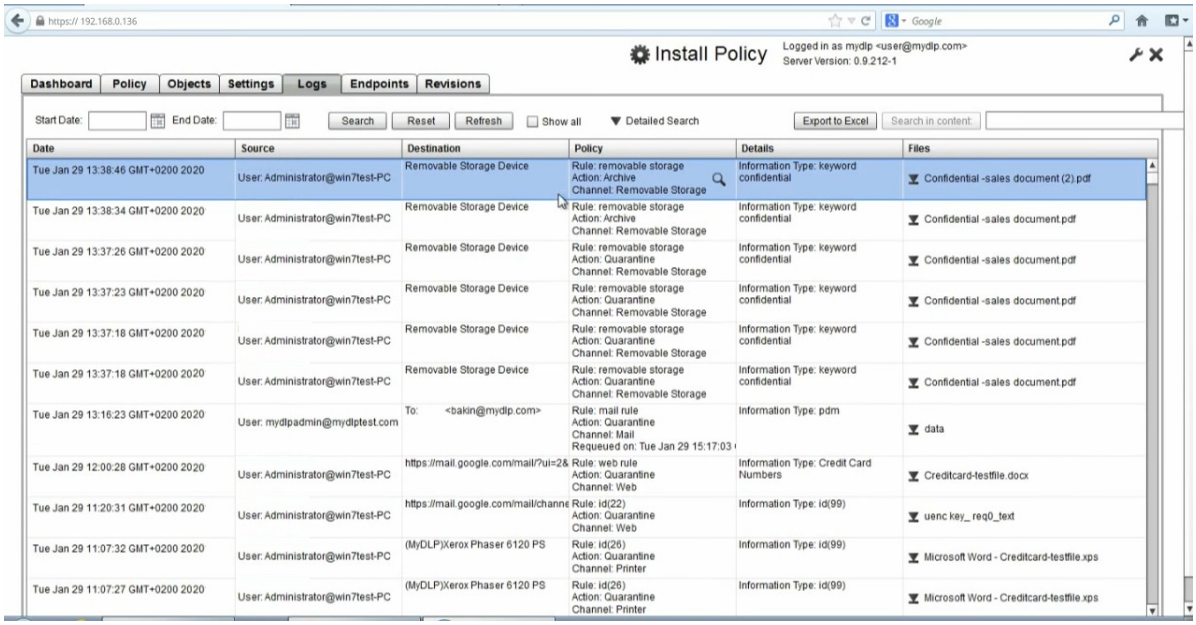


Figura 22: Log de la herramienta
Fuente: Elaborada por autor de la investigación

También cuando se pretende violentar una regla el servidor de MyDLP registra cada acción en los logs donde se almacena la hora, fecha, acción, fuente y la regla a ser violentada con el fin de realizar un análisis forense.

CAPÍTULO V

CONCLUSIONES Y TRABAJOS FUTUROS

5.1. Conclusiones

- Se planteó una herramienta que permite mitigar la problemática de la pérdida de información sensible en la Asamblea Nacional basada en software libre (open source) como lo son MyDLP y Opendlp, estas son las herramientas libres que lideran el mercado y se realizó una comparativa para determinar la eficiencia y eficacia de cada una de ellas y determinar cual se implementará en la institución.
- La herramienta MyDLP tiene la finalidad de disminuir la fuga de información gradualmente, sin embargo, no se puede decir que es 100% seguro que los datos de la Asamblea Nacional estén protegidos por lo que se sugerirá realizar evaluaciones periódicas de riesgos al software.
- La solución Data Loss Prevention es una herramienta que ayuda con la seguridad de la información, a pesar de implementar esta solución DLP se está lejos de cubrir al 100% a nivel de seguridad de la información, sin embago, MyDlp logra bajar la fuga de información gradualmente, a esto se debe realizar la gestión periódica de riesgos, lo cual implica la evaluación de controles.
- Se obtuvo una metodología para la implementación de una herramienta de DLP con software de código abierto, para la Asamblea Nacional, a quienes el Estado les solicita que aseguren la información personal de los funcionarios. La metodología también tomó características del software de GNU por el Decreto Ejecutivo No. 1014 sobre el uso de Software Libre en la Administración Pública, cabe indicar que las tecnologías de open source no cubren todas las necesidades de los administradores por su limitante.

