OFICINA DE POSGRADOS

Tema:

HERRAMIENTAS DATA LOSS PREVENTION (DLP) OPENSOURCE, PARA LA SEGURIDAD DE LA INFORMACIÓN

Proyecto de investigación previo a la obtención del título de Magister en Ciberseguridad

Línea de Investigación:

SISTEMAS DE INFORMACIÓN Y/O NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN Y SUS APLICACIONES

Autor:

ING. ANDRÉS SEBASTIÁN LAGUA GAVILANES

Director:

ING. ALBERTO LEOPOLDO ARELLANO AUCANCELA, MSc.

Ambato – Ecuador

Febrero 2021

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

HERRAMIENTAS DATA LOSS PREVENTION (DLP) OPENSOURCE, PARA LA SEGURIDAD DE LA INFORMACIÓN

Líneas de Investigación:

SISTEMAS DE INFORMACIÓN Y/O NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN Y SUS APLICACIONES

Autor:

ING. ANDRÉS SEBASTIÁN LAGUA GAVILANES

Alberto Leopoldo Arellano Aucancela, MSc. f. Firmado electrónicamente por: ALBERTO LEOPOLDO ARELLANO AUCANCELA

CALIFICADOR

Galo Mauricio López Sevilla, MSc. f.

CALIFICADOR

Paúl Hernán Zurita Llerena, MSc. f.

CALIFICADOR

Pontificia Universidad Católica del Ecuador
OFICINA DE POSGRADOS

Juan Carlos Acosta, Padre, MSc. f.

DIRECTOR UNIDAD ACADÉMICA

Hugo Rogelio Altamirano Villarroel, Dr. f.

SECRETARIO GENERAL PUCESA

Pontificia Universidad Católica del Ecuador
SECRETARÍA GENERAL
PROCURADURÍA

Ambato – Ecuador

Febrero 2021

DECLARACIÓN DE AUTENCIDAD Y RESPONSABILIDAD

Yo: **ANDRÉS SEBASTIÁN LAGUA GAVILANES,** con CC. **180382398-6** autor del trabajo de graduación intitulado: "HERRAMIENTAS DATA LOSS PREVENTION (DLP) OPENSOURCE, PARA LA SEGURIDAD DE LA INFORMACIÓN", previa a la obtención del título profesional de **MAGISTER EN CIBERSRGURIDAD**, en la **OFICINA DE POSGRADOS**.

1.- Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad

Ambato, febrero 2021

ANDRÉS SEBASTIÁN LAGUA GAVILANES

CC. 180382398-6

AGRADECIMIENTO

Quiero extender un profundo agradecimiento a Dios, por su infinita bondad además de ser esa luz que nos llena de sabiduría día tras día para ser mejores personas. A la Pontificia Universidad Católica del Ecuador Sede Ambato, mi segunda Alma Mater, por su calurosa acogida tanto como estudiante y aún más como colaborador de la misma dentro del Departamento de TI. A nuestra Coordinadora Msc. Teresita Freire, por su cariño, bondad y acompañamiento durante todo este proceso de crecimiento profesional. A mis apreciados docentes los cuales no solo supieron brindarnos sus conocimientos, sino también, muchos de ellos se ganaron el cariño de todos nosotros. Para finalizar quiero reconocer la gran labor del Msc. Alberto Arellano excelente docente profesional y amigo, cuyo conocimiento ha brindado un aporte importantísimo a la realización del presente proyecto de investigación.

DEDICATORIA

> “Instruye al niño en su camino y aun cuando fuere viejo no se apartará de él” (Proverbios 22-6)

El presente trabajo de investigación va dedicado a mis padres Silvia y Ángel, en ellos se refleja todo el esfuerzo dedicado para la culminación de esta etapa en mi vida. Gracias por apoyarme y estar conmigo por siempre y para siempre, a pesar de todas las circunstancias y todos los tropiezos, sé que al finalizar el día puedo contar con ustedes.

RESUMEN

La Pontificia Universidad Católica del Ecuador Sede Ambato (PUCESA), es una institución orientada a la Educación Superior, cuenta con una amplia oferta académica tanto para pregrado como posgrado, en la actualidad posee alrededor de 1500 estudiantes y 300 colaboradores entre personal administrativo y docente. El Departamento de Tecnologías de la Información, considera la importancia que ha tomado los datos digitales, dentro del recinto educativo; y, de este modo evitar una infracción de estos. Con este antecedente el objetivo de este estudio es desarrollar un prototipo *Data Loss Prevention* (DLP) en una plataforma de tipo opensource. Para cumplir con el mismo, se hace uso de las metodologías de tipo inductivo, deductivo, cualitativo, mixto transversal y cuasi experimental, los cuales contemplan el siguiente procedimiento: Análisis de vulnerabilidades, impacto, riesgos y propuesta de métodos de seguridad. Este proceso aplica a toda la infraestructura tecnológica de la PUCESA, el resultado obtenido ante la propuesta de seguridad demuestra que, las herramientas Data Loss Prevention de tipo OpenSource, no cumple con los parámetros necesarios para prevenir la fuga de información dentro del recinto educativo. Debido a que, la mayor parte de software DLP es de licenciamiento pagado, y se divide en dos: cliente y servidor. Esto genera un alto coste en la implementación de la plataforma.

PALABRAS CLAVE

Seguridad de la información, Gestion de seguridad de la información, Fuga de datos, Confidencialidad, Integridad, Disponibilidad, Ataques y delitos informáticos

ABSTRACT

The Pontifical Catholic University of Ecuador Sede Ambato (PUCESA), is an institution oriented to higher education, has a wide academic offer for both undergraduate and graduate, currently has about 1500 students and 300 collaborators between administrative and teaching staff. The Department of Information Technology considers the importance that has taken the digital data within the educational campus, and thus avoid a breach of these. With this background, the objective of this study is to develop a Data Loss Prevention (DLP) prototype in an opensource platform. In order to achieve this goal, we use inductive, deductive, qualitative, mixed transversal and quasi-experimental methodologies, which contemplate the following procedure: analysis of vulnerabilities, impact, risks and proposal of security methods. This process applies to the entire technological infrastructure of the PUCESA, the result obtained from the security proposal shows that the OpenSource Data Loss Prevention tools do not meet the necessary parameters to prevent the leakage of information within the educational campus. This is due to the fact that most DLP software is paid licensing and is divided in two: client and server. This generates a high cost in the implementation of the platform.

Keywords: Data security, data security management, data leakage, confidentiality, integrity, availability, cyber-attacks and cybercrimes.

ÍNDICE

PRELIMINARES

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

En la actualidad, la información digital es uno de los activos más críticos a proteger en una organización. Toda institución ya sea educativa, financiera, gubernamental no podría funcionar sin la misma, sin embargo, con el avance tecnológico de las comunicaciones, cada día surgen nuevas amenazas que buscan poner en riesgo la seguridad de la información (SI).

La seguridad de la información es un tema que, cada día, adquiere mayor relevancia a nivel mundial. Las amenazas, tanto externas como internas, se incrementan y diversifican sus patrones y frecuencias de ataques, esto genera, un aumento en el porcentaje de fuga de información. Las organizaciones conscientes de esta problemática global, se esfuerzan por implementar mejores controles que protejan la información sensible y/o confidencial, utilizando mecanismos orientados a prevenir los canales de fuga (Navarro, 2017, p. 2).

Una de las funciones más complejas para un profesional de tecnologías de la información (TI), es mantener seguras las comunicaciones y cumplir con una gran cantidad de regulaciones para la privacidad de datos, con el objetivo de evitar lidiar con la piratería tanto interna como externa. Hoy en día, a pesar de invertir en sistemas de protección tipo *hardware* y *software* para disminuir los riesgos informáticos de la organización, se ha evidenciado a través de reportes de (CSIRT), un incremento de ataques dirigidos de forma directa, a la información digital que cada una de las organizaciones posee.

Las nuevas tecnologías de transmisión de datos han permitido tener una facilidad de comunicación dentro de las empresas, sin embargo, esto incrementa el riesgo de seguridad a la confidencialidad de la información sensible que estas conservan. Ello ha generado que, toda organización, se enfoque en crear métodos de prevención de fuga de la información dentro del SGSI como:

- **Firewall o Cortafuegos:** Para controlar el tráfico entrante y saliente de la red.
- **Sistemas de detección de intrusos (IDS):** Permite mantener un registro de actividades sospechosas en la infraestructura tecnológica.

- **Sistemas de prevención de intrusiones (IPS):** Se encarga de bloquear la actividad sospechosa mediante una conexión automática al firewall.
- **Tecnología antispam:** Realizar un análisis dentro al servidor de correo para separar los correos mal intencionados.

A juicio de Navarro (2017) las herramientas *Data Loss Prevention* (DLP) son: Herramientas (hardware o software), centradas en la seguridad de los datos, siendo efectivas si, se cuentan con los insumos necesarios para su funcionamiento. Algunos analizan el tráfico en la red buscando coincidencia con patrones establecidos, otros inspeccionan en tiempo real la información en las estaciones de trabajo (p. 2).

Estas tecnologías, explicadas de forma breve, han permitido a las organizaciones mantener un control ante amenazas internas. Kingston (2019) indica que “la siguiente ola de tecnologías que las organizaciones de TI comenzaron a abordar, se ocupó del problema del 'usuario interno' (p. 3). Algunos ejemplos de estos tipos de tecnologías incluyen:

- **Filtrado web**. Administra el contenido a un usuario, especialmente cuando, se utiliza para restringir material entregado a través de la Web.
- **Servidores proxy**. Atiende las solicitudes de sus clientes reenviando las solicitudes a otros servidores y puede bloquear toda la funcionalidad, como mensajería de Internet, correo electrónico web y programas de intercambio de archivos de igual a igual (Kingston, 2019, p.3).

El *software* DLP clasifica los datos regulados, confidenciales y críticos para el negocio, además, identifica las infracciones a las políticas definidas, por las organizaciones o dentro de un paquete de políticas predefinido, generalmente, impulsado por un cumplimiento normativo como Sistema de gestión de seguridad de la información (SGSI). Una vez que, se identifican esas infracciones, DLP aplica la corrección con alertas, cifrado y otras acciones de protección para evitar que los usuarios finales compartan datos de forma accidental o maliciosa que, podrían poner en riesgo a la organización (Kingston, 2019).

En la actualidad la Pontificia Universidad Católica del Ecuador Sede Ambato (PUCESA), carece de un sistema de protección dedicado a prevenir el desvío de la información digital. Esto

genera que, los datos corran el riesgo de ser manipulados de forma maliciosa, lo cual, es una amenaza latente a cada una de las dependencias del recinto educativo. El área directamente involucrada es el Departamento de Tecnologías de la Información, mismo que, ha visto la necesidad de implementar diversos procesos orientados a la seguridad informática. Con este antecedente el problema científico expresado a manera de pregunta es: ¿Cómo mejorar la seguridad de la información dentro de la PUCESA?

El trabajo de investigación tiende a responder la pregunta científica si la implementación de un sistema de prevención de pérdida de datos (DLP), disminuye el riesgo al acceso no autorizado de la información sensible y confidencial de la Universidad.

La investigación, tiene por objetivo diseñar un modelo de seguridad para la prevención de fuga de información privada de la Pontificia Universidad Católica del Ecuador Sede Ambato (PUCESA), para ello, se utilizará herramientas DLP de tipo opensource, el cual está basado en las necesidades generales del recinto educativo.

Los objetivos específicos de este estudio son:

1. Fundamentar teóricamente los conceptos DLP a partir de los criterios de diversos autores, relacionados con la seguridad dentro de instituciones educativas.
2. Diagnosticar los riesgos y vulnerabilidades de confidencialidad de la información que posee la Universidad para el diseño de la herramienta.
3. Diseñar un prototipo de prevención de pérdida de datos aplicando la tecnología DLP Opensource que, se adapte a las necesidades de la PUCESA.
4. Evaluar el funcionamiento de la tecnología DLP en el mejoramiento de la seguridad de la información en la PUCESA.

EL presente estudio es de tipo inductivo el cual está relacionado con el planteamiento de los Ítems de la Norma ISO 27001 para definir los riesgos y vulnerabilidades. Por otro lado, el método deductivo es usado para evidenciar las vulnerabilidades de los activos de la información, acorde a los manifiestos de la normativa ISO 27001. Este estudio es de tipo cuantitativo, debido a que, se basa en una recopilación de información a través de una entrevista dirigida a las autoridades que manejan los datos sensibles de la PUCESA. Por último, para la realización de

pruebas y análisis de resultados, se hace uso de una investigación con metodología cuasi experimental y de corte mixto transversal.

El Departamento de Tecnologías de la Información de la PUCESA, considera la importancia que ha tomado la información digital dentro del recinto educativo, para ello, se considera viable el desarrollo de un prototipo Data Loss Prevention (DLP) en una plataforma de tipo opensource como una opción que aumente la seguridad informática de la institución. De modo que, esta propuesta, se extienda a disminuir el riesgo a la confidencialidad de la información digital que maneja la Universidad.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1. Caracterización y estudio de la seguridad de la información

Una expresión mayormente utilizada es “ciberseguridad”, a pesar de tener una visión universal sobre lo que constituye, usa como equivalente a los términos seguridad de la información, seguridad informática o seguridad en cómputo, pero dicha premisa no resulta la ideal. En referencia a esto, ESET (2015), aseguran que:

La disyuntiva, se presenta cuando es necesario aplicar de manera adecuada los conceptos, de acuerdo con las ideas, que se pretenden expresar. Si bien existen distintas definiciones para la ciberseguridad, es importante conocer cuándo, se utiliza de forma correcta de acuerdo con el contexto, e identificar sus diferencias con los otros términos -por ejemplo, el de seguridad de la información (p. 1).

Desde un concepto breve podemos decir que la ciberseguridad tiene por objetivo preservar la información digital, que se encuentra en los sistemas de una organización, y esta forma parte de la seguridad de la información. Sin embargo, si deseamos otorgar un concepto más técnico a la ciberseguridad podemos decir que, acorde al congreso de la Information *Systems Audit and Control Association* (ISACA) en el año 2016 definen a la ciberseguridad como la “Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información, que se encuentran interconectados”.

La información en la actualidad, se en encuentra en diversas maneras, de forma digital como, por ejemplo: documentos electrónicos digitales u ópticos. Así también, en forma física, escrita o impresa en papel. Por otra parte, la seguridad de la información tiene por propósito reducir los riesgos a un mínimo nivel con el fin de, disminuir las amenazas latentes. Es decir, si lo explicamos en un aspecto más general podemos definir a la seguridad de la información como todas las actividades orientadas a proteger la información de algún tipo de peligro en el medio.

Desde la perspectiva de ESET (2015) aseguran que “la información requiere de medidas de protección adecuadas de acuerdo con su importancia y criticidad, y éste es precisamente el ámbito de la seguridad de la información” (p. 1).

La seguridad de la información está dividida en diversas categorías:

- La seguridad de red.
- La seguridad de aplicaciones.
- La seguridad operativa.
- La recuperación ante desastres y la continuidad del negocio.
- La capacitación del usuario final.

1.1.1. Análisis de la triada de la seguridad de la información

La tecnología es un componente fundamental, para cualquier organización por lo que, se usa de forma correcta a fin de evitar riesgos en la gestión de la información. De acuerdo con el Instituto Nacional de Ciberseguridad en España (INCIBE) indican que "la seguridad de la información, se articula sobre tres dimensiones, que son los pilares sobre los que, se aplica las medidas de protección de la información" (INCIBE, 2020, p. 6). Como, se muestra en la Figura 1.1:

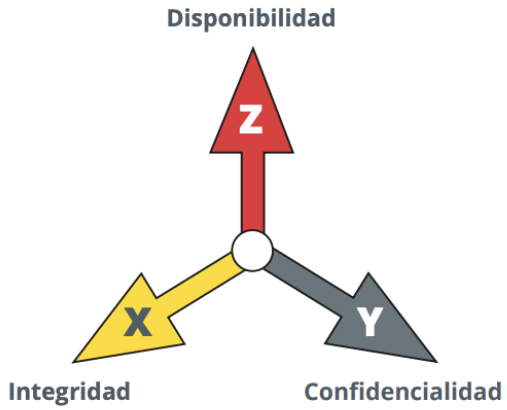


Figura 1.1. Dimensiones de la seguridad

Fuente: INCIBE (2020, p. 6)

Las tres dimensiones presentadas en la Figura 1.1., Integridad, disponibilidad y confidencialidad, son también, conocidas como la tríada de la información, mismas que, toda

organización ya sea, gubernamental, privada, educativa, médica o hasta religiosa, está en la obligación de garantizar para los datos de los usuarios internos y externos en la institución.

- **La disponibilidad de la información:** Hace referencia a que la información esté accesible cuando, se la requiera. Algunos ejemplos de falta de disponibilidad de la información son: cuando no es imposible acceder al correo electrónico corporativo debido a un error de configuración, o bien, cuando, se sufre un ataque de denegación de servicio, en el que el sistema «cae» impidiendo accesos legítimos. Ambos tienen implicaciones serias para la seguridad de la información (INCIBE, 2020, p. 6).

- **La confidencialidad**: Implica que la información es accesible únicamente por el personal autorizado. Es lo que, se conoce como *need-to-know*. Con este término, se hace referencia a que la información solo debe ponerse en conocimiento de las personas, entidades o sistemas autorizados para su acceso. Ejemplos de falta de confidencialidad, son el robo de información confidencial por parte de un atacante a través de Internet, la divulgación no autorizada a través de las redes sociales de información confidencial o el acceso por parte de un empleado a información crítica de la compañía ubicada en carpetas sin permisos asignados, a la que no tendría acceso (INCIBE, 2020, p. 6).

- **La integridad de la información**: Hace referencia a que la información sea correcta y esté libre de modificaciones y errores. Que la información ha podido ser alterada intencionadamente o ser incorrecta. Ejemplos de ataques contra la integridad de la información son la alteración malintencionada en los ficheros del sistema informático mediante la explotación de una vulnerabilidad, o la modificación de un informe de ventas por un empleado malintencionado o por error humano (INCIBE, 2020, p. 6).

Indudablemente, estos tres principios son imperativos para el profesional de seguridad de la información “pero considerarlos como una tríada obliga a que los profesionales de la seguridad

deban realizar el difícil trabajo de pensar cómo es que, se superponen y, a veces cómo pueden oponerse entre sí, lo que puede ayudar a establecer prioridades en la implementación de las políticas de seguridad"(CambioDigital OnLine, 2020, p.1).

En base a los principios mencionados se entiende que, la seguridad de la información no es un activo para comprar ni un fin en sí mismo, y no solo basta de una determinada inversión para asegurar los datos de una institución. Así mismo dicha información será gestionada hacia una meta concreta; con criterios generales de evaluación y decisión. De forma adicional, la seguridad de la información, se mantiene en constante monitoreo y actualización, con diversos escenarios que permitan tomar decisiones respecto a los diversos riesgos que, se afronta día tras día.

Desde el punto de vista de Pallas (2009) manifiesta que "existen diferentes enfoques para abordar la implementación y mantenimiento de un Sistema de Gestión de Seguridad de la Información (SGSI)". Algunos de ellos mantienen un enfoque crítico sobre el otro" (p. 5). Entre los enfoques principales están los estándares de la Organización Internacional para la Estandarización (ISO) número 27.000, que son un contenedor de diversas normativas con requerimientos específicos sobre la gestión de riesgos, auditorías, directrices e incluso contiene una guía completa de implementación de un SGSI.

