FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

DESARROLLO DE UN MODELO DE SEGURIDAD PARA LA PREVENCIÓN DE PÉRDIDA DE DATOS DLP, EN EMPRESAS PYMES

Trabajo de Titulación presentado en conformidad a los requisitos establecidos para optar por el título de Ingeniera en Electrónica y Redes de Información

Profesor Guía

Ing. Mario Andrés Jaramillo Astudillo

Autora

Ximena Rocio Acosta Robles

Año

2015

DECLARACIÓN DEL PROFESOR GUÍA

"Declaro haber dirigido este trabajo a través de reuniones periódicas con la estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación".

_____

Mario Andrés Jaramillo Astudillo
Ingeniero Especialista en Telecomunicaciones
C.I.: 010242420-7

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

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

_____

Ximena Rocio Acosta Robles

C.C.: 171752280-7

DEDICATORIA

Dedico este trabajo de titulación, a mis padres y a mi hermano; pilares fundamentales y motores en mi vida. Por apoyarme en todos los momentos que han pasado a lo largo de este camino; a los cuales les dirijo mis palabras que sin ustedes nada hubiera sido posible.

Ximena

AGRADECIMIENTO

Agradezco a Dios y a la Virgen Morena por darme la sabiduría de realizar este trabajo, además de su cuidado en todos los años que han transcurrido en mi vida universitaria. De igual manera, mi mayor gratitud a mis padres y mi hermano; quienes me apoyaron incondicionalmente en cada decisión tomada, y por su incondicional amor y sabios consejos, los cuales me permitieron completar con éxito uno de mis mayores logros profesionales. A mis profesores, por su gran dedicación al impartir el conocimiento que lo llevo con orgullo; en especial al Ingeniero Mario Jaramillo, que con su paciencia y gran conocimiento en todo momento ha guiado este trabajo de titulación; mis más profundo agradecimiento para todos.

Ximena

RESUMEN

Este trabajo de titulación ofrece sus capítulos al desarrollo e implementación de un modelo de prevención de pérdida de datos (DLP), en las empresas PYMES del Ecuador, enfocándose principalmente en la identificación de las causas que conlleva a la fuga y pérdida de información en cada una de ellas.

Definir cuál herramienta será la más útil para desarrollar la metodología la cual está basada en la legislación ecuatoriana y en las normas mundialmente establecidas ISO 27001 Y 27002, por medio del análisis de varios estudios realizados a nivel global tal como Gartner.

Así mismo, se implementará el diseño elaborado en una de las empresas pymes ecuatorianas, de acuerdo a los requerimientos dados, con la finalidad de generar un análisis de resultados y costo-beneficio que se generará al implementar el sistema de prevención de perdida de datos DLP.

ABSTRACT

This dissertation and this work is dedicated to the development and implementation of data loss prevention model, in Ecuadorian PYMES business, focusing in the causes identification that loss and escaped information carries in all of them.

Define which tool would be more useful to the development of the methodology, which is based in Ecuadorian legislation and in the established international rules ISO 27001 and 27002; through the analysis of various studies realized at global level like Gartner.

As well, it would be implement that elaborated design in one of an Ecuadorian PYMES business, in accordance to the given requirements with the finality of generating an analysis of results and benefic-cost that it is generated by implementing the Data Loss Prevention System.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

INTRODUCCIÓN

Para este trabajo de titulación, el desarrollar una metodología de seguridad para evitar la fuga de información, es uno de los puntos clave; que en la actualidad la información es uno de los activos principales de cualquier empresa a nivel mundial; por lo cual no debería haber ningún tipo de percance para la protección de la misma.

Es por eso que el objetivo de este trabajo, es proponer un modelo de seguridad para la implementación que está directamente relacionada con la prevención de pérdida de datos en las empresas pymes de Ecuador, lo cual puede generar buenas practicas con el fin de proponer soluciones que integren un sistema lo más completo posible en base a la seguridad de la información empresarial.