- Para precautelar la información, se implementó políticas que se adapten al control de la información en la institución, de esta manera se probó el método basado en el software de código libre y se analizó si la metodología y la tecnología DLP, son efectivas en la mitigación en la pérdida de datos.
- La conclusión más relevante del presente trabajo es que este tipo de iniciativas son eficientes siempre y cuando sean apoyadas por la alta gerencia u altos mando de las organizaciones donde se aplican. Esto se debe a la necesidad de evaluar periódicamente su funcionamiento y poder hacerlo sin encontrarse trabas en el camino.
- El usuario final en la Asamblea Nacional es el eslabón más débil, si bien ningún sistema es totalmente seguro, es posible concluir que actualmente la Asamblea no cuenta con las medidas pertinentes para proteger los datos de los usuarios que trabajan en ella.

5.2. Trabajos futuros

- Cabe indicar que las herramientas DLP en el Ecuador son poco explotadas, ya que no se encuentra suficiente información de éstas, especificamente de MyDLP y Opedlp Esto permitiría realizar un análisis más profundo sobre el tema. Debido a esto se sostiene que hay especio para realizar investigaciones tanto de estas herramientas como para el desarrollo de manuales sobre las mismas y bechmarks de su funcionamiento.
- Otro tarabajo que resultaría de gran relevancia para el tema de prevención de pérdida de datos es un estudio sobre la aplicación de normativas nacionales e internacionales en el tema. Actualmente no se pudo encontrar esta información, y de hecho las normativas en el Ecuador son aún muy escasas.

- Las instituciones públicas y privadas deben mantener un plan de capacitación y concienciación de sus funcionarios y empleados con el fin de garantizar el cumplimiento de las políticas y las herramientas a ser implementadas por los administradores, con esto se reducirá en un gran porcentaje, el número de incidentes de pérdida de datos en la institución.

BIBLIOGRAFÍA

Acosta, X. R. (2015). *Desarrollo de un modelo de seguridad para la prevención de pérdida de datos DLP, en empresas PYMES*. (Bachelor's thesis). Quito: Universidad de las Américas.

Almeida, C. A. T., & Herrera, L. R. (2019). La ciberseguridad en el Ecuador, una propuesta de organización. *Revista de Ciencias de Seguridad y Defensa, IV (7)*, 156–169.

Andrade Canales, I. (2015). DLP: Tecnologías para la prevención de la fuga de información. Revista *Seguridad Cultura y Prevención para TI, 1251478.*

Bertolín, J. A. (2008). *Seguridad de la información. Redes, informática y sistemas de información*. Editorial Paraninfo.

Cardona, O. D. (1993). Evaluación de la amenaza, la vulnerabilidad y el riesgo. En: A. Maskrey (Ed.) *Los Desastres No Son Naturales*, 51–74.

Castrillón Cadavid, M. A., & Lezcano Gallego, M. A. (2013). *Metodologia para prevenir la fuga de información aplicando un sistema DLP en las empresas del sector financiero*. (Bachelor's thesis). Medellín: Universidad de San Buenaventura

Código Orgánico Integral Penal*, COIP*. *Registro Oficial*, 180. (2017)

Constitución de la República del Ecuador. *Registro Oficial*, 449. (2008).

Decreto Ejecutivo 1014. Sobre el uso de software libre en la Administración Pública. (2008).

Digital G. (2015, Octubre). *Data Loss Prevention.* Recuperado de: http://digitalguardian.com/product/digital-guardian-plataform

García, J. A., Redingl, A., & López, J. C. (2013). Cálculo del tamaño de la muestra en investigación en educación médica. *Investigación En Educación Médica*, *2*(8), 217–224.

Godínez Chávez, A. D., & Espinoza, I. O. (2017). *Implementación de un sistema de seguridad dlp (data loss prevention)*. (Bachelor's thesis). Ciudad Universitaria, Cd. Mx.

Hauer, B. (2015). Data and Information Leakage Prevention Within the Scope of Information Security. *IEEE Access*, *3*, 2554–2565. https://doi.org/10.1109/ACCESS.2015.2506185

Koutsourelis, D. (2014). *Designing a free Data Loss Prevention System*. (MSc Thesis). Piraeus: University of Piraeus.

León, C. (2015). *Estrategias para la clasificación de la información y prevención de fuga de información*. (Bachelor's thesis). Universidad Piloto de Colombia.

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. *Registro Oficial*, *557*. (2002).

Ley Orgánica de Telecomunicaciones. *Registro Oficial*, *676*. (2015)

Lopez, G., Richardson, N., & Carvajal, J. (2015). Methodology for data loss prevention technology evaluation for protecting sensitive information. *Revista Politécnica*, *36*(3), 69.