1.2. Estándares ISO/IEC

El grupo de estándares creados por la Organización Internacional para la Estandarización (ISO) y gestionados por la Comisión Electrónica Internacional (IEC), están orientadas a la implementación de buenas prácticas para la implantación, mantenimiento y administración de un SGSI.

Cada norma está reservada dentro de una serie y van en orden numérico desde la 27000 hasta la 27019 y desde la 27030 hasta la 27044, cada una de estas contiene diferentes definiciones y términos, es importante conocer la definición de todas ellas para su correcta implementación. Además, es significativo resaltar que, los estándares son gratuitos a diferencia de otros que tiene un precio para su implementación.

La ISO 27000 es una sucesión de la norma BS 7799 de BSI que apareció por primera vez en 1995 y cuyo objetivo proporciona una visión general de las normas que componen la serie

27000, para brindar a cualquier empresa un conjunto de buenas prácticas hacia la gestión de la seguridad de su información (ISO, 2020). En la Figura 1.2 presentada a continuación, se evidencia la evolución de la normativa.

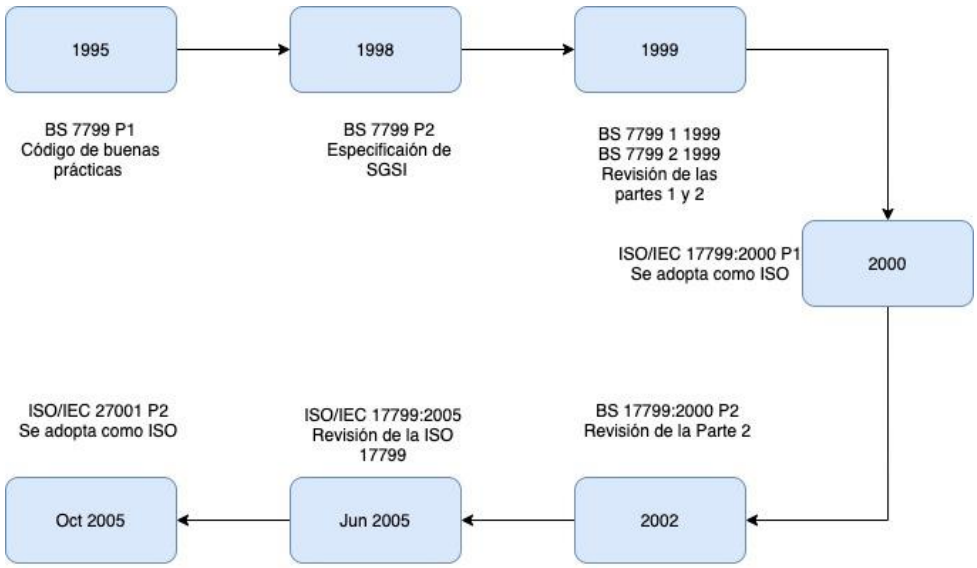


Figura 1.2. Evolución normativa 27000

Fuente: elaboración propia

1.2.1. ISO 27001

Fue publicada el 15 de octubre de 2005, revisada el 25 de septiembre de 2013 (segunda edición). Es la norma principal de la serie y contiene los requisitos para la implementación del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual, se certifican por auditores externos los SGSI de las organizaciones (ISO, 2020).

De acuerdo con la ISO, este estándar en su Anexo A, contiene enumerado en un resumen los objetivos de control de la ISO 27002:2005, para que estos puedan ser seleccionados por las instituciones en el momento de desarrollar su SGSI. Cabe destacar que, a pesar de no ser obligatoria la implementación de todos los controles, se justifica de forma sólida la no aplicabilidad de los controles no usados. Es decir que, la adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una institución. El establecimiento

e implementación del sistema de gestión de seguridad de la información de una organización está influenciado por las necesidades y objetivos de esta, los requisitos de seguridad, los procesos organizacionales utilizados y el tamaño y estructura del recinto. Se espera que todos estos factores de influencia cambien con el tiempo. (ISO / IEC 27001, 2013, p. 1).

Una de las principales características que posee esta norma es que, se utiliza desde una parte interna o externa a fin de evaluar la capacidad que tiene la organización de cumplir los requisitos para la protección de seguridad de la información (SI). De acuerdo con la ISO "el orden en el que, se presentan los requisitos en esta Norma Internacional no refleja su importancia ni implica el orden en el que, se implementarán. Los elementos de la lista, se enumeran solo con fines de referencia" (ISO / IEC 27001, 2013, p.1).

1.2.2. ISO 27002

El objetivo principal de esta norma es que una organización conozca de forma exacta y detallada sus activos como parte esencial de la administración de riesgos.

Acorde a la norma los activos son:

- **Recursos de información:** Datos contenidos dentro de la organización en general.
- **Recursos de *software*:** Sistemas Operativos, aplicaciones en general, herramientas de desarrollo.
- **Activos físicos:** Equipamiento informático y de comunicaciones.
- **Servicios:** Aplicaciones informática y de comunicaciones. (ISOTools Excellenge, 2020).

Estos siempre estarán clasificados según la sensibilidad y criticidad de la información que contiene dentro de la organización, para de esta forma tratarla y protegerla en una forma adecuada. Cabe señalar que:

Es necesario, que se realice una clasificación de la información, en la que, se indica la necesidad, las prioridades. También, habrá que clasificar el nivel de protección, que se necesite para llevar a cabo el tratamiento. La información tiene diversos grados de

> sensibilidad y criticidad. En algunos casos, se pueden requerir niveles de protección que resulten adicionales o de un tratamiento especial (ISOTools Excellenge, 2020, p.1)

Es recomendable usar un esquema de clasificación de la información para definir de manera adecuada sus niveles de protección. Además, se informa la necesidad de medidas especiales en el tratamiento de la información, para esto es importante distinguir todos los requisitos de seguridad.

Acorde a ISOTools Excellenge (2020) las actividades para establecer el control de riesgo son:

- **Clasificación:** La información, se tendrá que clasificar en relación con el valor que tenga, los requisitos legales, la sensibilidad del documento y lo crítico que sea para la empresa.
- **Etiquetado y manipulado de la información:** Se tendrán que llevar a cabo una serie de procedimientos para establecer un etiquetado y tratamiento de la información según el esquema de clasificación que, se ha realizado por la empresa.
- **Manipulación de los activos:** Se tienen que desarrollar e implementar procedimientos para la manipulación de todos los activos según el esquema de clasificación, que se ha generado por la propia empresa.

Cabe recalcar que, es necesario distinguir los requisitos de seguridad, pero según el acuerdo de la ISO/IEC, siempre, se inicia a controlar la confidencialidad de la información, sin descuidar los demás aspectos de la tríada de la información.

1.2.3. Sistema de Gestión de la Seguridad de la Información (SGSI)

Independientemente del tipo de actividad y tamaño, cualquier organización recopila, procesa, almacena y transmite información mediante el uso y aplicación de procesos, sistemas, redes y personas internos y/o externos. Todos ellos son activos de información esenciales para lograr los objetivos de la organización (iso27000.es, 2005)

Acorde a la ISO y su SGSI, toda institución está de forma inevitable expuesta a riesgos de diversos factores que podría comprometer los activos de información de una organización. Por tal motivo, la supervivencia de las organizaciones siempre estará relacionada con una buena identificación en los riesgos más relevantes y asociarlos con el nivel de impacto en caso de que uno de estos haya sido vulnerado.

La Norma ISO 27001 en complemento con la ISO 27002, estas proponen un Sistema de Gestión de la Seguridad de la Información centrado en la evaluación de riesgos, y está basado en 10 fases detalladas a continuación:

1) **Definir el alcance:** Aclara los límites de un SGSI en base a la ubicación e importancia de sus activos críticos de datos dentro de la organización, posterior a eso los asocia con los riesgos propios y externos asociados. Siempre, se debe considerar la información que sobrepasa el alcance de la institución, uno de los principales alcances de la SGSI es la concientización y promoción de esta.
2) **Política del SGSI:** Permite comprometer a la dirección con los objetivos de seguridad de la información para así obtener una mejora continua, se debe considerar que, la alta gerencia puede preferir una política de tipo variada como de gobierno único, amplio, sucinta o general y complementarlas con un conjunto de políticas como riesgo, seguridad o cumplimiento a fin de satisfacer el requisito ISO.
3) **Evaluación de riesgos:** Está determinado por cada organización el proceso más adecuado con la ayuda de las guías ISO, para esto, se espera un proceso documentado el cual explique el análisis e identificación, así como también, las consecuencias y probabilidades de ocurrencia de los riesgos en los activos de la organización, para de esta forma priorizarlos.

Es importante mantener una revisión y actualización periódica de dichos riesgos debido a los cambios sustanciales que afronta una institución frente a los avances tecnológicos, para así poder conservar un enfoque preventivo en acciones mitigadoras o de control. La ISO 27001 dice que “en definitiva, recopile evidencia material suficiente para tranquilizar a los auditores de que

el proceso está genera resultados útiles sobre los riesgos de la información" (iso27000.es, 2005, p.1).

4) **Declaración de aplicabilidad:** Es la encargada de establecer los riesgos de información y sus debidos controles de seguridad en un orden de relevancia y aplicabilidad al SGSI de la organización, y esta determina las evaluaciones periódicas de los riesgos, su objetivo esencial es evidenciar los controles recomendados en el Anexo A de la ISO/IEC 27001 o entre otros estándares.
5) **Tratamiento de riesgos:** Esta incluida por un procedimiento redactado el que permite implementar el plan para el tratamiento de riesgo adecuado al activo, esto es una forma para demostrar a los auditores que el proceso funciona de manera correcta, este documento puede contener listas, estructuras de matriz o base de datos para el control de las tareas, cuando, se acepta los riesgos siempre debe quedar en evidencia las firmas del riesgo relevante, para admitir formalmente la responsabilidad ante un incidente.
6) **Objetivos y planes:** Está enfocado a los compromisos para cumplir con los compromisos aceptados en la política del SGSI, estos a diferencia de las declaraciones de la política debe contener de forma determinada responsables, evaluación de objetivos, para así constatar el cumplimiento alcanzado de la SGSI. Los objetivos están estructurados por diferentes niveles según el caso que determine cada organización.
7) **Competencias:** Según la ISO afirma que: "retener información documentada como evidencia de la competencia, es muy variable según el tamaño de la organización y el número de personas implicadas en el alcance del SGSI" (iso27000.es, 2005, p. 1).

Hay que considerar las funciones y responsabilidades específicas para cada persona relacionada con la SGSI, estas, se extienden con otras funciones que, se relacione con los riesgos de la seguridad de la información.

8) **Planificación y control operacional y métricas:** Se debe mantener siempre una información documentada a tal medida que permita tener la seguridad de saber que

los registros, se llevan acorde a las planificaciones realizadas. Estos varían según la organización y su documentación está realizada en base a un nivel de eficacia requerido y con acciones de corrección, por ejemplo: presupuestos, recuentos de personal e informes de progreso con métricas relevantes, estrategias, planes, políticas, procedimientos y pautas de seguridad de la información.

9) **Auditorías internas y revisión por la dirección:** Permite obtener una evidencia documentada de los principales hallazgos, así como también, conclusiones y recomendaciones a fin de informar las no conformidades y acciones correctivas para una mejora de un SGSI. Se debe considerar que dichos informes sean imparciales y competentes a los profesionales designados el SGSI, todos estos informes pueden verificarse mediante calendarios, presupuestos, alcances, documentos de trabajo con evidencia, planes de acción entre otros.
10) **No conformidades y acciones correctivas:** Son las no conformidades de un SGSI, están basados en el ISO/IEC 27001 pero también surge por la necesidad de ser aplicada a cada organización por una parte externa para la gestión de un mejor alcance de la SGSI, se debe documentar en forma de los inconvenientes hallados a los activos, también son conocidos como no conformidades y deberán estar certificados por los auditores manteniendo un registro o índice de no conformidades.

Una correcta implementación de un SGSI permite obtener diversos beneficios a un menor costo como, por ejemplo:

- Brindar confianza y satisfacción de los requisitos de seguridad de los usuarios de la organización.
- Establece una metodología para la gestión del tratamiento en la ciberseguridad.
- Permite gestionar los activos de la organización de una manera organizada para facilitar una mejora continua y un ajuste a los objetivos organizacionales.
- Reduce el riesgo de pérdida de información, así como también, permite mantener una actividad después de un incidente.

1.3.Análisis de incidentes de fuga y pérdida de información:

En los últimos años, debido al caso *WikiLeaks,* uno de los temas más discutidos dentro del área de ciberseguridad es la fuga de la información, a pesar de ser un tema nuevo para la industria de la seguridad de la información cada día aparece nuevos casos de ataques y violaciones a la privacidad y confidencialidad de datos dentro de una institución.

La fuga de información es lo que ocurre cuando algún dato o activo de información que tenga valor para una organización pasa a manos ajenas, perdiendo la cualidad de confidencialidad que le fue asignada. Esto, se puede ver representado, por ejemplo, en documentos que pasan a ser accesibles por personas no autorizadas, o también por cualquier dato secreto que alguien interno le facilite a un externo sin pasar por un medio digital (Pacheco, 2011, p. 3).

Las instituciones siempre buscaran proteger la información de la mejor forma y toma las mejores consideraciones que estén a su alcance, para esto, se hace uso de la implementación de Antivirus, *Firewalls*, y políticas de contraseñas. Sin embargo, no siempre, se tiene control total de todos los datos de la organización, muchas, en repetidas ocasiones están relegadas a los servicios de otra empresa, o cada usuario maneja cierta información, cuyo mal manejo ocasionaría llevar a una fuga de la misma.

En el estudio sobre el estado global de la ciberseguridad en las pequeñas y medianas empresas realizado por Ponemon Institute (2019) manifiesta que:

Más de un 30% de las pequeñas y medianas empresas no cuentan con un plan de respuesta a incidentes para responder a las violaciones de datos y ataques cibernéticos. Esto es a pesar del hecho de que, de los mismos participantes del estudio, el 60 por ciento había experimentado una pérdida o robo de datos confidenciales en los últimos 12 meses. Esta falta de preparación podría ser extremadamente costosa, las empresas deben luchar para que sus sistemas vuelvan a la normalidad después de un ataque (p. 1).

Este reporte manifiesta además que, con la nueva modalidad de teletrabajo a la cual la globalización, se encuentra encaminada los ataques informáticos de robo de información han crecido de forma exponencial, como, se evidencia en la Figura 1.3:

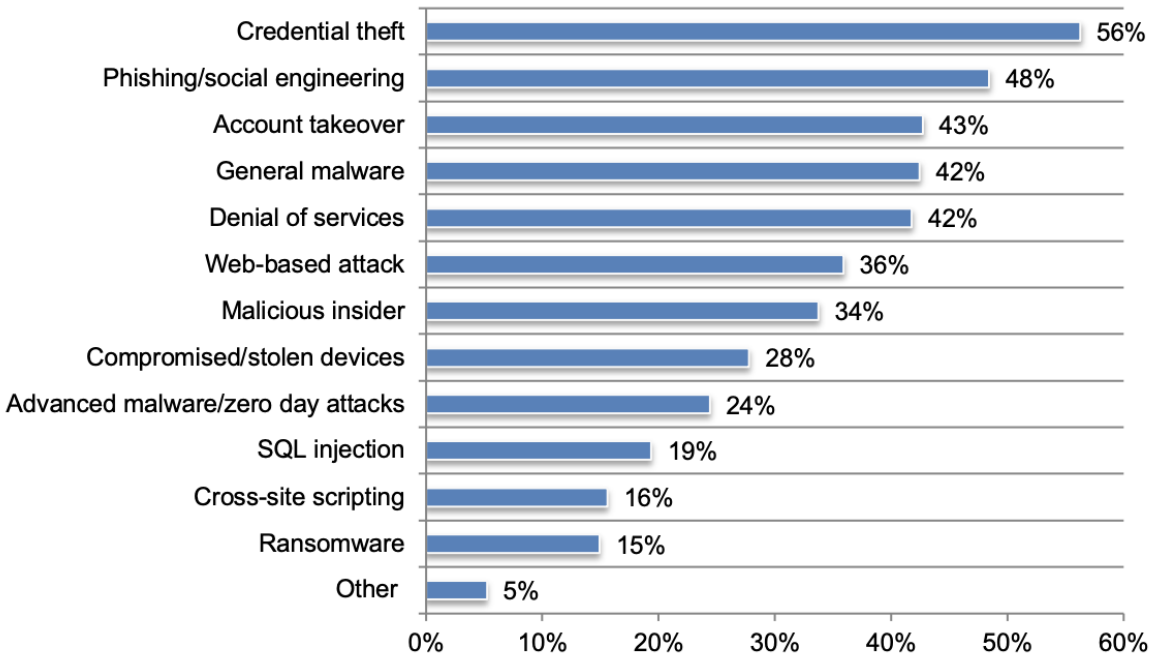


Figura 1.3. Reporte de ataques más comunes

Fuente: Ponemon (2020b, p.11)

1.3.1. Estudio de las principales causas de fuga de información

A juicio de Bortnik (2010), asegura que:

Algunos ejemplos de fuga de información pueden ser desde un empleado vendiendo información confidencial a la competencia, una secretaria que pierde un documento en un lugar público o en la misma línea la pérdida de una laptop o un pen drive, así como también el acceso externo a una base de datos en la organización o un equipo infectado con un Spyware que envíe información a un delincuente (p. 1).

A pesar de ello, existen otras causas para la fuga de información, como:

a) **Malware:** Existe diferentes causas para la pérdida de información, estos pueden ser errores humanos o hasta robos físicos. Sin embargo, otra gran causa relacionada a la fuga de la información, son los programas malignos, estos operan ya sea mediante la infección de navegadores o por sistemas de dominios DNS, lo cual permite iniciar comunicaciones

cifradas a través de puertos no autorizados para robar datos. Acorde al informe de Investigaciones de Violación de datos de Verizon (2020) manifiesta que “un tipo de malware estuvo involucrado en aproximadamente el 17 por ciento de las filtraciones de datos” (p. 7). El resumen de este reporte lo podemos apreciar en la Figura 1.4:

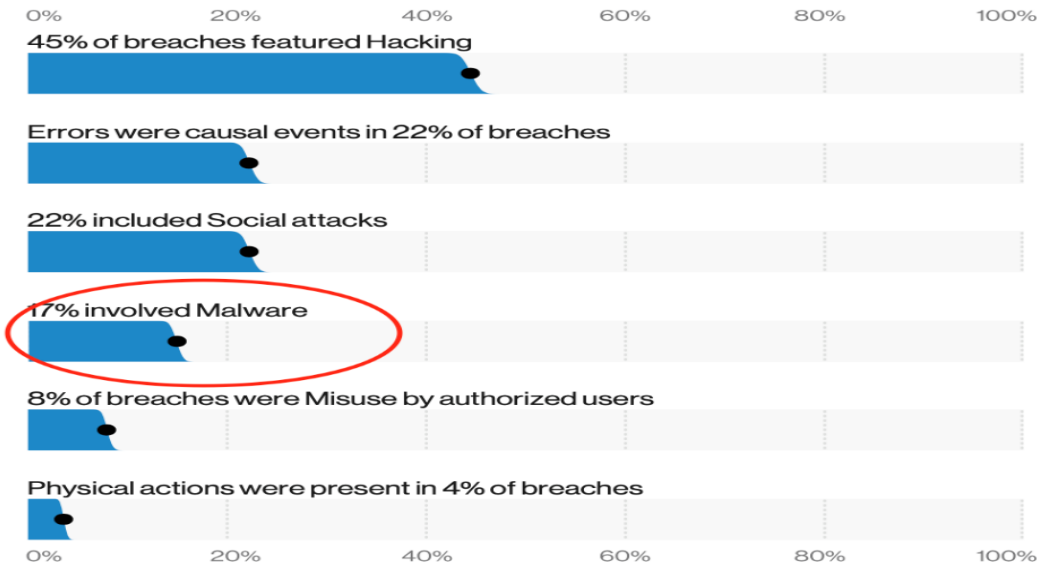


Figura 1.4. Reporte de Incidentes por Malware

Fuente: Verizon (2020, p.7)

b) **Servicios en la nube:** El crecimiento desmedido de los servicios ofrecidos en la nube, virtualización y las redes sociales, proporcionaron nuevos modelos de comunicación y contribuyeron a ampliar la brecha de seguridad (Navarro, 2017, p. 4).

Este servicio es un riesgo latente para toda organización debido a que la información no está contenida en el SGSI de la institución, sino más bien depende de los servicios brindados de otra empresa proveedora. Hoy en día tenemos una gran diversidad de herramientas de tipo *hardware*/*software* (HW/SW), que permiten identificar vulnerabilidades en la nube y en el caso de no tomar acciones para proteger este recurso, estos, se convierten en un blanco fácil para un ataque. En el reporte entregado por Symantec (2019), manifiesta que “una amenaza más insidiosa para la nube surgió en 2018 con la revelación de varias

vulnerabilidades en chips de hardware. Meltdown y Spectre" (p. 19), esta explotación brinda acceso a ubicaciones de memorias confidenciales.

c) **Tecnologías móviles:** A pesar de mantener conectado a los usuarios en todo momento, su gran difusión y fácil acceso aumentó el riesgo de pérdida o fuga de información una de las principales causas es la integración de la información de la organización con el dispositivo móvil personal. De acuerdo, con el Instituto Nacional de estadísticas y Censos (INEC) (2014), el 16.9% de las personas mayores a 5 años, posee un teléfono inteligente, esto sobrepasa la cifra registrada en 2011 en un 141%. El estudio refleja también, que el 28% de la población tiene acceso a internet, y el 40% utilizo datos en su celular (Navarro, 2017, p. 4).

Si bien el número total de infecciones de *malware* móvil disminuyó durante el año 2018, hubo un rápido aumento en la cantidad de infecciones por *ransomware* en dispositivos móviles, un tercio más en comparación al 2017. Estados Unidos fue el país más afectado por este tipo de ataques a la tecnología móvil, con aproximadamente un 63% de las infecciones. Le siguió China con un 13% y después Alemania con un 10%. La gestión de la seguridad de los dispositivos móviles sigue siendo un desafío para las organizaciones. A partir del 2018, uno de cada 36 dispositivos utilizados en las organizaciones, se clasificó como de alto riesgo. Esto incluyó dispositivos que fueron *rooteados* o liberados, junto con dispositivos que tenían un alto grado de certeza de que, se ha instalado malware (Symantec, 2019, p. 19). Ver Figura 1.5

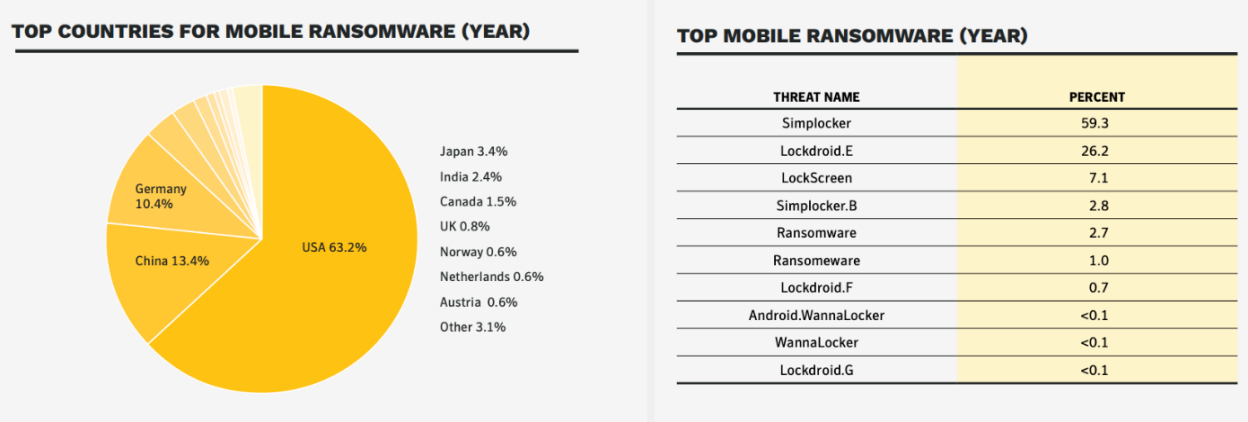


Figura 1.5. Reporte de ataques a la tecnología móvil

Fuente: Symantec (2019)

De acuerdo con los reportes entregados por empresas dedicadas a la seguridad informática, se evidencia que, las irrupciones informáticas han crecido año tras año y siguen nuevos patrones de ataque a las tecnologías más usadas por las instituciones. Esto atenta de forma directa a su reputación debido a que, si una empresa es afectada por el robo de información, esto ocasionará de forma directa la pérdida de confianza de sus clientes, y según una encuesta generada por Ramos (2011) especialista de Ciberseguridad de ESET, la empresa perdería 6 de cada 10 clientes, estos resultados la podemos apreciar en la Figura 1.6:

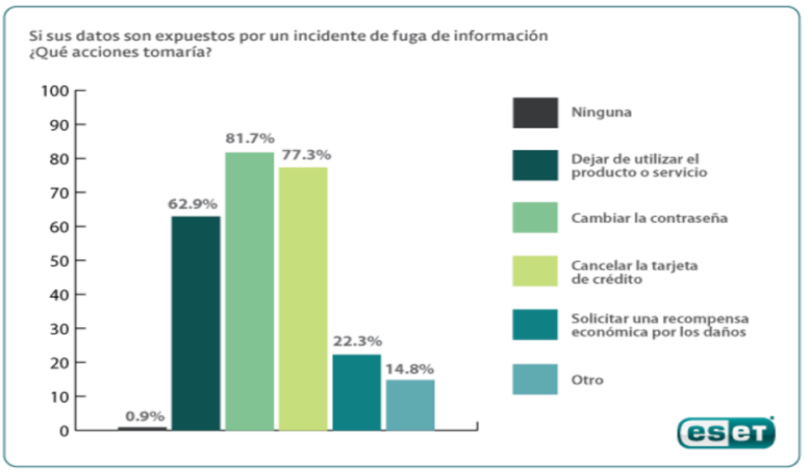


Figura 1.6. Encuesta realizada por ESET

Fuente: Ramos (2011, p. 1)

Día a día existe casos reales de fuga de la información a nivel mundial y según el reporte de Kaspersky (2020) los peores casos de fuga de la información contra grandes empresas a nivel mundial son cinco:

1) *Avanti Markets:* 1,6 millones de cuentas
2) *Election Systems* & *Software*: 1,8 millones de cuentas
3) *Dow Jones* & *Compay*: 2,2 millones de cuentas
4) *America's Job Link Alliance*: 5,5 millones de cuentas
5) *Equifax*: 145,5 millones de cuentas

Estas filtraciones, se hubieran podido evitar mediante una auditoría de la infraestructura informática, algo que, se hace con frecuencia en todas las compañías, sin importar su tamaño (Kaspersky Lab, 2020).

Ecuador no está libre de ataques, es así como en el año 2017, se realizó una publicación donde, se encontraba una supuesta base de datos, que según los autores pertenecía a la Policía Nacional del Ecuador, en la que, se mostraba información de carácter personal de más de 58336 agentes pertenecientes a diferentes instituciones gubernamentales como la Fiscalía General o la Policía Judicial. La información publicada contenía datos tan sensibles como, las credenciales de acceso a la plataforma institucional, con las debidas contraseñas encriptadas por el algoritmo SHA md5. Según el reporte de seguridad de Elevenpaths (2017) el 70% de las credenciales fueron comprobadas. Las cuentas de correo electrónico pertenecían a diversos dominios y los datos de las personas pertenecían a diversas instituciones como, se muestra en la Tabla 1.1 presentada a continuación:

Tabla 1.1. Número de usuarios afectados en cada institución

Institución	Número de usuarios
Policía Nacional del Ecuador	56247
Otros	2075
Fiscalía General del Estado	7
Policía Nacional del Perú	4
Nelson Andy	1
Policía Judicial	1
Prueba	1

Fuente: ElevenPaths (2017, p. 4)

1.3.2. Fuga de información en Instituciones Educativas

Uno de los objetivos principales para los delincuentes informáticos, son los recintos educativos debido a la información sensible que manejan, esta información, se usa de diversas formas maliciosas como: secuestros, estafas, robos, entre otros.

La red nacional de educación e investigación (CEDIA) en Ecuador, realizó una encuesta acerca de la seguridad de la información en las Instituciones de Educación superior (IES), pertenecientes a la red, en la cual, se evidencia que el 82% no cuentan con presupuestos asignados para la gestión de seguridad, aunque 36% de la IES si posee un área destinada a tratar las amenazas y riesgos relacionados con la seguridad de la Información, mientras que el 50% de las IES encuestadas, se encuentra en un nivel jerárquico Operativo. Por lo anterior, se evidencia la falta de sensibilización y compromiso por parte de los empresarios y directivos, para mitigar y reducir los riesgos de la fuga de información desde el interior de la organización. (Navarro, 2017, p. 3).

En los últimos años, se evidencia un crecimiento de intento de ataques a las instituciones universitarias, muchos de estos han tenido éxito en su tentativa de vulnerar la información de

dichos recintos, sin embargo, esta información es confidencial en cada universidad. En la Figura 1.7 podemos apreciar las estadísticas de alertas monitoreados por el CSIRT de CEDIA de los últimos 6 años.

Última actualización:
@2020-10-19 11:18:48

Alertas Procesadas

2014:	28.880
2015:	798.660
2016:	991.519
2017:	39.703
2018:	53.514
2019:	36.472
2020:	21.310
Total:	1.970.058

Figura 1.7. Alertas de intentos de ataques

Fuente: Csirt Cedia (2020, p. 1)

Como, se evidencia en las estadísticas presentadas por el CSIRT de CEDIA, las instituciones educativas están en constante amenaza debido a la información delicada que estas manejan. A pesar del monitoreo y protección por parte de CEDIA la mayoría de las universidades no cuentan con un SGSI bien definido dentro de la institución. De modo que, esto pone en riesgo a la institución como tal, la hace vulnerable a una fuga de información interna.

1.4. Estudio de las herramientas *Data Loss Prevention* (DLP)

Uno de los pilares fundamentales que requiere cualquier organización es mantener un control de acceso al igual que la prevención de la fuga de la información, con la ayuda de *Data Loss Prevention,* se dispone de una gran cantidad de herramientas orientadas a la protección de la información sensible de la institución, esta aplica un rastro imperceptible sobre los documentos.

DLP (Prevención de Fuga de Información - Data Loss Prevention (DLP) es un término de seguridad informática que comprende un conjunto de herramientas destinadas a evitar el envío de información sensible, confidencial o crítica, fuera del entorno de la organización,

adicionalmente describe las soluciones tecnológicas que detectan, monitorean y evitan que la información clasificada como confidencial sea transmitida y usada de forma indebida hacia el exterior de las organizaciones. (Torres, 2015, p. 2).

El objetivo principal de un DLP es alertar a la organización acerca de un mal uso de loa datos internos por parte de un usuario ligado íntimamente a la organización. En principio este sistema estaba orientado a una amenaza interna, y esta no siempre podía ser maliciosa, por lo general una amenaza de fuga de la información es común cuando un usuario interno hace un uso indebido con los datos, filtrándolos o haciéndolos públicos.

Con el pasar de los años, el uso de los DLP también sufrió cambios debido al aumento de usuarios mal intencionados, y violaciones de datos para comprometer el sistema y la red de la institución. Es así como "este aumento provocó una reevaluación de los actores de amenazas interesados en acceder, robar o destruir datos. Esta reevaluación, a su vez, definió dos actores de amenazas adicionales, el interno y el externo maliciosos" (Devlin & Northcutt, 2016, p. 4). Cabe señalar que:

Las aplicaciones de DLP intentan alejarse de la aplicación puntual o de nicho y brindan un enfoque más holístico a la cobertura, reparación y notificación de problemas de datos. Una forma de evaluar el nivel de riesgo de una organización es mirar a su alrededor de manera imparcial. Las tecnologías de comunicación más benignas podrían utilizarse contra la organización y causar daños (Kingston, 2019, p. 2)

Un DLP, se encarga de clasificar los datos regulados, confidenciales y críticos dentro de una organización, una vez realizada la identificación selecciona el tipo de infracciones dentro de las políticas definidas en un SGSI. Posteriormente a la identificación de las infracciones, se aplica la corrección, a fin de prevenir la fuga de la información, estas son: alertas, cifrado u otras acciones de protección que evite la compartición de datos ya sea de forma intencional o accidental, lo que pone de riesgo la confidencialidad de la institución.

1.4.1. Características

Según el criterio de Torres (2015) asegura que "la infraestructura DLP ofrece una solución robusta orientada a la detección, monitoreo, protección y administración de información

sensible dependiendo de su categorización, del medio de almacenamiento y de los propietarios identificados" (p. 2). Así:

- Detectar información sensible que, se encuentra almacenada, lo que genera un inventario de la información, a fin de mantener un control de la información tratada.
- Administrar el modo de uso de la información sensible utilizado por los usuarios dentro de la organización.
- Brindar protección a la información sensible mediante el uso de aplicaciones automatizadas controladas por las políticas de seguridad.
- Monitorear incidentes de seguridad para generar informes a través de una plataforma normalizada.

En la actualidad, los DLP son diseñados por diversas empresas orientadas a la seguridad de la información, en forma de complemento a sus servicios ofertados a fin de integrarlos a la infraestructura tecnológica.

Desde la perspectiva de Gómez (2011) asegura que:

Las tecnologías aplicables dependerán del entorno de tratamiento de la información: los documentos estructurados o preformateados por un sistema de información concreto precisarán de diferentes técnicas a los documentos no estructurados procedentes, por ejemplo, de herramientas ofimáticas. Los diferentes soportes del ciclo de almacenamiento de la información también condicionarán extraordinariamente las soluciones a emplear: no, se protege igual la información almacenada exclusivamente en una base de datos centralizada a nivel corporativo que aquella otra que pasa por diferentes estados desde la agenda personal del empleado hasta consolidarse en los sistemas TI centrales de la organización. (p. 7).

Un sistema DLP estándar estará formado por dos componentes, el de red que interactúa de forma permanente con todo el tráfico de la red, para así controlar todo el conjunto de datos que circulan en el sistema de información. Además, tenemos el componente de *EndPoint* o punto final denominado de esta forma porque está ubicado en los equipos de usuario final, para otorgar una administración de interacción del usuario con los medios de almacenamiento, o alteraciones

a la configuración del sistema. La arquitectura de las herramientas *Data Loss Prevention* está formada por un *software* ya sea libre o de paga, este esta configurado como seguridad dentro del área de seguridad perimetral para un correcto funcionamiento, como, se evidencia en la Figura 1.8:

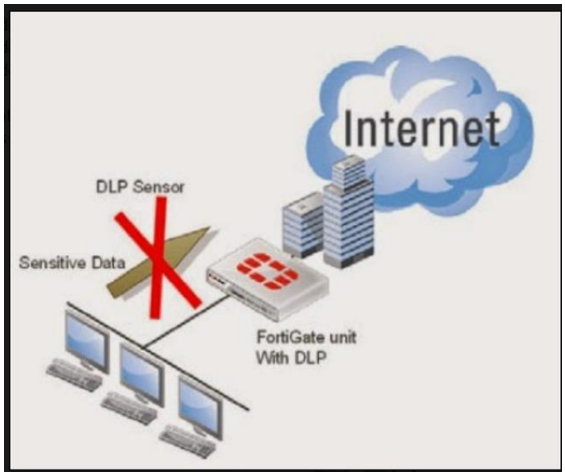


Figura 1.8. Instalación de software *Data Loss Prevention*

Fuente: Daffara Carlo (2015)

Desde su creación DLP, se ha utilizado en diversas industrias o en diversos ámbitos como el financiero, educacional, o hasta el gubernamental. Este, se encarga de brindar protección a la información que la organización considere confidencial. Es necesario aclarar que, cada empresa siempre maneja su base de datos de manera diferente, además que ofrece ciertas ventajas en su uso como:

- Recursos de *hardware* mínimos lo que disminuye el costo de implementación de un sistema DLP para permitir a cualquier tipo de organización tener acceso al mismo.
- Manejo de inteligencia artificial enfocada al contenido y contexto de la información, esto ayuda a juntar información del tratamiento de datos.

Además, otra característica de un DLP es que, permite obtener informes del manejo que los usuarios dan a la información de la red, para mantener un control adecuado acerca del uso de la

información de la empresa u organización. En definitiva, estas son herramientas muy robustas y están al alcance de cualquier industria, lo que ha permitido generar un gran interés dentro de los SGSI en los departamentos de Ciberseguridad.