López, J. F. (2019). Propuesta de DLP (Grabada por Edwar Chalá). Quito, Ecuador.

López, P. (2010). *Seguridad informática*. Editex.

Piattini Velthuis, M. (2015). *Auditoría de tecnologías y sistemas de información*. Retrieved from http://ebookcentral.proquest.com/lib/biblioseksp/detail.action?docID=5758908

Purohit, B., & Singh, P. P. (2013). Data leakage analysis on cloud computing. *International Journal of Engineering Research and Applications*, *3*(3), 1311–1316.

Raj, S. R., Cherian, A., & Abraham, A. (2013). A survey on data loss prevention techniques. *International Journal of Science and Research*, *2*(4), 240–241.

Reed, B., & Wynne, N. (2017). *Magic quadrant for enterprise data loss prevention*. Gartner Group Research Note, 38.

Rendón, M. (2014). *Prevención y Minimización de Fuga de Información Implementando DLP (Data Loss Prevention)*. (Bachelor's thesis). Universidad del Azuay.

Sánchez, J. I., & Ignoto, M. J. (1991). *La seguridad informática*. Instituto de la Pequeña y Mediana Empresa Industrial.

Silowash, G. J., & King, C. (2013). *Insider threat control: Understanding data loss prevention (DLP) and detection by correlating events from multiple sources*.

Sola, A., & Crespo, A. (2016). *Principios y marcos de referencia de la gestión de activos*. AENOR-Asociación Española de Normalización y Certificación.

Solarte, F. N. S., & del Carmen Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica-ESPOL*, *28*(5).

Tahboub, R., & Saleh, Y. (2014). Data Leakage/Loss Prevention Systems (DLP). *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*, 1–6.

Torres Martínez, M. A. (2015). *DLP: prevención fuga de información (Data Loss Prevention)*. (Bachelor's thesis). Universidad Piloto de Colombia.

Torsteinbo, T. (2012). *Data Loss Prevention Systems and Their Weaknesses.* (Bachelor's thesis). University of Agder.

Vieites, A. G. (2011). *Enciclopedia de la seguridad informatica* (Vol. 6). Grupo Editorial RA-MA.

VpnMentor. (2019). *Report: Ecuadorian Breach Reveals Sensitive Personal Data*. Retrieved from New York, VpnExpert website:

https://www.vpnmentor.com/blog/reportecuadorleak

ANEXOS

ANEXO 1

ENCUESTA

1. ¿Cree Ud. qué el uso de herramientas tecnológicas es beneficio para su trabajo?
   a. Si b. No

2. ¿Dónde archiva toda su información generada?
   a. PC b. USB c. Correo d. Cloud

3. ¿Utiliza frecuentemente el correo institucional?
   a. Siempre b. Rara vez b. Nunca

4. ¿Qué dificultad tiene al usar el correo institucional?
   a. Bastante b. Poco c. Ninguna

5. ¿Utiliza el correo personal para sus labores en la institución?
   a. Si b. No

6. ¿De qué tamaño es la contraseña que usa para su correo electrónico?
   a. Menor a 8 caracteres b. Mayor a 8 caracteres

7. ¿Qué pasa si no termina su trabajo en la oficina, continúa en casa?
   a. Si b. No

8. ¿Qué medio electrónico utiliza para movilizar la información?
   a. USB b. Correo c. Otros

9. ¿Alguna vez ha identificado algún problema de seguridad? ¿Cómo lo ha reportado?
   a. Si b. No
   ---

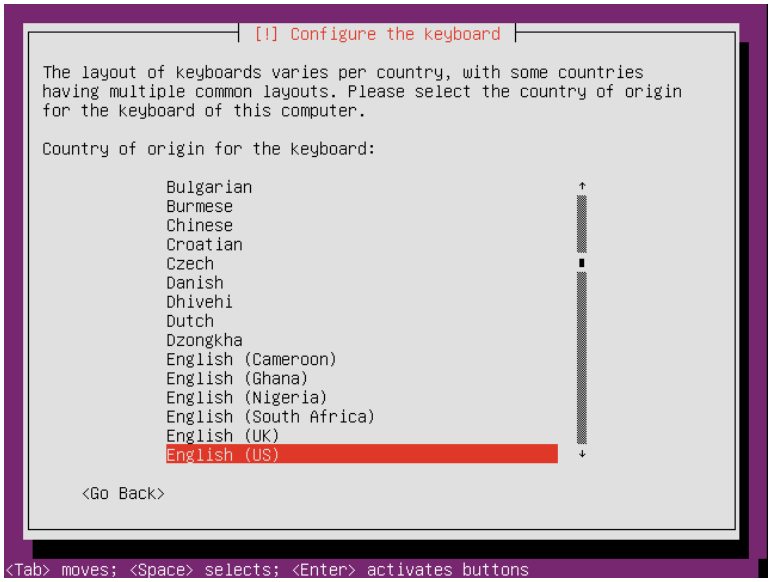
10. ¿Conoce Ud. las políticas y normas de la Asamblea Nacional?
    a. Si b. No

ANEXO 2

INSTALACIÓN

Para la instalación de la herramienta MyDLP se puede descargar la ISO desde la página oficial https://download.comodo.com/mydlp/iso/latest.html, hay que tener en cuenta las características mencionadas anteriormente ya sea en máquina virtual o física.

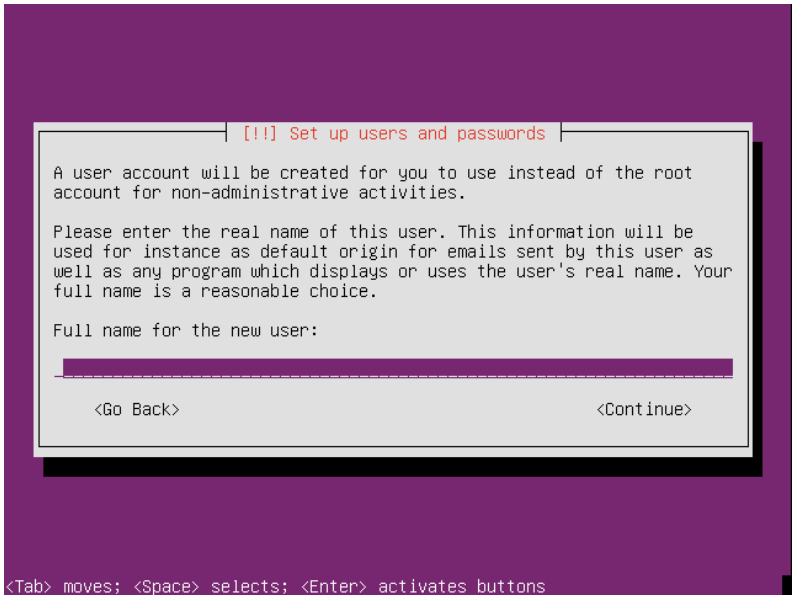
Escoger idioma



Fuente: Elaborada por autor de la investigación

Se debe escoger el idioma en inglés de preferencia para no tener problemas de imcompatibilidad con la herramienta Mydlp.

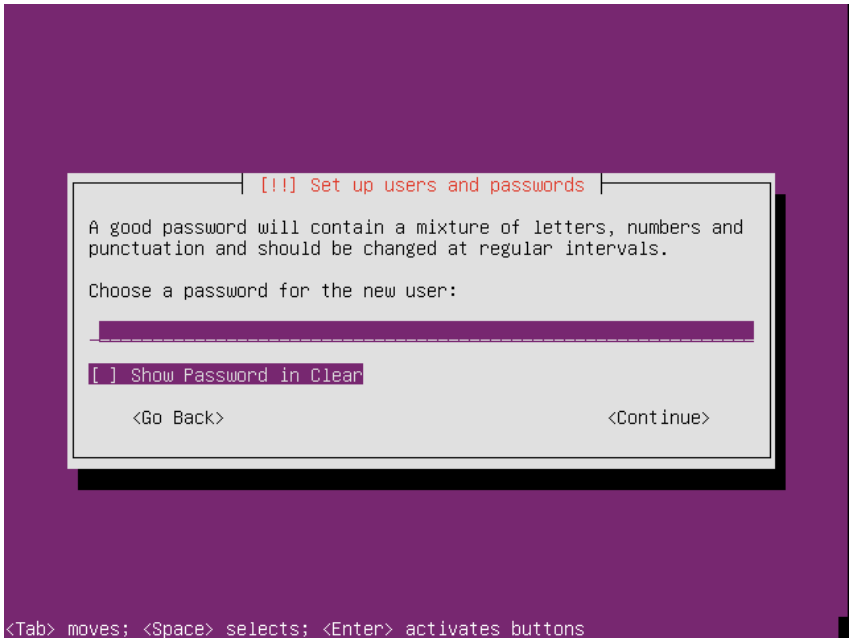
Creación de usuarios



Fuente: Elaborada por autor de la investigación

Se procede a digitar el nombre del servidor, de preferencia puede ser mydlp; este usuario será usado en el aplicativo web, es tan sencillo que solo se debe llenar los capos que se muestra en la figura.