1.4.2. Análisis y estudio de la implementación de las plataformas DLP

De acuerdo con las publicaciones realizadas por Gartner (2020), en los últimos años las empresas líderes en el desarrollo e implementación de sistemas DLP son: *Symantec*, *ForcePoint*, Digital Guardian y, se ha evidenciado una mejora constante en las tecnologías *Data Loss Prevention* realizadas por *Intel Security* como, se muestra en la Figura 1.9 presentada a continuación:

Figura 1.9. Cuadrante de Gartner

Fuente: Gartner (2020, p. 1)

1.4.3. Herramientas DLP Opensource

El coste de las herramientas DLP de grandes fabricantes, abre la posibilidad de un estudio definido acerca de las soluciones *opensource* como una posible estrategia o recurso más económico a la prevención de fuga de la información. Entre las principales soluciones tenemos:

a) **OpenDLP:** Es un *software* de código abierto que permite realzar diversas técnicas de control como, búsquedas masivas de la información en varios equipos al mismo tiempo sin consumir una gran cantidad de recursos, además, brinda la opción inspeccionar los contenidos de cada uno de los ficheros, consta de una interfaz GUI Web, como, se muestra en la Figura 1.10 presentada a continuación:

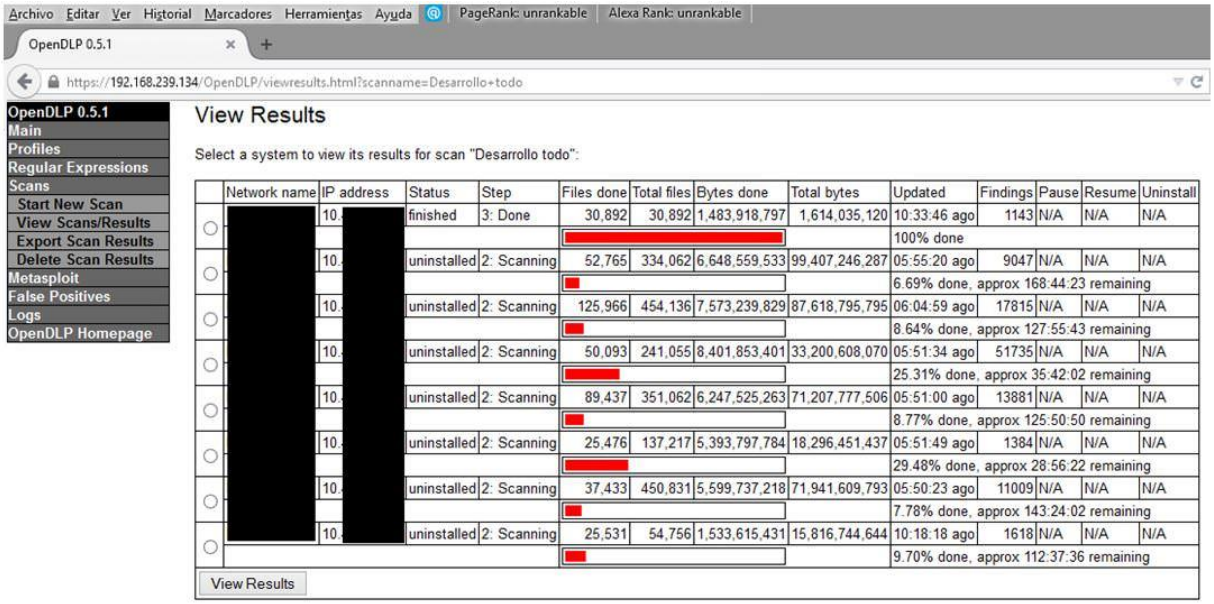


Figura 1.10. Interfaz OpenDLP

Fuente: Armado (2015)

OpenDLP realiza básicamente 3 tipos de búsquedas:

1) Búsquedas sin despliegue de un agente de ficheros en la maquina objetivo

2) Búsquedas mediante el despliegue de agente en la máquina remota.

3) Búsqueda sin despliegue de agente en bases de datos Mysql y MSSQL.

CAPÍTULO II. DISEÑO METODOLÓGICO

2.1. Caracterización de la institución

La Pontificia Universidad Católica del Ecuador, es una institución dedicada a la educación superior, en la actualidad es la universidad privada más antigua del país y está en el ranking de las mejores universidades a nivel latinoamericano en conjunto con la Universidad San Francisco de Quito y la Escuela Politécnica Nacional. La PUCE fue fundada en el año 1946 por la Compañía de Jesús, cuenta con sedes en diferentes regiones del Ecuador, es la Sede Ambato el recinto universitario en el cual, se aplicará el tema de investigación planteado en este documento.

La PUCE Sede Ambato fue creada en el año de 1986, con el objetivo de brindar una educación superior de alto nivel a toda la zona centro del país, se encuentra ubicada en la Av. Manuelita Sáenz, sector el tropezón. Cuenta con una amplia oferta académica con más de 20 carreras entre pregrado, posgrado y cursos abiertos, entre las cuales, se destacan áreas administrativas, técnicas, y de salud, donde busca mantener el legado de San Ignacio de Loyola "Ser más para servir mejor".

- **Misión**

En la página WEB institucional, la PUCE Sede Ambato (2020) manifiesta que, la misión de la institución es:

a) Es una comunidad académica que, modo riguroso y crítico, contribuye a la tutela y desarrollo de la dignidad humana y de la herencia cultural mediante la investigación, la docencia y los diversos servicios ofrecidos a las comunidades locales, nacionales e internacionales.

b) Presta particular atención a las dimensiones éticas de todos los campos del saber y del actuar humano, tanto a nivel individual como social. En este marco, propugna el respeto a la dignidad y derechos de la persona humana y sus valores trascendentes, apoya y promueva la implantación de la justicia en todos los órdenes de la existencia, promueve la preservación del medio ambiente y el respeto a la vida.

c) Goza de la autonomía a su condición de universidad, que le es necesaria para cumplir sus funciones eficazmente. Ejerce dicha autonomía con responsabilidad, y consiguientemente cumple con la rendición social de cuentas, tal y como lo determina la ley.

d) Garantiza a sus miembros la libertad académica, salvaguardando los derechos de la persona y de la comunidad dentro de las exigencias de la verdad y del bien común.

e) Dirige su actividad hacia la formación integral del ser humano. Por ello trata de formar a sus miembros intelectual y éticamente para el servicio a la sociedad en el ejercicio profesional y en el compromiso con el desarrollo sustentable del país.

f) Pretende la integración del saber mediante el examen de la realidad con los métodos propios de cada disciplina académica y propiciando, al mismo tiempo, el diálogo entre estas para que se enriquezcan mutuamente.

g) Promueve el compromiso de todos los miembros de la comunidad universitaria para la consecución de los fines institucionales a través del diálogo y la participación, de la conformidad con el presente Estatuto.

h) Como universidad particular ofrece una alternativa específica en el ámbito académico conforme a su propio Estatuto y reglamentos.

i) Como universidad católica, se inspira en los principios cristianos ante Dios, el respeto a la dignidad y derechos de la persona humana y a sus valores trascendentales; apoya y promueve la implantación de la justicia en todos los órdenes de la existencia; propicia el diálogo de las diversas disciplinas con la fe, la reflexión sobre los grandes desafíos morales, religiosos y la praxis cristiana.

- **Visión**

El recinto universitario tiene como visión:

La Pontificia Universidad Católica del Ecuador Sede Ambato (PUCESA), es el referente nacional en formación integral e inclusiva con impacto social. La innovación, agilidad y compromiso identifican su cultura organizacional. Es reconocida internacionalmente por su producción científica y la calidad de sus estudiantes y docentes. (PUCE Sede Ambato, 2020, p. 1)

Es necesario resaltar que la sede consta con alrededor de 300 colaboradores entre personal administrativo, de servicios y planta docente, además, debido al prestigio y la amplia oferta académica que la universidad mantiene, ha permitido a la misma contar con alrededor de 2000 estudiantes distribuidos en todas las carreras ofertadas. Esto, no se podría mantener si, no se constituyera de un marco legal estructurado de acuerdo con las necesidades que el recinto educativo mantiene. En la Figura 2.1 se aprecia el organigrama que mantiene le PUCE Sede Ambato:

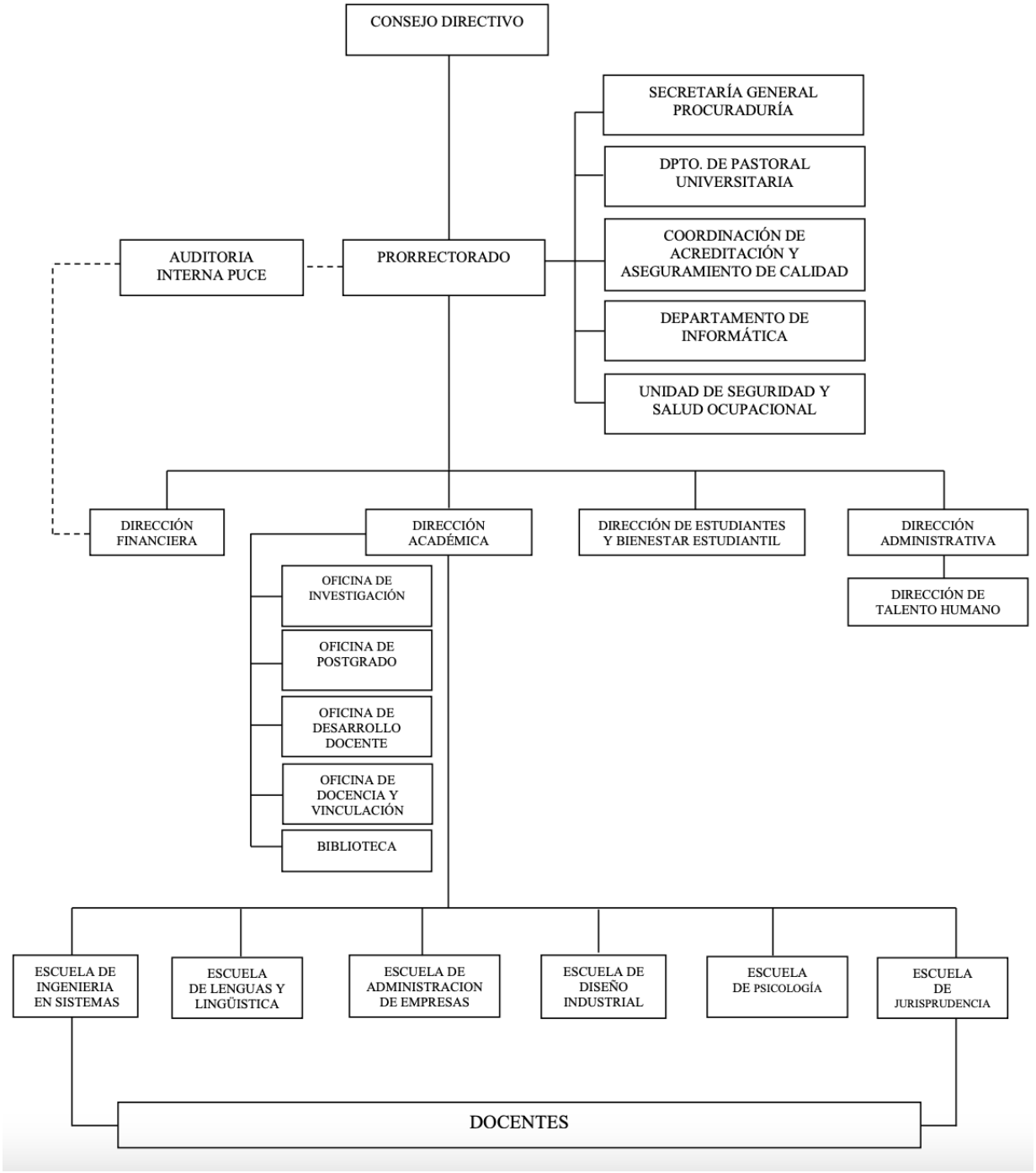


Figura 2.1. Organigrama funcional PUCE Sede Ambato

Fuente: PUCE Sede Ambato (2018)

Como, se evidencia, acorde al organigrama funcional que tiene la Universidad, existe una diversa cantidad de información de cada uno de los colaboradores y estudiantes de la PUCESA, esta realidad evidencia el riesgo que, se presente una fuga de información sensible en cualquier área. El departamento de Tecnologías de la Información consciente de esta amenaza latente busca en forma periódica nuevos métodos para protección a los servidores y equipos de comunicación que cuenta la Infraestructura Tecnológica de la Institución, entre estos métodos, se ha evidenciado la necesidad de realizar pruebas con plataformas *Data Loss Prevention* para brindar un nivel adicional a la confidencialidad del Sistema de Gestión de la Seguridad de la Información.

2.2. Argumentación de la metodología de investigación

El proyecto de investigación busca proteger la Confidencialidad de los datos de la Pontificia Universidad Católica del Ecuador Sede Ambato, a fin de disminuir el riesgo de fuga de información sensible que esta posee en sus bases de datos, a través de la implementación de un DLP, el documento contiene una variada metodología de investigación y, se basa en los métodos detallados a continuación:

Método Inductivo: Según el criterio de Abreu (2014) asegura que "el método inductivo plantea un razonamiento ascendente que fluye de lo particular o individual hasta lo general. Se razona que la premisa inductiva es una reflexión enfocada en el fin" (p. 6). A través de este método, se busca conocer las características generales de la información digital que posee la PUCESA. Además, gracias al uso de este método, se tiene como objetivo elaborar la propuesta de la herramienta prototipo *Data Loss Prevention OpenSource*, para prevenir la fuga de los datos.

Este método está relacionado con el planteamiento de los Ítems de la Norma ISO 27001 para definir los riesgos y vulnerabilidades, estos según el estado del arte explicado en el capítulo I del presente estudio manifiesta los tres pasos para el análisis de los riesgos, mismos que son: Clasificación, Manipulación y Etiquetado de la información.

Método cualitativo: Este método está orientado a una recopilación de información, por lo general, se usa en estudios basados en una investigación del estado del arte, se considera importante el uso de esta metodología para comprender la importancia de la información que la PUCESA a través de una entrevista a las autoridades que manejan los datos sensibles de la institución.

Acorde a lo mencionado la entrevista está contenida por dos partes, a fin de obtener una justificación técnica-gerencial, se detalla a continuación la encuesta realizada a las autoridades administrativas de la PUCESA. Esta entrevista consta de cuatro preguntas las cuales tienen su enfoque orientado al Área de la persona entrevistada.

En la tabla 2.1 presentada a continuación, se evidencia los resultados de la pregunta 1 de la entrevista realizada a las autoridades de la Universidad, la cual está orientada al robo de la información dentro del recinto universitario:

Tabla 2.1. Fuga de información

Pregunta 1: ¿Sabe usted, si la PUCE Sede Ambato ha sido víctima de algún ataque informático o robo de información?
R1: SI **Comentario:** Es un tema de alta preocupación
R2: SI **Comentario:** Si se ha puesto en riesgo la seguridad de algunas máquinas en la Institución, no sé si de manera consciente o accidental
R3: SI **Comentario:** Contesto que sí, porque se ha escuchado que en alguna ocasión se había borrado información de la PUCESA, cuando uno de los compañeros salió de la Institución o que puedan ponerse claves de no acceso a la información.
R4: NO **Comentario:** La protección de información es fundamental en toda Institución, representa una ventaja competitiva.

Análisis: Acorde a las respuestas manifestadas por parte de las autoridades de la PUCE Sede Ambato, se evidencia algún tipo de fuga de información, a pesar de no tener la certeza si la fuga de información fue de forma intencional o accidental, es un tema que preocupa a las personas responsables del recinto educativo.

Fuente: elaboración propia

La segunda pregunta de la entrevista realizada tiene por objetivo obtener una idea clara acerca de que piensan las autoridades administrativas acerca de la información digital sensible que, se encuentra vulnerable en la institución. Los resultados, se evidencian a continuación:

Tabla 2.2. Información digital sensible vulnerable

Pregunta 2: ¿Considera usted que la PUCE Sede Ambato maneja información sensible que no se encuentra protegida?
R1: SI **Comentario:** Siempre existe la posibilidad de ataques informáticos, en vista del rápido avance de la tecnología
R2: SI **Comentario:** Creo que en todas las Instituciones hay información sensible que debe protegerse; porque la alteración, pérdida o destrucción puede causar daños; se considera que la pérdida de información puede ser accidental o malintencionada.
R3: SI **Comentario:** Específicamente de la seguridad interna, por cuanto podría darse el caso de que algún funcionario descontento filtre información hacia fuera de la Institución.
R4: SI **Comentario:** La PUCE Sede Ambato maneja información Académica, esta es susceptible de plagio o copia de tareas, investigaciones; si bien no sería externo el interés, se puede correr el riesgo de estos perjuicios entre estudiantes, docentes o empleados.

Análisis: Acorde a los aportes generados por los entrevistados se concluye que, uno de los riesgos latentes que presenta la PUCE Sede Ambato quizá al igual que cualquier otra institución pública o privada, es la falta de seguridad a la información digital ante amenazas internas.

Fuente: elaboración propia

La tercera pregunta hace referencia acerca de las amenazas presentes en la información digital que maneja la PUCE Sede Ambato, la misma tiene por objetivo ver la necesidad de emplear métodos de prevención ante ataques a la confidencialidad de los datos. Las respuestas, se detallan a continuación:

Tabla 2.3. Prevención de fuga de información digital

Pregunta 3: ¿Piensa usted que la PUCE Sede Ambato, mantiene una amenaza presente de fuga de información digital sensible?
R1: SI **Comentario:** Fortalecer la seguridad.
R2: SI **Comentario:** Mantener políticas y procedimientos claros. Diseñar estrategias de concientización sobre la responsabilidad en el manejo de información.
R3: SI **Comentario:** Actualizar constantemente los sistemas o herramientas de seguridad que permita un mayor resguardo de la información de la Universidad.
R4: SI **Comentario:** Aplicación técnica de resguardo de la información, mantener actualizadas licencias, procesos que se mantienen en la actualidad, pero es una actividad continua y permanente.
Análisis: En base a las respuestas por parte de los entrevistados se evidencia una clara necesidad de la implementación de métodos y técnicas dedicadas a proteger la información

digital sensible. Además, se destaca la clara preocupación por parte de las autoridades acerca de la vulnerabilidad presente.

Fuente: elaboración propia

La cuarta pregunta tiene como finalidad, justificar la necesidad de implementación de herramientas *Data Loss Prevention*, dentro del recinto educativo con el fin de disminuir los riesgos de fuga de información. Los aportes entregados por parte de las autoridades institucionales, se evidencian en la Tabla 2.4:

Tabla 2.4. Implementación herramientas *Data Loss Prevention*

Pregunta 4: Considera usted que es importante el diseño de un prototipo Data Loss Prevention (herramienta para prevenir fuga de información digital sensible).
R1: SI **Comentario:** No conozco del tema, pero imagino que puede ayudar a prevenir.
R2: SI **Comentario:** Si se debiera contar con herramientas, que puedan proteger la información de la Institución; la misma puede caer en manos de la competencia. Nuestra actividad como universidad es bastante sensible. Como se mencionaba anteriormente puede darse incidentes provocados para filtrar información, llevarse a cabo para diferentes fines.
R3: SI **Comentario:** Porque es bueno contar con la mayor cantidad de herramientas informáticas que resguarden la información, más aún cuando existen hackers (personas o empresas externas) que buscan acceder a sistemas informáticos no solo de las universidades sino incluso de cuentas personales con la finalidad de robar o modificar su información.
R4: SI

Comentario: El desarrollo de herramientas informáticas propias garantiza la aplicación de lo que la Institución necesita y la confidencialidad de la información a la que el técnico accede.
Análisis: En conclusión, con los comentarios dichos por las autoridades de la institución, se evidencia la gran acogida al prototipo de una herramienta *Data Loss Prevention* como un primer método de seguridad a la prevención o fuga de información sensible.

Fuente: elaboración propia

Una vez analizados los resultados de la entrevista realizada a las autoridades de la PUCE Sede Ambato, es importante considerar también, la visión desde un aspecto técnico. Esta encuesta está orientada al director del Departamento de TI como máxima autoridad y al Especialista de Comunicaciones e Infraestructura, persona encargada de mantener las comunicaciones del recinto universitario.

La pregunta técnica 1 está orientada a conocer de forma breve, con que herramientas tecnológicas cuenta la PUCESA para proteger la información digital sensible que administra. Los resultados, se aprecian en la Tabla 2.5 presentada a continuación:

Tabla 2.5. Plataformas de seguridad para la infraestructura tecnológica

Pregunta 1: ¿Cuenta la PUCE Sede Ambato con una infraestructura tecnológica proteger sus aplicativos y sistemas de comunicación?
R1: SI **Comentario:** La PUCESA, a través del Dpto. de Tecnología procura trabajar sus proyectos anuales en función de la seguridad informática, por ello implementa nueva infraestructura tecnológica y mejora la existente a través del manejo de: Controlador de Dominio Firewall Perimetral Firewall de Publicaciones de Aplicaciones

Sistema Antivirus Sistema de Respaldos, entre otros.
R2: SI **Comentario:** Firewall Perimetral Firewall de Publicaciones de Aplicaciones Sistema Antivirus Controlador de Dominio Sistema de Respaldos.
Análisis: Como se evidencia en las respuestas presentadas por los participantes, la PUCESA cuenta con varias plataformas de seguridad, esto disminuye el riesgo ante amenazas externas a la organización, sin embargo, la institución no cuenta con mecanismos de protección internas para la información digital sensible.