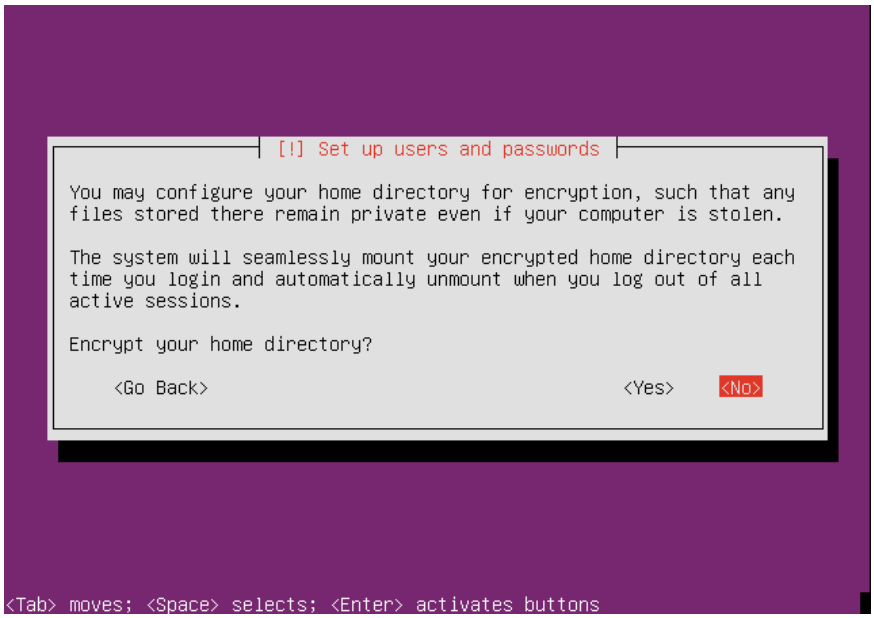
Creación de contraseña



Fuente: Elaborada por autor de la investigación

Después de digitar el usuario que de preferencia será mydlp, ahora digitar una contraseña para dicho usuario, cabe mecionar que la contraseña puede contener 8 caracteres y pueden ser mayusculas, minusculas y simbolos especiales.

Configuración de encriptado

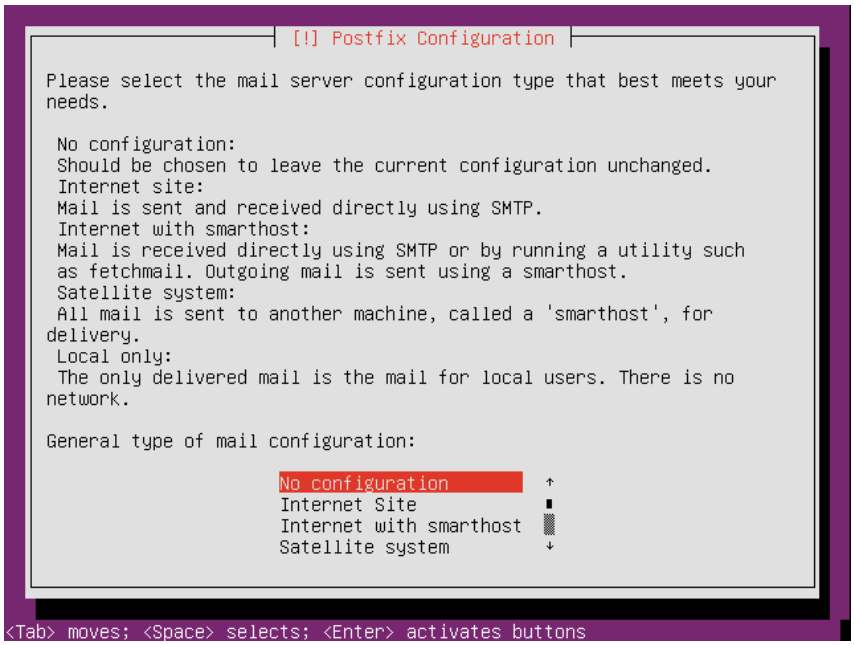


Fuente: Elaborada por autor de la investigación

A continuación, escoger “no” encriptar el directorio y hacer click en siguiente.

Configuración de SMTP

Escoger la configuración de smtp para nuestro servidor, de acuerdo a las configuración de la organización.



Fuente: Elaborada por autor de la investigación