Fuente: elaboración propia

La pregunta técnica 2 tiene como finalidad, conocer si el departamento de TI cuenta con una política de seguridad implementada dentro de su SGSI, los resultados de la pregunta lo evidenciamos en la Tabla 2.6:

Tabla 2.6. Políticas de seguridad dentro del SGSI

Pregunta 2: ¿Existe alguna norma/estándar o política de seguridad para la protección de información digital con la finalidad de que, esta no sea vulnerada?
R1: SI **Comentario:** El Dpto. de Tecnología actualmente no cuenta con una política de seguridad estandarizada, fruto de ello y según el informe 2018 de Auditoría Interna de la PUCE, se ha solicitado la elaboración de una política de seguridad que se ajuste al contexto de nuestra Sede, sin embargo, dada la pandemia desde marzo 2020, ha sido un tanto difícil ajustar dichos estándares a la nueva normalidad. No obstante, se trabaja en su elaboración

actualmente como parte de un POA 2020, pero de manera independiente y no en la generalidad a nivel de PUCE.
R2: NO **Comentario:** No se cuenta con normas aprobadas por las autoridades Institucionales, pero se cuenta con normas a nivel de departamento, además; se está trabajando en la elaboración de la Política de Seguridad de la Información, a fin de que sea aprobada por las autoridades respectivas.
Análisis: Acorde con lo expuesto, la institución tiene una política de seguridad en desarrollo con el fin de mantener un correcto tratamiento a la información digital. Esto permite una realización de pruebas en base a los datos sensibles de la Universidad.

Fuente: elaboración propia

La pregunta técnica 3, orienta en la necesidad de una auditoría externa a fin de conocer las vulnerabilidades que la infraestructura tecnológica mantiene, para de esta forma mejorar la seguridad de la institución. Los resultados, se evidencian en la Tabla 2.7 presentada a continuación:

Tabla 2.7. Auditoria externa

Pregunta 3: ¿Considera usted la importancia de una auditoría externa que, permita el hallazgo de vulnerabilidades a fin de mejorar la protección de la información?
R1: SI **Comentario:** Siempre el apoyo de una instancia externa en la labor de seguridad informática en la búsqueda de hallazgos de vulnerabilidades es muy importante, siempre y cuando éstas garanticen su prestigio, evidencien un nivel de tratamiento superior e imparcial y guarden la debida confidencialidad del caso.
R2: SI

Comentario: Las auditorías externas son un buen punto para determinar las brechas de seguridad, en las cuales, se mejoraría.
Análisis: Las personas responsables de la seguridad de la información consideran importante mejorar la seguridad de la información mediante técnicas de protección, como es el caso de una auditoría externa, esto pone en manifiesto la preocupación del Departamento de TI por brindar una mejor protección a los datos.

Fuente: elaboración propia

La pregunta técnica 4, justifica la necesidad de implementación de una herramienta DLP, para proteger la confidencialidad de la información dentro de la PUCE Sede Ambato, los resultados, se evidencian en la Tabla 2.8:

Tabla 2.8. Herramientas DLP dentro de la PUCE Sede Ambato

Pregunta 4: ¿Piensa que el departamento de Tecnologías de la Información debe hacer énfasis en prevenir el manejo indebido de la información sensible de la PUCE Sede Ambato, mediante herramientas *Data Loss Prevention*
R1: SI **Comentario:** Toda herramienta tecnológica de seguridad informática en este caso un DLP, que aporte en el objetivo común de precautelar la seguridad, integridad y confidencialidad de datos e información, sería bien acogida por el Dpto. de Tecnología, para garantizar la confianza en el uso y manejo de información por parte de nuestros usuarios internos y externos de la PUCESA.
R2: SI **Comentario:** Es muy importante, actualmente se desconoce el nivel de fuga de información que existe, no solo a nivel administrativo, sino a nivel Docente y Autoridades. El disponer de un DLP sería un termómetro para medir el nivel de fuga existente.
Análisis: El departamento de TI, a través de los responsables de proteger la información digital de la PUCE Sede Ambato, muestran un claro interés en el uso de herramientas DLP a

fin de garantizar una mejor confidencialidad de los datos de los usuarios dentro de la institución.

Fuente: elaboración propia

Método Deductivo: Una vez obtenidos los resultados de las entrevistas realizadas a las autoridades de la PUCESA, se hace uso del método deductivo para realizar el análisis y la justificación de la necesidad para implementar un prototipo de *Data Loss Prevention* dentro del departamento de Tecnologías de la Información, acorde al criterio de Abreu (2014) indica que "el método deductivo permite determinar las características de una realidad particular que, se estudia por derivación o resultado de los atributos o enunciados contenidos en proposiciones o leyes científicas de carácter general formuladas con anterioridad" (p. 6).

En concordancia con ello, se resalta los factores importantes que esta metodología usa, para evidenciar las vulnerabilidades de los activos de la información, acorde a los manifiestos de la normativa ISO 27001.

Método mixto transversal: El trabajo de titulación tiene además un enfoque mixto-transversal, debido a que la investigación consta de los siguientes pasos que son: recolección de datos para el estudio del estado del arte, análisis de *software* para la implementación del prototipo, y realización de pruebas. Todos estos pasos fueron realizados en un determinado tiempo el cual, se detalla en la Figura 2.2 mostrada a continuación:

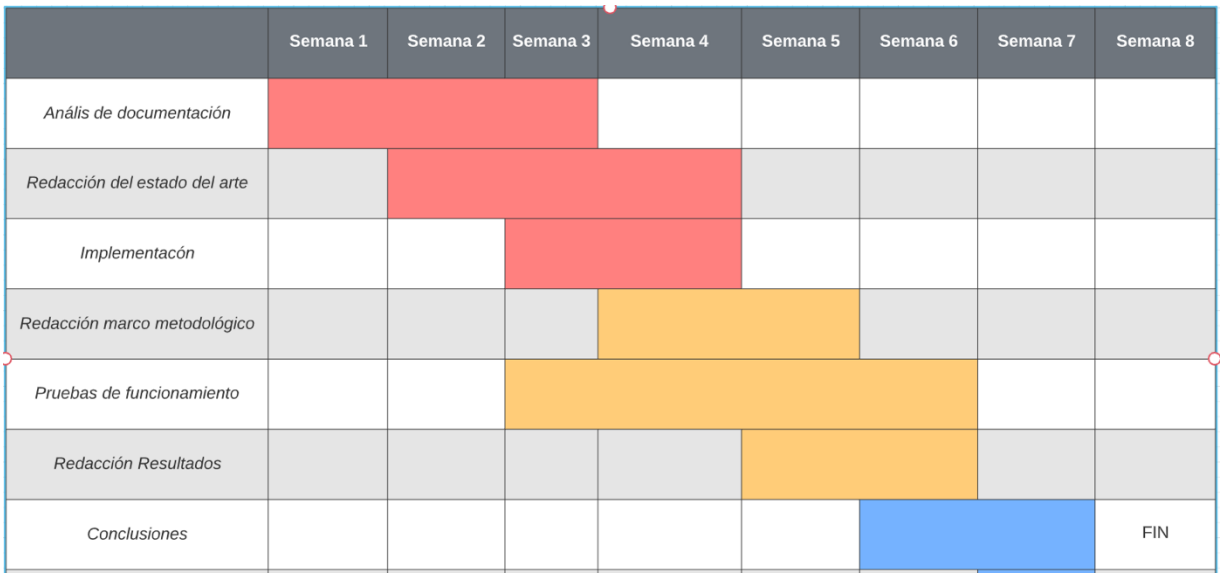


Figura 2.2. Uso del método mixto transversal para planificación

Fuente: elaboración propia

Método cuasi experimental: Este método, se usa para la realización de pruebas y análisis de resultados, es importante destacar que, la investigación hace uso de este método debido a la falta de control en todas las variables que en este caso es la información. Se considera importante el uso de esta metodología por la sencillez de esta, en el momento de la realización de las pruebas.

2.3. Implementación del prototipo *Data Loss Prevention*

Para la implementación del prototipo, y a fin de realizar una implementación de forma ordenada, se hizo uso del ciclo de *Deming*. Según el criterio de Ocrospoma (2017) manifiesta que "la filosofía de este ciclo lo hace de gran utilidad para perseguir la mejora mediante diferentes metodologías. En general, para cumplir efectivamente el ciclo PHVA, es clave usar las herramientas básicas" (p. 36).

Este ciclo consta de cuatro etapas conocidas como PDCA (por sus siglas en inglés *Plain, Do, Check, Act*) cuyo significado es: Planificar, Hacer Verificar y Actuar. Para un mejor entendimiento, se aprecia la Figura 2.3 la cual detalla las acciones realizadas por cada etapa.

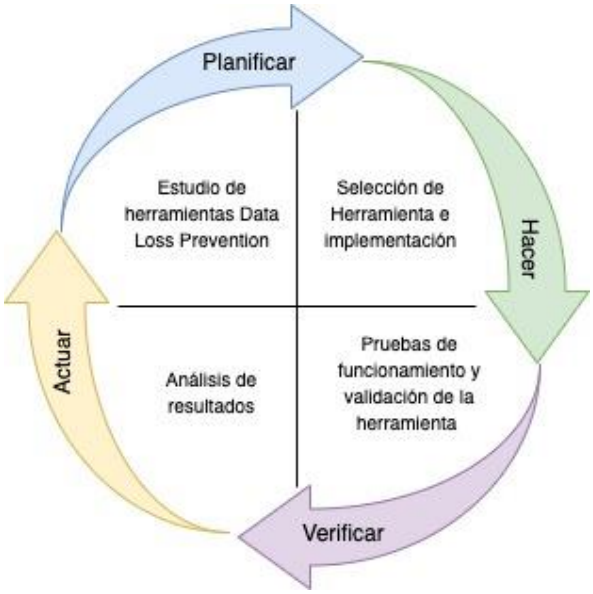


Figura 2.3. Ciclo de Deming

Fuente: elaboración propia

2.3.1. Selección de herramienta

Para la selección de la herramienta, se realiza un análisis comparativo entre diferentes plataformas y seleccionar la que mejor, se adapte a los requerimientos para la implementación del prototipo *Data Loss Prevention OpenSource*, para esta selección, se considera los siguientes requerimientos:

- **Licenciamiento Gratuito:** A fin de disminuir costos en el diseño del prototipo DLP, se evidencia la necesidad de que, la herramienta sea de licenciamiento Opensource.
- **Documentación:** La plataforma requiere de variada documentación para una correcta implementación y realización de pruebas.
- **Compatible con GNU Linux:** Existen muchas herramientas DLP en el mercado, pero la gran parte de ellas corren sobre Windows Server, un requerimiento

importante es que, al ser una plataforma de tipo Opensource tiene que ser compatible con GNU Linux.

- **Soporte y actualización:** La plataforma necesita contar con soporte y actualizaciones para mantener una robustez en el sistema.

Cada requerimiento posee una calificación que varía entre 1, si cuenta con la especificación y en caso contrario su nota será 0. Esto, se realiza con el objetivo de seleccionar la herramienta que más, se adapte a los requerimientos del prototipo a implementarse. El análisis y selección de la herramienta, se aprecia en la Tabla 2.9 presentada a continuación:

Tabla 2.9. Selección de *software*

Plataforma	Licenciamiento Gratuito	Documentación	Compatible con GNU Linux	Soporte y actualización	Total
Dlp Symantec	0	1	0	1	2
Dlp Digital Guardian	0	1	0	1	2
Opendlp	**1**	**1**	**1**	**1**	**4**
Mydlp	0	1	1	1	3
Dlp Force Point	1	1	0	0	2

Fuente: elaboración propia

Como, se evidencia en la Tabla 2.9 de selección las herramientas *Data Loss Prevention* que lideran el cuadrante de Gardner no son de licenciamiento gratuito, esto limita las pruebas de investigación. Sin embargo, la herramienta seleccionada es *Opendlp*, un *software OpenSource* compilado en GNU *Linux Ubuntu*, esta plataforma posee todas las especificaciones necesarias para la implementación y realización de pruebas en el prototipo a implementar. Cabe resaltar

que, el trabajo de titulación busca brindar una solución *OpenSource* de costos reducidos, para aquello la virtualización de la herramienta será en *Virtual Box.*

2.3.2. Implementación de plataforma

- *Descarga de Ubuntu:* En la página de OpenDLP, se procede con la descarga de la versión servidor, para disminuir el consumo de recursos de *hardware* en las pruebas a realizarse. Esta descarga, se evidencia en la Figura 2.4

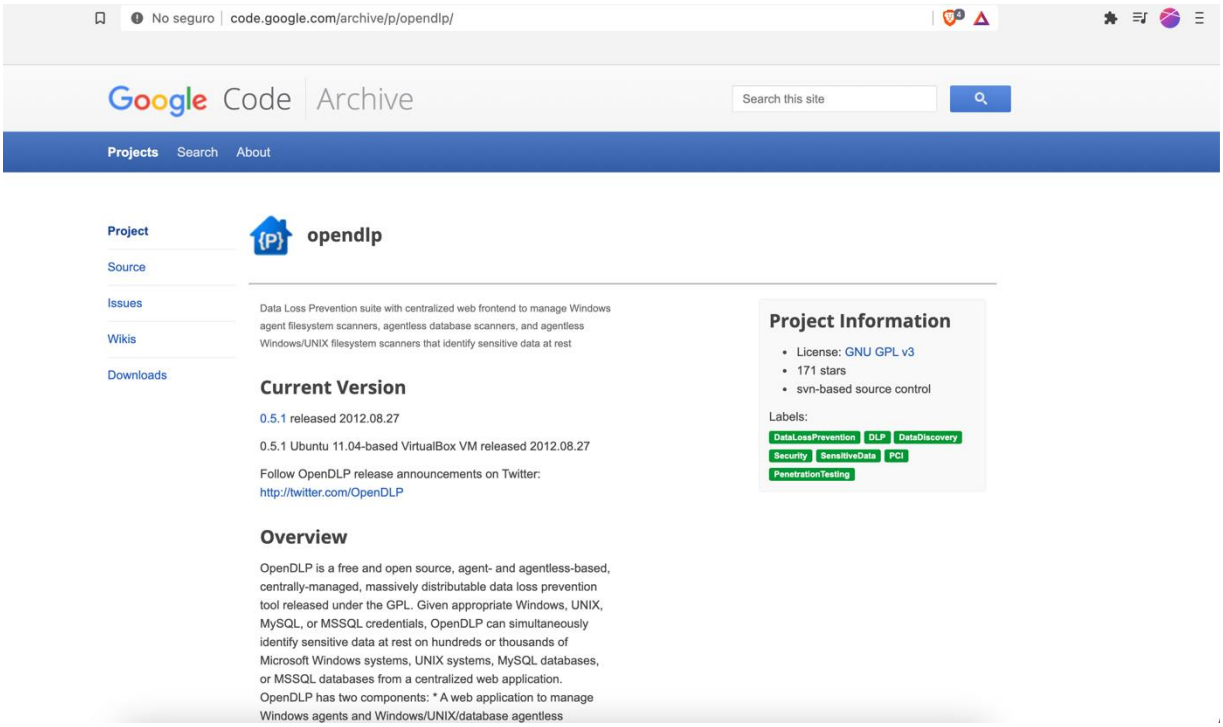


Figura 2.4. Descarga de OpenDLP

Fuente: elaboración propia

- **Descarga de *VirtualBox:*** Este *software*, se descarga de la página oficial, como, se manifiesta en el apartado anterior, se hace uso de esta herramienta por ser una plataforma de virtualización de licenciamiento gratuito. La descarga, se evidencia en la Figura 2.5:

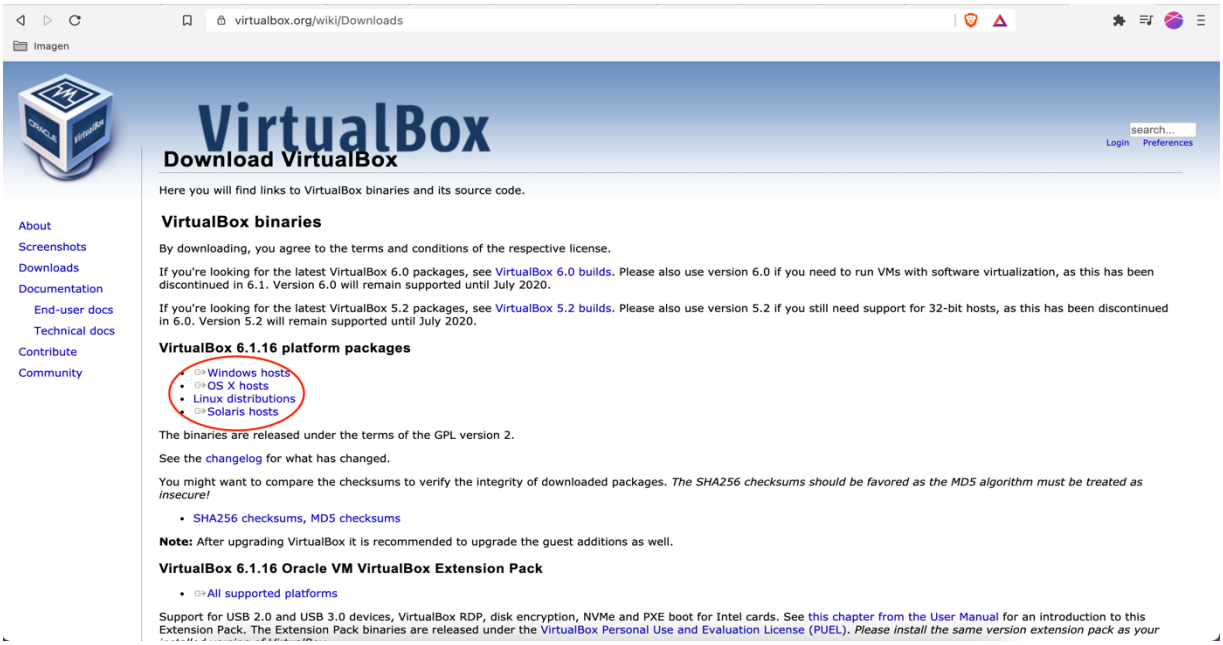


Figura 2.5. Descarga de Virtual Box

Fuente: elaboración propia

Para que Opendlp funcione de manera correcta hay que descargar el *plugin Extension Pack*, caso contrario, se tendrá inconvenientes en la virtualización del *software*, esta opción, se encuentra en la parte inferior de la página oficial, como se evidencia en la Figura 2.6:

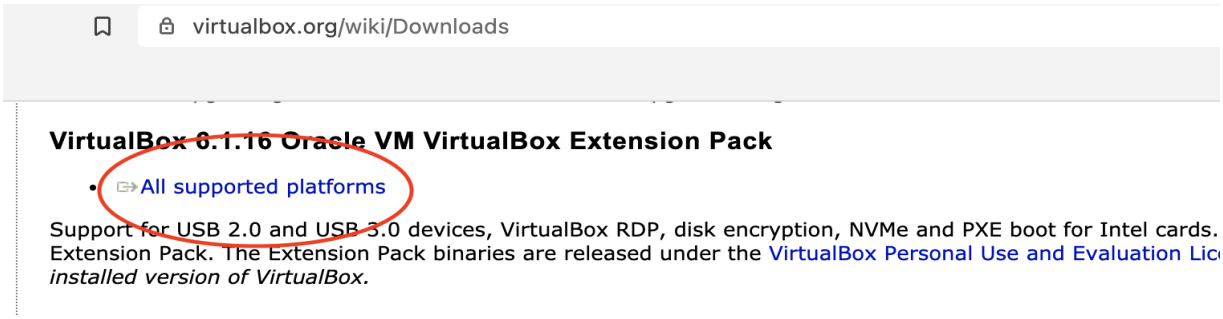


Figura 2.6. Descarga Extension Pack de VirtualBox

Fuente: elaboración propia

- **Virtualización:** Una vez descargado el archivo de OpenDLP, se ejecuta la plataforma de virtualización y abrir el archivo de extensión *ova*. Como, se evidencia en la Figura 2.7:

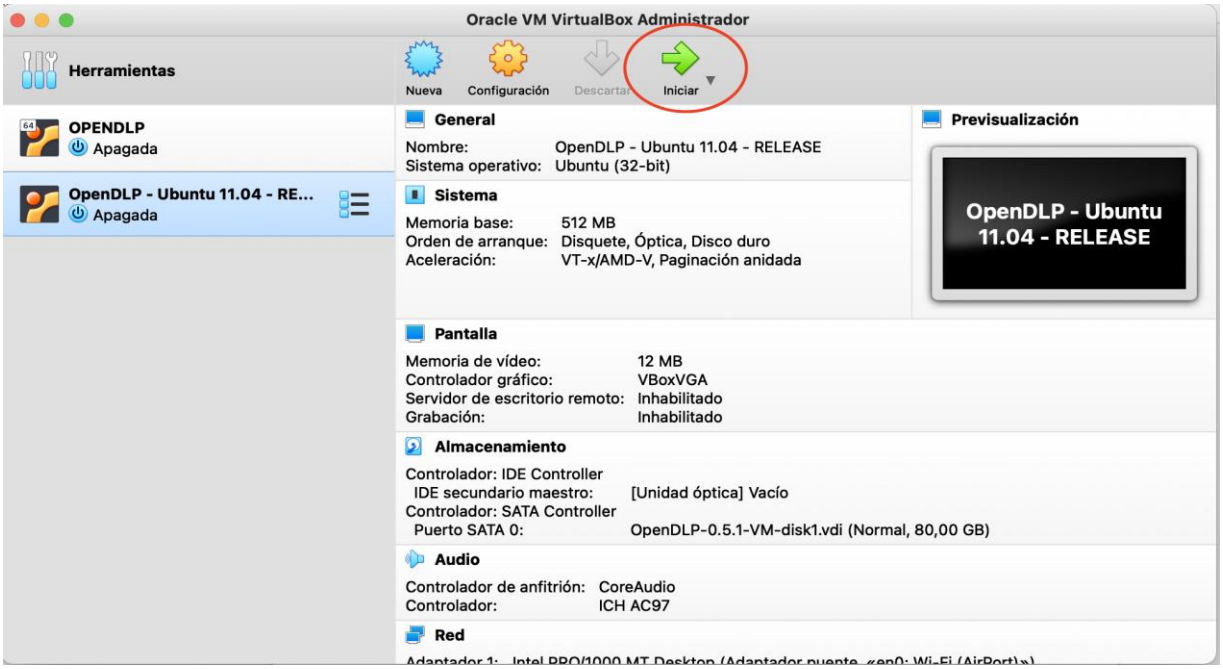


Figura 2.7. Inicio de OpenDLP

Fuente: elaboración propia

- **Configuración de Certificado de seguridad:** En la carpeta contenedora existe un certificado de seguridad con el nombre client.p12, este es un archivo de certificación para el uso de la herramienta y se, tiene que instalar en el navegador *web*. El archivo, se evidencia en la Figura 2.8 presentado a continuación:

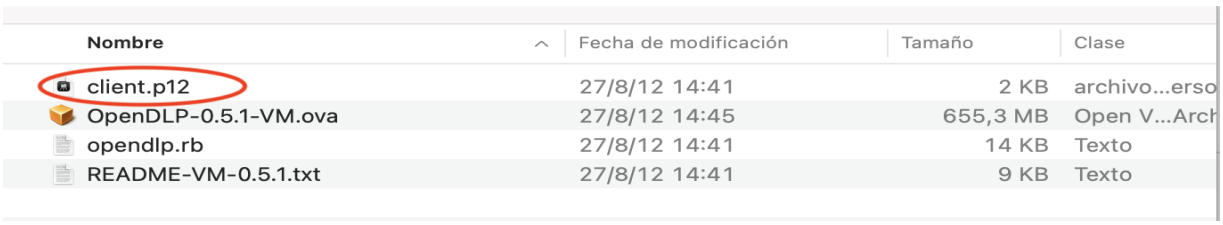


Figura 2.8. Certificado de confianza OpenDLP

Fuente: elaboración propia

En la Figura 2.9, se aprecia el certificado importado al navegador para la confirmación de la interfaz *web* del prototipo implementado:

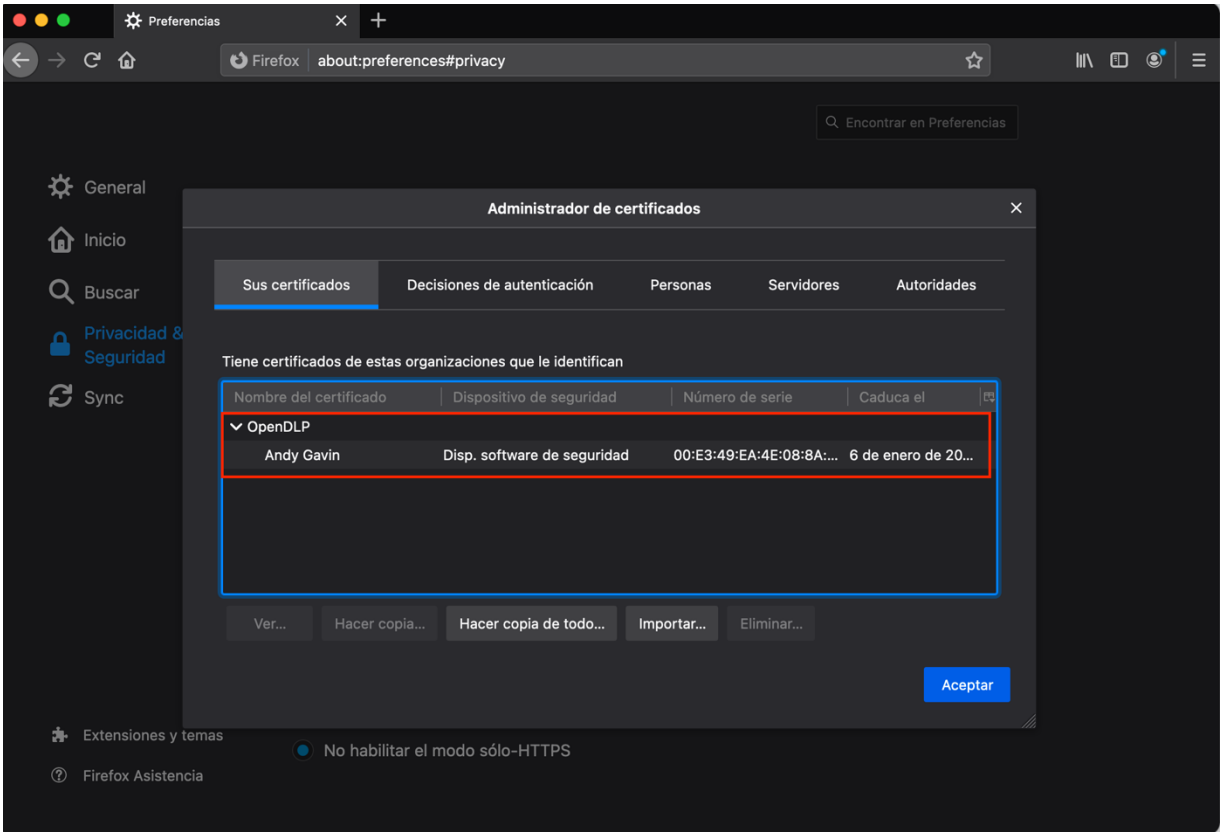


Figura 2.9. Importación del certificado OpenDLP

Fuente: elaboración propia

2.3.3. Pruebas de funcionamiento de la herramienta

Para validar que la herramienta, se encuentre en funcionamiento de manera correcta, es necesario verificar el *software* en modo consola como, se evidencia en la Figura 2.10 presentada a continuación:

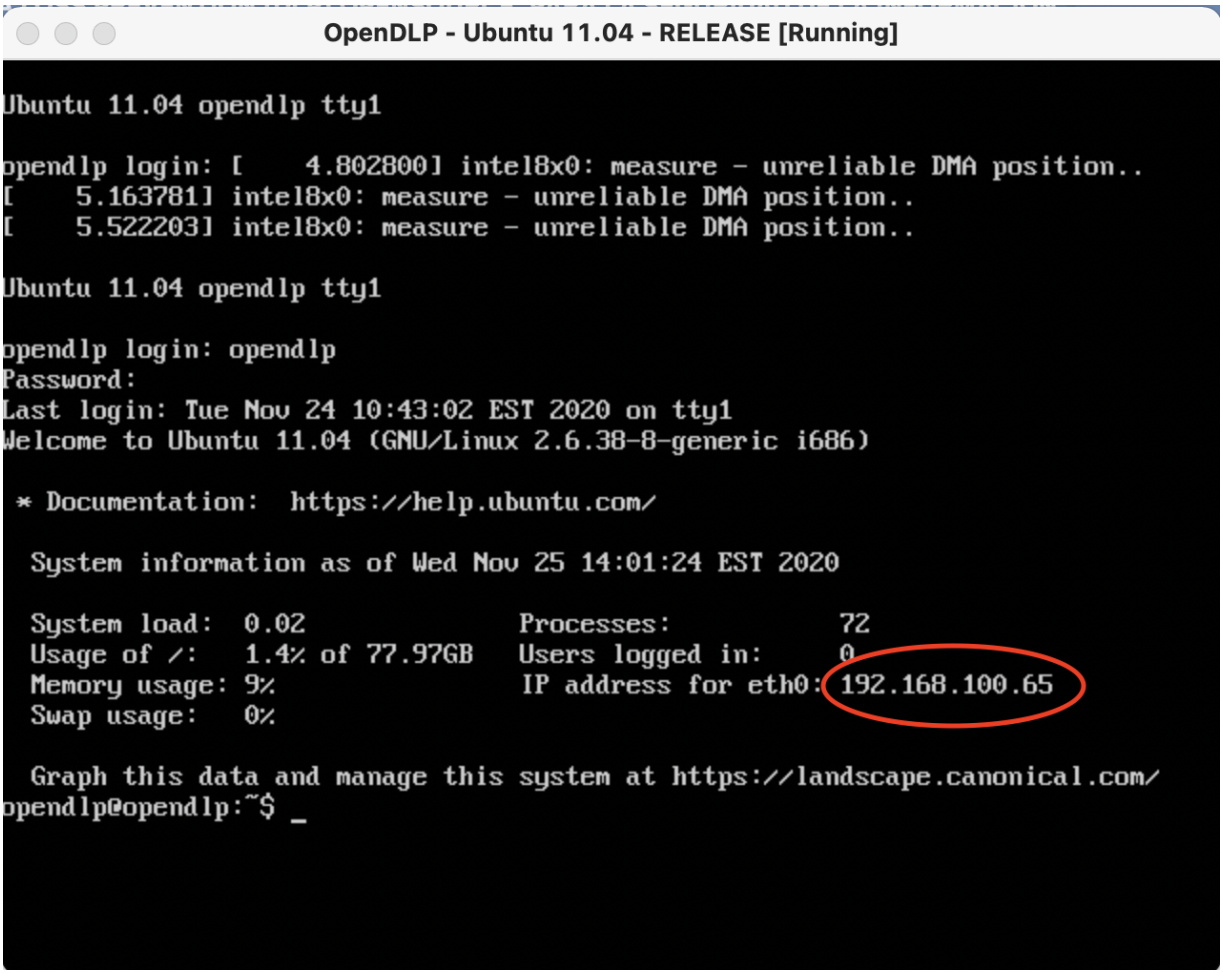


Figura 2.10. Interfaz prototipo OpenDLP virtualizado

Fuente: elaboración propia

Como, se evidencia en la Figura 2.11 una vez instalado el certificado, se obtiene el acceso al interfaz web a través de un usuario y contraseña:

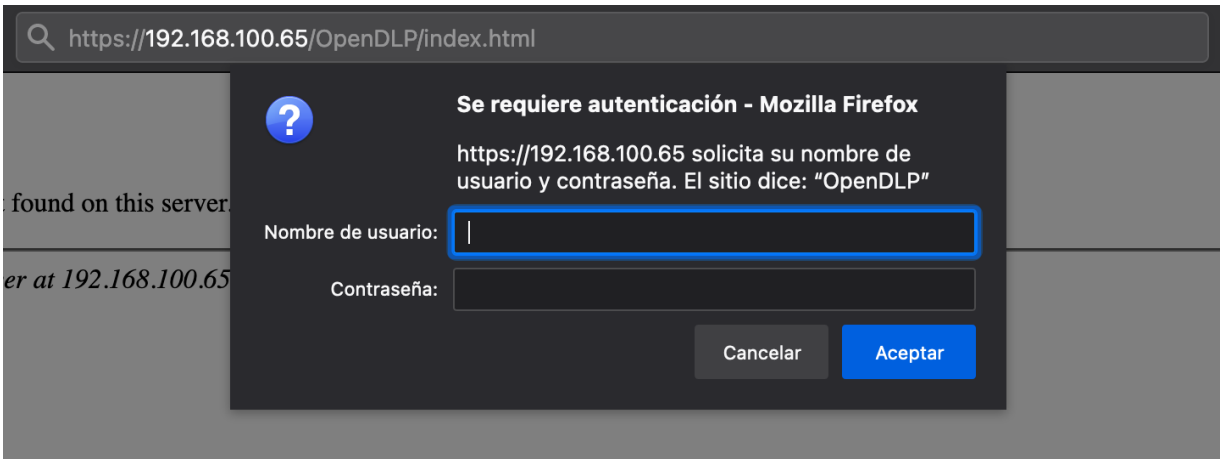


Figura 2.11. Ingreso a interfaz OpenDLP

Fuente: elaboración propia

En la Figura 2.12 presentado a continuación, se evidencia el interfaz *web* configurado y en funcionamiento de manera correcta del prototipo.

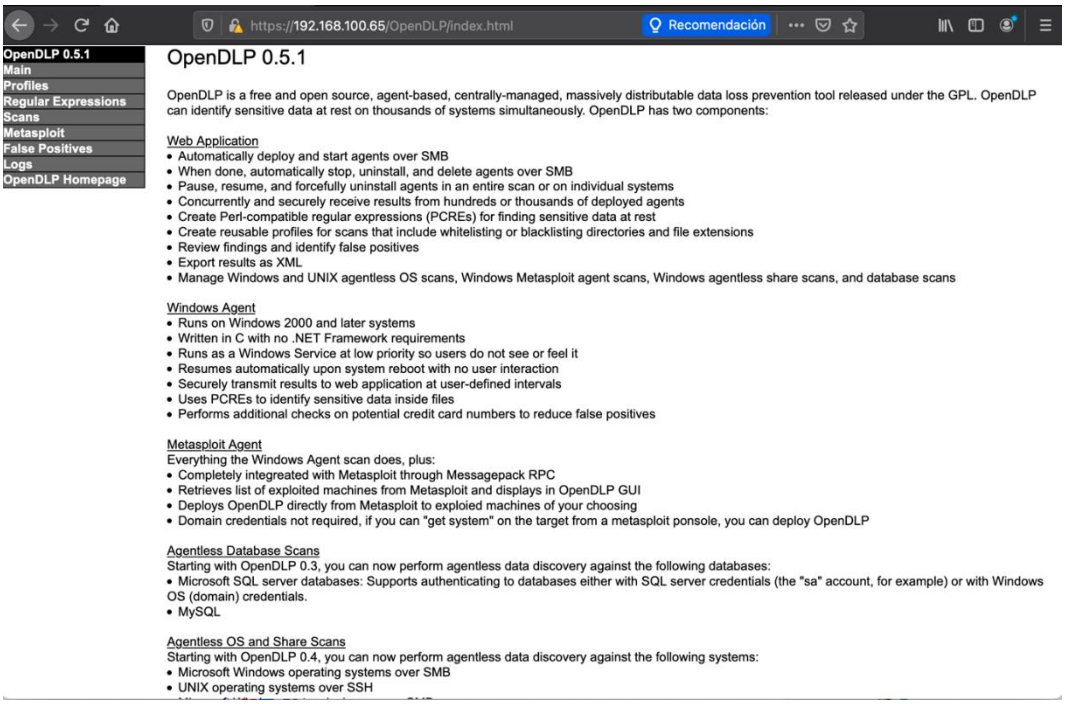


Figura 2.12. Interfaz prototipo OpenDLP

Fuente: elaboración propia

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

Una vez realizado el estudio de las herramientas DLP, y al culminar el análisis de funcionamiento de la plataforma OpenDLP, un *software* de tipo *OpenSource* usada en su mayor parte de tiempo en empresas con escenarios de prueba en ambientes controlados, se realiza la implementación y evaluación de la plataforma mencionada.

Estas pruebas están guiadas en las investigaciones de Acosta (2015) quien realiza pruebas de funcionamiento con la herramienta McAfee DLP *Endpoint* una plataforma de licenciamiento pagado, y la investigación de Ramos y Sierra ejecutada en el año 2017. Los estudios mencionados sirven de guía en las pruebas realizadas con OpenDLP, la cuales están realizadas bajo los siguientes parámetros:

- **Interfaz gráfica:** para una mejor administración de la plataforma.
- **Monitoreo de archivos por extensión:** Para analizar diferentes tipos de archivos que maneja un ordenador.
- **Monitoreo de base de datos:** Para una mejor supervisión de la data sensible que maneja la Pontificia Universidad Católica del Ecuador Sede Ambato, dentro de sus servidores y aplicativos.
- **Análisis programados:** A fin de automatizar el control y monitoreo del flujo de información en la red de datos del recinto universitario.
- **Control de flujo de datos:** A fin de restringir la salida de datos sensibles que posee la PUCE Sede Ambato
- **Resultados estadísticos:** Para un mejor entendimiento en los resultados generados por la plataforma.
- **Bajo consumo de recursos en *Hardware:*** Para un análisis de requerimientos de *hardware* para la instalación de la plataforma.

3.1. Prueba 1 Interfaz Gráfica:

OpenDLP cuenta con una interfaz gráfica de tipo *web*, esta funciona en cualquier navegador de internet, siempre y cuando tenga instalado el certificado digital de seguridad. Dentro de la página

encontramos las opciones que posee la plataforma. Esta interfaz, se evidencia en la Figura 3.1 mostrada a continuación:

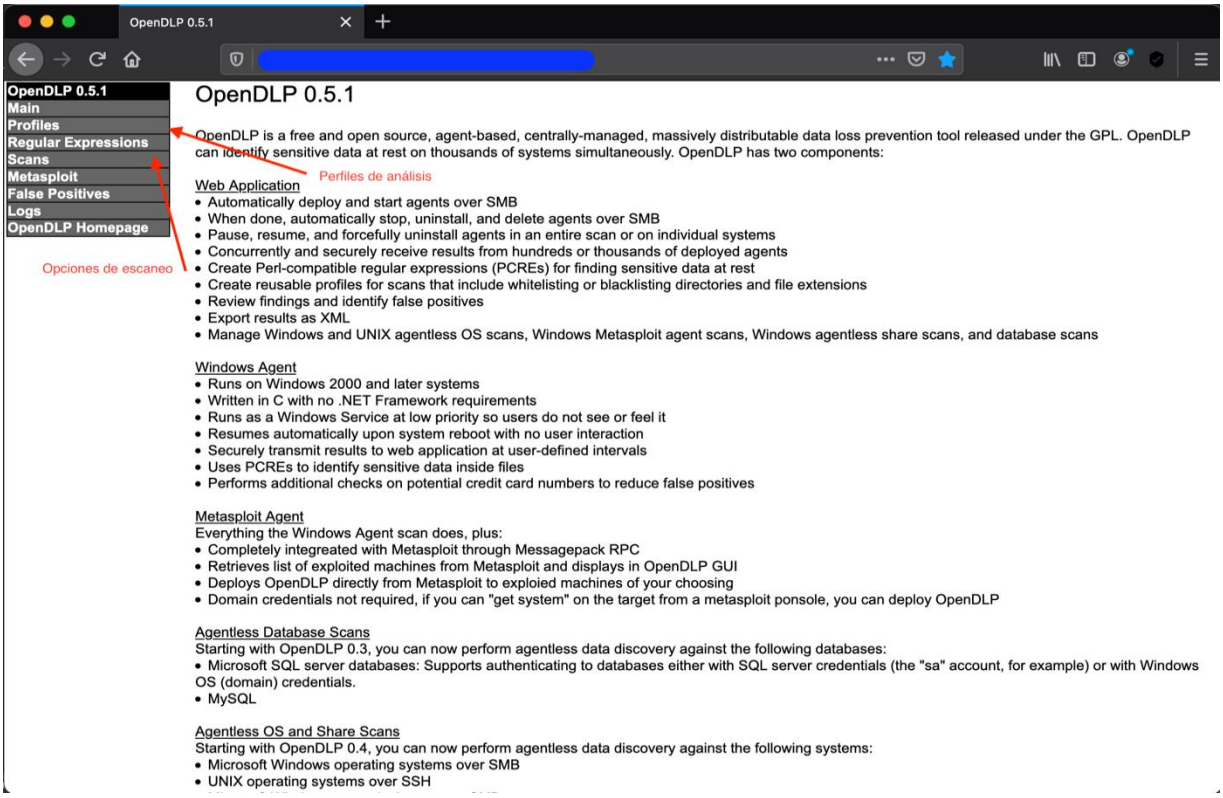


Figura 3.1. Interfaz Web en Firefox de OpenDLP

Fuente: elaboración propia

El certificado implementado se aprecia en la Figura 3.2:

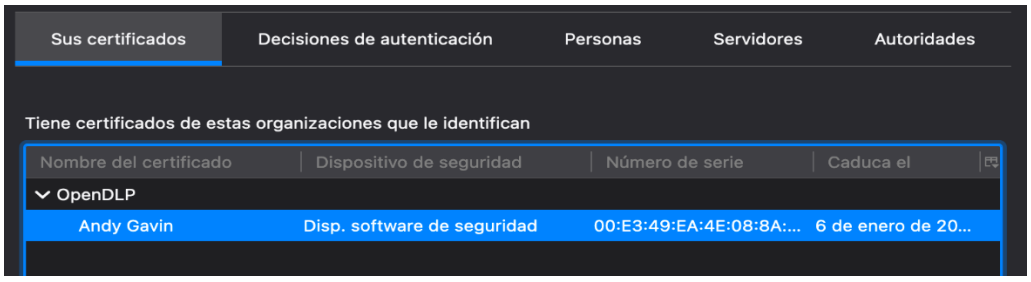


Figura 3. 2. Certificado de confianza OpenDLP

Fuente: elaboración propia

3.2. Prueba 2 Monitoreo de archivos por extensión

Para cualquier escaneo hay que crear un perfil y escoger el tipo de análisis que, se desea realizar. OpenDLP posee diferentes opciones de escaneo, como, se evidencia en la Figura 3.3 presentada a continuación:

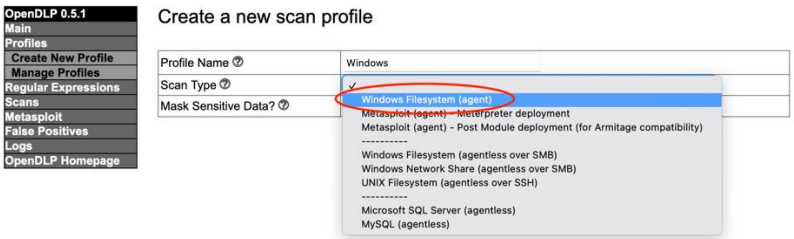


Figura 3. 3. Selección de tipo de escaneo

Fuente: elaboración propia

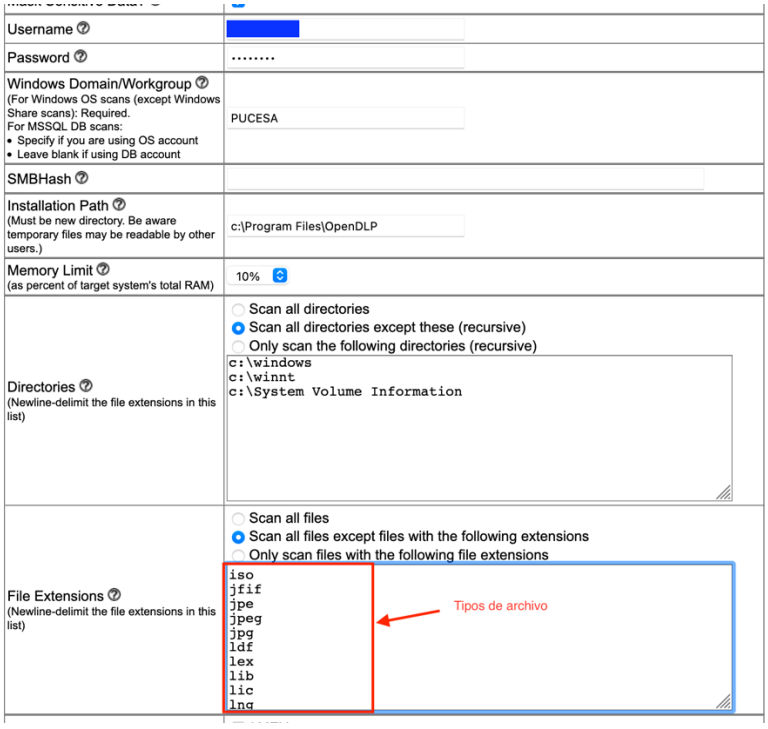


Figura 3.4. Tipo de archivo a escanear

Fuente: elaboración propia

Para la evaluación del prototipo, se realiza el análisis de los archivos mostrados en la Figura 3.5:

Profile Name	Windows
Scan type	win_agent
Username	[redacted]
SMBHash	
Password	**********
Domain Name	PUCESA
Installation Path	c:\Program Files\OpenDLP
Memory Limit	10%
Mask Sensitive Data	Yes
Scan directories	ignore
Directories	c:\windows c:\winnt c:\System Volume Information
Scan file extensions	ignore
Extensions	323 386 3g2 3gp 3gp2 3gpp 7z aac aca ace aif aifc aiff al amc ani arj asx au au3 avi bmp bz bz2 cab caf cda cdda cdf cdx cgi chm chr cmf cnv cod com ctx datasource del dep dev devp dib dl_ dll dmg don dpbcc drv dsp elm exe flt fon frm gen gif gz hiv hlp hpp hxs hxx ico idl inf ink inl ism iso jfif jpe jpeg jpg ldf lex lib lic lng lnk lxa m3u mdi mib mid miv mk mmp mov mp2 mp2v mp3 mp4 mpampe mpeg mpegmpv2maw mpg mpq msi msp ncb nlb nls nrg o obj ocx otf p pch pct pf pfm pic pict pll pm pnf png pnt pntg ppi psp pst pyc pyo pywqpa qt qti qtif qtl rar rb rbw rc rc2 rco rdd rmi rnd s scr sd2 sst sy_ sys tar tgz tif tiff tlb tmf ttf url uu vmss vmdk vmem vxd wav wax wma wmf wmv wpc wpl
Regular Expressions	Diners_Club_1, JCB_1, Mastercard, Visa
Credit Cards	Mastercard Visa AMEX Diners_Club_1 Diners_Club_2 Discover JCB_1 JCB_2
Zip File Extensions	zip jar xlsx docx pptx odt odp ods odg
Phone home URL username	ddt
Phone home URL password	**********
Phone home delay	300
Concurrent deployments	30
Windows Service description	Analisis de archivos
Log Verbosity	0

Archivos a evaluar

Figura 3.5. Extensiones analizar

Fuente: elaboración propia

El escaneo de archivos con OpenDLP será realizado a las direcciones IP mostradas en la Figura 3.6:

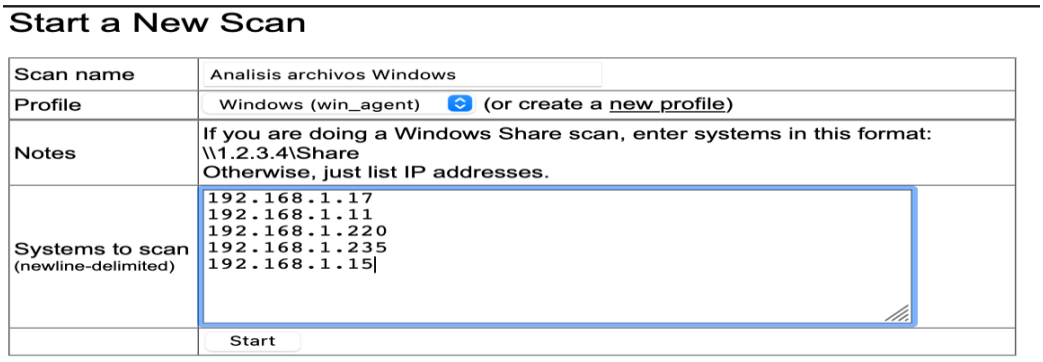
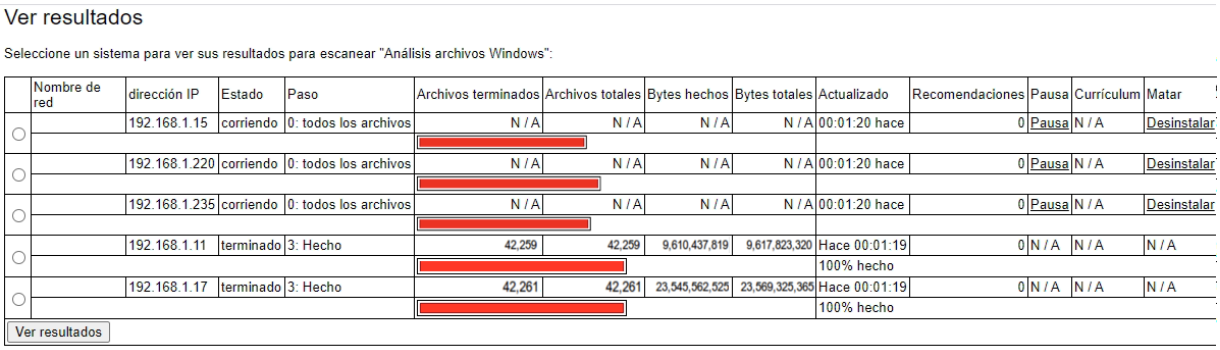


Figura 3.6. Direcciones de red a escanear

Fuente: elaboración propia

En la Figura 3.7, se aprecia el estado de los escaneos realizados a las direcciones programadas:



Ver resultados

Seleccione un sistema para ver sus resultados para escanear "Análisis archivos Windows":

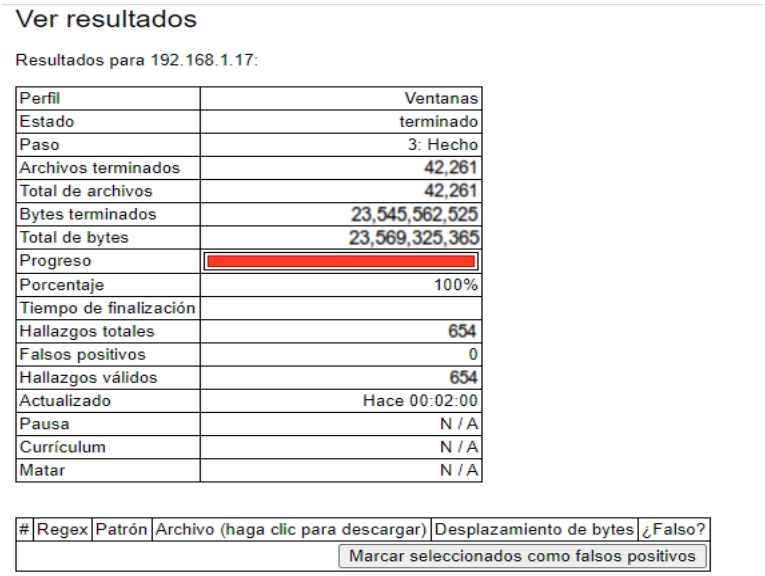
	Nombre de red	dirección IP	Estado	Paso	Archivos terminados	Archivos totales	Bytes hechos	Bytes totales	Actualizado	Recomendaciones	Pausa	Currículum	Matar
○		192.168.1.15	corriendo	0: todos los archivos	N / A	N / A	N / A	N / A	00:01:20 hace	0	Pausa	N / A	Desinstalar
○		192.168.1.220	corriendo	0: todos los archivos	N / A	N / A	N / A	N / A	00:01:20 hace	0	Pausa	N / A	Desinstalar
○		192.168.1.235	corriendo	0: todos los archivos	N / A	N / A	N / A	N / A	00:01:20 hace	0	Pausa	N / A	Desinstalar
○		192.168.1.11	terminado	3: Hecho	42,259	42,259	9,610,437,819	9,617,823,320	Hace 00:01:19	0	N / A	N / A	N / A
									100% hecho				
○		192.168.1.17	terminado	3: Hecho	42,261	42,261	23,545,562,525	23,569,325,365	Hace 00:01:19	0	N / A	N / A	N / A
									100% hecho				

Ver resultados

Figura 3.7. Proceso de escaneo en la red

Fuente: elaboración propia

En el análisis realizado al equipo con el direccionamiento 192.168.1.17, se aprecia que existen 654 hallazgos de archivos con extensiones similares a las configuradas en el escaneo. Estos resultados, se evidencian en la Figura 3.8:



Ver resultados

Resultados para 192.168.1.17:

Perfil	Ventanas
Estado	terminado
Paso	3: Hecho
Archivos terminados	42,261
Total de archivos	42,261
Bytes terminados	23,545,562,525
Total de bytes	23,569,325,365
Progreso	
Porcentaje	100%
Tiempo de finalización	
Hallazgos totales	654
Falsos positivos	0
Hallazgos válidos	654
Actualizado	Hace 00:02:00
Pausa	N / A
Currículum	N / A
Matar	N / A

#	Regex	Patrón	Archivo (haga clic para descargar)	Desplazamiento de bytes	¿Falso?

Marcar seleccionados como falsos positivos

Figura 3.8. Resultados del escaneo

Fuente: elaboración propia

3.3. Prueba 3 Monitoreo de Base de datos

OpenDLP posee la capacidad de escanear base de datos de SQL Server y MySQL, como, se muestra en la Figura 3.9 a continuación:

New Profile Submission:

Profile Name	Datos
Scan type	mssql_agentless
Username	administrator
Password	**********
Mask Sensitive Data	Yes
Scan databases	ignore
Databases	master tempdb model msdb pubs Northwind
Scan tables	ignore
Tables	syssegments sysconstraints dtproperties
Scan columns	everything
Columns	
Limit to rows	1000
Regular Expressions	Mastercard, Social_Security_Number_dashes
Credit Cards	Mastercard Visa AMEX Diners_Club_1 Diners_Club_2 Discover JCB_1 JCB_2
Concurrent deployments	30
Log Verbosity	0

Figura 3 9. Escaneo de bases de datos

Fuente: elaboración propia

El escaneo está realizado a las direcciones mostradas en la Figura 3.10 que, se muestra a continuación:

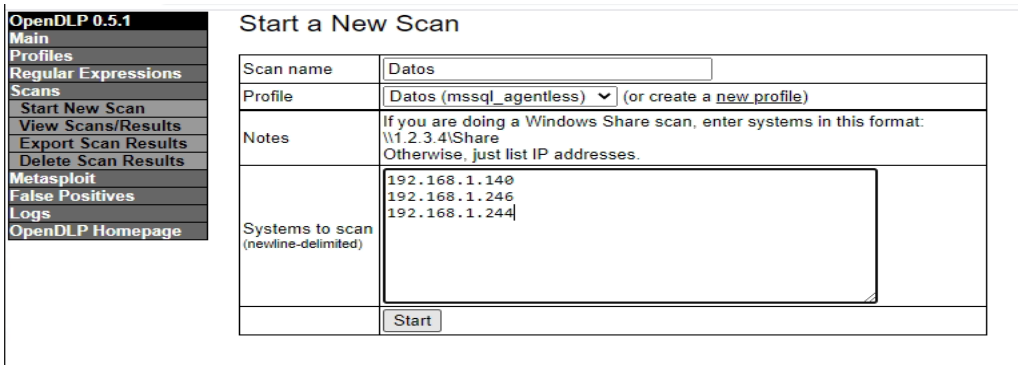


Figura 3.10. Configuración de escaneo de base de datos

Fuente: elaboración propia

En la Figura 3.11, se apreciar los resultados entregados por el escaneo de base de datos. Sin embargo, con el fin de mantener la confidencialidad de la información de las bases de datos de la Pontificia Universidad Católica del Ecuador Sede Ambato, esta información no, se muestra en la figura:

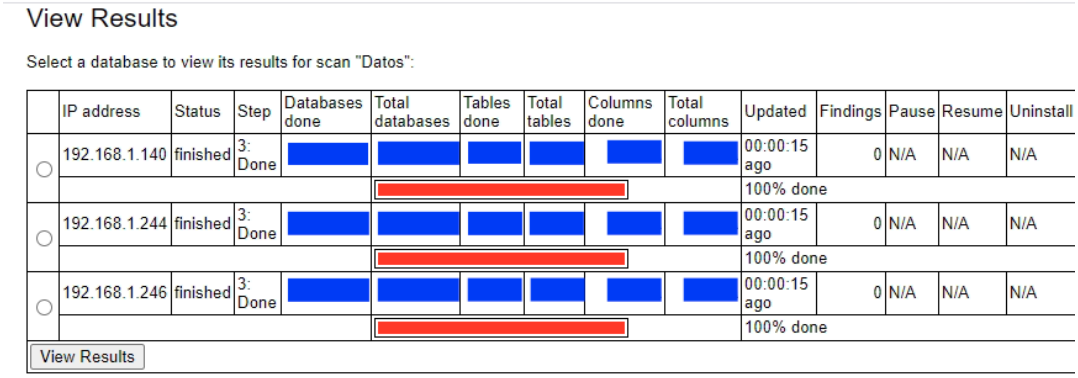


Figura 3.11. Resultado de escaneo en la base de datos

Fuente: elaboración propia

3.4. Prueba 4 Análisis programados

OpenDLP no cuenta con la capacidad de realizar análisis programados, debido a la falta de soporte que ha tenido esta herramienta en los últimos años. En la Figura 3.12, se evidencia todas las opciones que tiene OpenDLP.

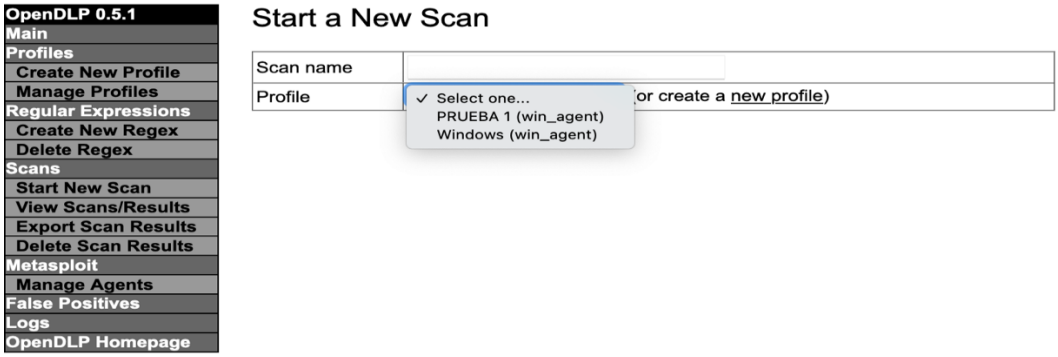


Figura 3.12. Opciones de OpenDLP

Fuente: elaboración propia

3.5. Prueba 5 Control de flujo de datos

OpenDLP no posee un control de flujo de datos, esto hace que la herramienta no sea un *software* DLP confiable para prevenir la fuga de la información. Esta herramienta, se usa para monitorear el tráfico de la red, mas no para el control de esta. En la Figura 3.13, se aprecia los resultados de monitoreo a la red:

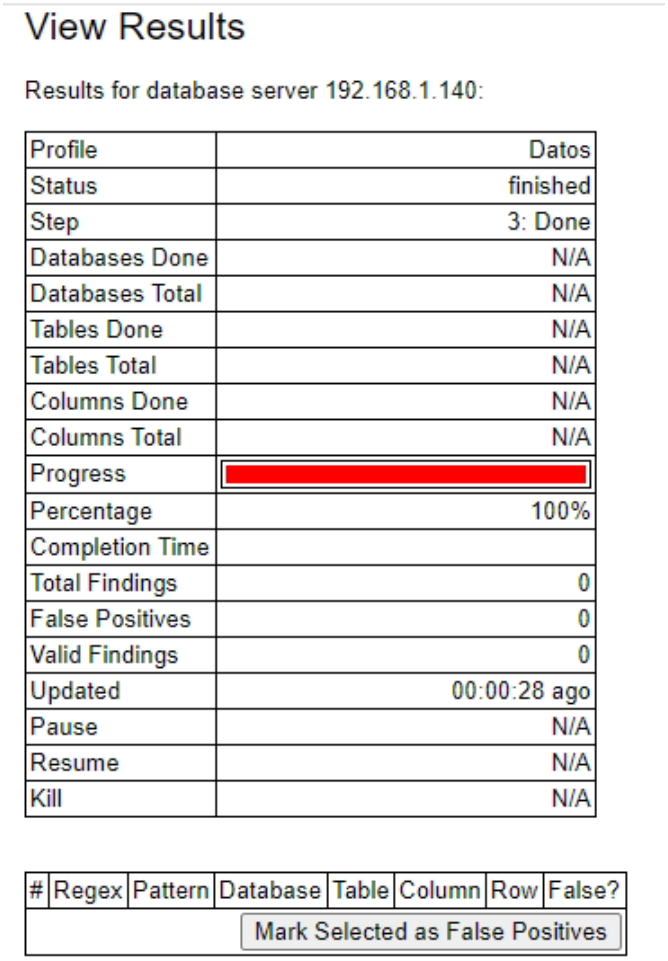


Figura 3.13. Monitoreo de OpenDLP

Fuente: elaboración propia

3.6. Prueba 6 Resultados estadísticos

Como, se evidencia en la Figura 3.14 OpenDLP no cuenta con un interfaz dedicado a generar resultados estadísticos, esto limita aún más el uso del *software*, debido a que de esta forma no hay resultados profundos en un análisis de fuga de información en la red.

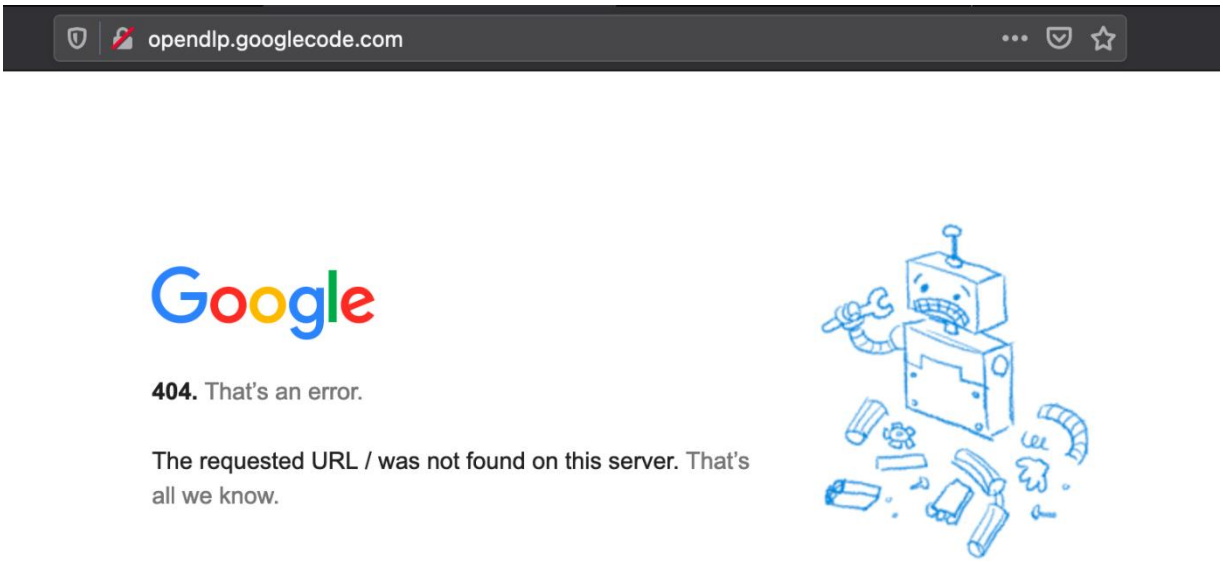


Figura 3.14. Error en resultados estadísticos

Fuente: elaboración propia

3.7. Prueba 7 Recursos de hardware

OpenDLP al ser una herramienta basada en GNU *Linux Ubuntu Server*, tiene una demanda de muy bajos recursos a nivel de *hardware*, esto a diferencia de otras herramientas DLP de paga, permite que dicho *software* pueda ser implementado en redes pequeñas que posea una infraestructura limitada, y que tenga la necesidad de protección básica en la fuga de la información. En la Figura 3.15, se muestra las características de la plataforma:

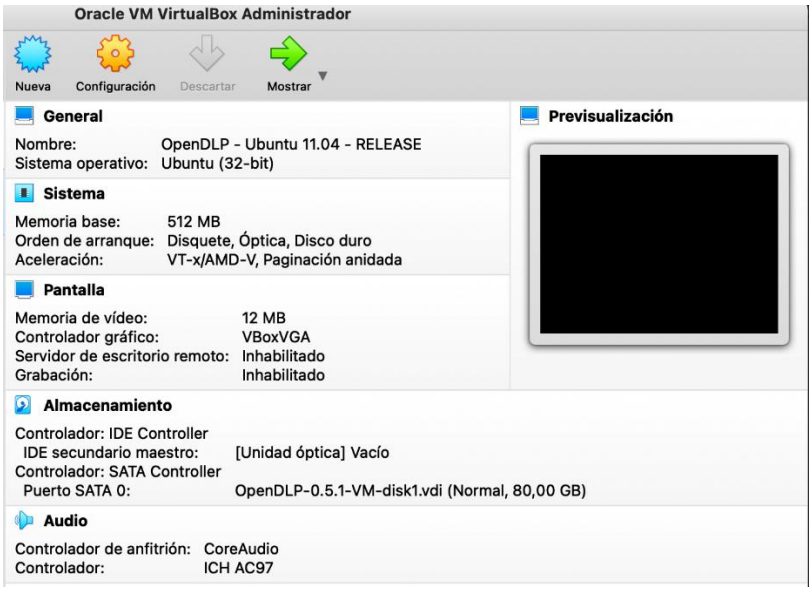


Figura 3.15. Características de OpenDLP

Fuente: elaboración propia

A continuación, se presenta la Tabla 3.1, en la que, se detalla las características que cuenta OpenDLP después de haber realizado todas las pruebas pertinentes:

Tabla 3.1. Resumen de resultados pruebas OpenDLP

CARACTERÍSTICA	CUMPLE	NO CUMPLE
Interfaz gráfica	**X**	
Monitoreo de archivos por extensión	**X**	
Monitoreo de base de datos	**X**	
Análisis programados		**X**
Control de flujo de datos:		**X**
Resultados estadísticos		**X**
Bajo consumo de recursos en *Hardware*	**X**	

Fuente: elaboración propia

CONCLUSIONES

- La fundamentación teórica acerca de las herramientas DLP, evidencia como los riesgos de fuga de información son un problema, que en la actualidad no solo afecta a Instituciones Educativas. Uno de los factores más complejos de proteger los datos es quizá el de los recursos internos a una organización. Para ello, las herramientas DLP brindan la oportunidad de disminuir este riesgo dentro de una Institución.

- El diagnóstico en los riesgos y vulnerabilidades de la Pontificia Universidad Católica del Ecuador Sede Ambato, pone en manifiesto, cuales son las amenazas latentes ante una posible fuga de información, esto hace que las autoridades del recinto universitario en conjunto con el Departamento de Tecnologías de la Información mantengan un continuo plan de mejora para la seguridad de la información, como: el uso de Políticas de seguridad o planes de contingencia ante un desastre.

- El diseño del prototipo estudiado demuestra cómo, en la actualidad existen limitadas herramientas DLP de licencia *OpenSource*, esto es debido a la gran acogida que estas han recibido, razón por la cual los desarrolladores de estas han vendido el código a grandes fabricantes de *software*, como es el caso de MyDLP.

- La evaluación del funcionamiento de la herramienta OpenDLP, deja en manifiesto las vulnerabilidades ante la fuga de información, como falta de control en el flujo de datos o programación de tareas, su Core es muy antiguo y debido a la falta de recursos, dicha plataforma no ha sido actualizada desde hace varios años. Además, al ser una herramienta de tipo *OpenSource* no posee las mismas características que un DLP con Licenciamiento.

RECOMENDACIONES

- Se recomienda a todas las instituciones, ya sean públicas o privadas mantengan una concientización acerca de la información que manejan, a fin de que el personal interno de la organización genere una cultura de la gravedad de una violación a la fuga de la información.

- Como PUCE Sede Ambato, se recomienda mantener planes de mejora e implementación de un Sistema de Gestión de Seguridad de la Información y respuesta a incidentes a fin de elevar la protección de los datos sensibles que maneja la institución.

- Se recomienda realizar análisis de herramientas DLP alojados en la nube, con el objetivo de entender la arquitectura y funcionamiento de estas plataformas, debido al ahorro de recursos en infraestructura que estas herramientas brindan a la organización.

- Realizar pruebas de funcionamiento y rendimiento con herramientas DLP con licenciamiento pagado, debido a las amplias características que estás poseen, ello brinda la oportunidad de realizar un estudio más profundo acerca de métodos de protección en la confidencialidad de la información.

BIBLIOGRAFÍA

Acosta, X. (2015). *Desarrollo de un modelo de seguridad para la prevención de pérdida de datos DLP, en empresas pymes (Tesis de pregrado)*. Recuperada de http://dspace.udla.edu.ec/bitstream/33000/4476/1/UDLA-EC-TIERI-2015-02.pdf

Armado, R. (2015). *OpenDLP para pentesters—Security Art Work*. Recuperado de https://www.securityartwork.es/2015/07/10/opendlp-para-pentesters/

Bortnik, S. (2010, abril 13). *¿Qué es la fuga de información?* WeLiveSecurity. Recuperado de https://www.welivesecurity.com/la-es/2010/04/13/que-es-la-fuga-de-informacion/

CambioDigital OnLine. (2020). *La tríada CIA: Definición, componentes y ejemplos | CambioDigital OnLine*. Recuperado de https://cambiodigital-ol.com/2020/03/la-triada-cia-definicion-componentes-y-ejemplos/

Csirt Cedia. (2020). *Estadísticas @ CSIRT Cedia*. Recuperado de https://yari.cedia.org.ec/index.php?r=site%2Fstats

Daffara Carlo. (2015). *INSEGUROS Seguridad informática: OpenDLP. Data Loss Prevention open source. Monitoriza las fugas de información.* Recuperado de https://kinomakino.blogspot.com/2015/03/opendlp-data-loss-prevention-open.html

Devlin, R., & Northcutt, S. (2016). *Data Loss Prevention*. 30.

ElevenPaths. (2017). *Fuga de información de la Policía Nacional del Ecuador*.

ESET. (2015, junio). *¿Ciberseguridad o seguridad de la información? Aclarando la diferencia | WeLiveSecurity*. Recuperado de https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/

Navarro Espinosa, J. A. (2017). *Desarrollo de un modelo de seguridad utilizando herramientas Data Loss Prevention (DLP), en las instituciones de Educación superior (IES) (Tesis de posgrado). Caso Universidad ECOTEC.* 16. Recuperada de http://repositorio.uees.edu.ec/bitstream/123456789/1437/1/Trabajo%20de%20titulaci%c3%b3n%20Johanna%20Navarro.pdf

Gartner. (2020). *Gartner*. Recuperado de https://www.gartner.com/en

Gómez Ruedas, J. (2011). *Dialnet-DeWikiLeaksALaDataLossPrevention-7271598.pdf*.

INCIBE. (2020). *Proteccion de la informacion*. 33.

ISO. (2020). *La familia de normas ISO 27000*. Recuperado de https://www.isotools.org/2015/01/21/familia-normas-iso-27000/

ISO / IEC 27001. (2013). *ISO / IEC 27001: 2013 (en), Tecnología de la información—Técnicas de seguridad—Sistemas de gestión de seguridad de la información—Requisitos*. Recuperado de https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

iso27000.es. (2005). *IS027000 SGSI*. ISO27000.ES. Recuperado de https://www.iso27000.es/iso27000.html

ISOTools Excellenge. (2020). *ISO 27002. La importancia de las buenas prácticas en los Sistemas de Seguridad de la Información*. ISO 27002. Recuperado de https://www.isotools.org/2019/06/11/iso-27002-la-importancia-de-las-buenas-practicas-en-los-sistemas-de-seguridad-de-la-informacion/

Kaspersky Lab. (2020). *El top 5 de los peores fugas de datos de 2017 (hasta ahora)*. Recuperado de https://www.kaspersky.es/blog/data-leaks-2017/14572/

Kingston, M. (2019, agosto). KingstonMwilaDataLossPreventionSystem.pdf. *ResearchGate*, 8.

Pacheco, F. (2011). *Fuga de Información: ¿una amenaza pasajera?* 11.

Pallas Mega, G. (2009, diciembre). Metodología de Implantación de un SGSI en un grupo empresarial jerárquico (Tesis de posgrado)**.** Recuperada de https://www.colibri.udelar.edu.uy/jspui/bitstream/20.500.12008/2954/1/tesis-pallas.pdf

Ponemon Institute (2019a). *Aumentan los ciberataques a las pymes en todo el mundo y cada vez son más selectivos y sofisticados*. Recuperado de https://www.prnewswire.com/news-releases/ponemon-aumentan-los-ciberataques-a-las-pymes-en-todo-el-mundo-y-cada-vez-son-mas-selectivos-y-sofisticados-808617104.html

Ponemon. (2020). Cybersecurity in the Remote Work Era—A Global Risk Report. *Research Report*, 63.

PUCE Sede Ambato. (2020). *Misión y Visión—PUCE Sede Ambato*. Recuperado de https://www.pucesa.edu.ec/mision-vision/

Ramos, P. (2011). *Fuga de información: Una realidad que preocupa a todos*. WeLiveSecurity. Recuperado de https://www.welivesecurity.com/la-es/2011/07/08/fuga-de-informacion-realidad-preocupante/

Ramos, J., y Sierra, L. (2017). *Análisis, diseño e implementación de una solución DLP (Data Loss Prevention) para la empresa BHA (Tesis de pregrado)*. Recuperad de http://polux.unipiloto.edu.co:8080/00004371.pdf

Symantec. (2019). *Internet Security Threat Report*.

Torres Martinez, M. A. (2015). *DLP: prevención de fuga de información (Data Loss Prevention)*. 6.

Verizon. (2020). *Data Breach Investigations Report*.

ANEXOS

ANEXO A: Formato entrevista autoridades PUCE Sede Ambato

Entrevista dirigida a las autoridades de la PUCE Sede Ambato

NOMBRE:

CARGO:

1. ¿Sabe usted, si la PUCE Sede Ambato ha sido víctima de algún ataque informático o robo de información?

SI	
NO	

Que piensa usted al respecto:

2. ¿Considera usted que la PUCE Sede Ambato maneja información sensible que no se encuentra protegida?

SI	
NO	

Por favor, argumente su criterio:

3. ¿Piensa usted que la PUCE Sede Ambato, mantiene una amenaza presente de fuga de información digital sensible?

SI	
NO	

Que sugerencias usted podría dar al departamento de Tecnologías de la Información:

4. Considera usted que es importante el diseño de un prototipo Data Loss Prevention (herramienta para prevenir fuga de información digital sensible)

SI	
NO	

Argumente su decisión:

¡MUCHAS GRACIAS!

ANEXO B: Formato entrevista Departamento de TI

Entrevista dirigida al Departamento de Tecnologías de la Información.

NOMBRE:

CARGO:

1. ¿Cuenta la PUCE Sede Ambato con una infraestructura tecnológica para proteger sus aplicativos y sistemas de comunicación?

SI	
NO	

Por favor, descríbalos:

2. ¿Existe alguna norma/estándar o política de seguridad para la protección de la información digital con la finalidad de que, esta no sea vulnerada?

SI	
NO	

Por favor, argumente su criterio:

3. ¿Considera usted la importancia de una auditoría externa que permita el hallazgo de vulnerabilidades a fin de mejorar la protección de la información?

SI	
NO	

Por favor, argumente su respuesta:

4. ¿Piensa que el departamento de Tecnologías de la Información debe hacer énfasis en prevenir el manejo indebido de la información sensible de la PUCE Sede Ambato, mediante herramientas Data Loss Prevention

SI	
NO	

Argumente su decisión:

¡MUCHAS GRACIAS!