Este trabajo de investigación y desarrollo consta de seis capítulos. En el capítulo primero denominado Marco Teórico y Referencial se encuentra definido los conceptos a utilizar en cada una de las partes del trabajo de titulación, con la finalidad de dar una explicación y una visión del tema principal. También se puede dar una explicación clara y concisa de las principales causas que hay en cada empresa para que haya una fuga y perdida de información masiva así como las consecuencias que conllevan dicha perdida. El análisis de la herramienta que puede ser de gran utilidad para la implementación de este trabajo es un punto esencial que se ve en este capítulo.

Por su parte en el segundo capítulo se abordan las leyes ecuatorianas y las normas internacionales que protegen la información. En el tercer capítulo se define modelo de seguridad para la prevención de pérdida de datos, en el cuál contribuirá a la disminución de los riesgos encontrados, por medio de la identificación de la información que hay en la empresa así como la creación de políticas y procedimientos.

En el cuarto capítulo se realizará la implementación de la solución dada en el desarrollo de la metodología para una correcta administración de los datos en base a la seguridad proporcionada con el fin de tener una evaluación del sistema mostrando las ventajas y desventajas de la herramienta que fue seleccionada por la empresa.

En el quinto capítulo se hará un análisis costo-beneficio de la solución proporcionada a la empresa para la administración de seguridad y prevención de perdida de datos. En el sexto capítulo se dará las conclusiones que se han dado al transcurso del desarrollo de este trabajo, así como las recomendaciones que se da a todos los usuarios en el caso de que este trabajo sea utilizado con fines posteriores.

Con el desarrollo de este trabajo de titulación se observará la importancia que tiene el proteger y prevenir la fuga y pérdida de información en cualquier empresa; así como el ciclo de vida que tiene cada información desde su creación hasta la destrucción y lo vital que es la protección de la misma durante este ciclo contra cualquier tipo de ataque sea interno o externo.

ANTECEDENTES

Gracias a la evolución de las TICS y la gran acogida que ha tenido los sistemas de redes en los últimos tiempos, han permitido a las empresas obtener grandes beneficios, sobretodo en este aspecto. Empresas privadas y organizaciones del estado, actualmente, dependen de este tipo de tecnologías para efectuar sus operaciones, generando así calidad y eficiencia en cada uno de sus procesos.

Grandes y medianas empresas, se ven en la necesidad de tener mayor eficiencia y rapidez en cada uno de los procesos que conforman las mismas. La sociedad se ha dado cuenta que en la actualidad el compartir información de forma segura es ya un requerimiento indispensable.

Las empresas están tomando con responsabilidad el manejo de la información que otorgan a las personas que colaboran con ellas, puesto que si la información no es manejada como debe de ser, puede ocasionar situaciones de riesgo que pueden llegar a ser irreversibles.

Año a año se ha visto que el número de incidentes relacionados con la pérdida de la información ha aumentado considerablemente, por varios factores como las fallas humanas, tecnológicas y vulnerabilidades que se dan a día a día, por ende han creado una brecha entre los intrusos informáticos y la seguridad.

El internet, es uno de los medios más susceptibles para cometer delitos informáticos. La protección de la información ya es considerada como un derecho fundamental, por ende los países han planteado regular y controlar la protección de datos, generando normas para evitar cualquier tipo de percance y brindar seguridad a los usuarios.

MARCO REFERENCIAL

DLP, conocido como sistema DLP (Data Loss Prevention o Prevención de Pérdida de Datos), son sistemas que tienen la principal función de identificar, clasificar, monitorear la información de las empresas. En Ecuador, las empresas PYMES, ya se ven en obligación de proteger toda la información, debido a que un incidente de estos, podrá costar miles de dólares en daños, perdidas de negocios, entre otras.

El usuario final de cada empresa tiene la disponibilidad de acceder a información sensible y extraerla en dispositivos, pero esto se puede prevenir con un sistema DLP. Cada una de las herramientas que conforman un sistema DLP, permite controlar el uso de los dispositivos extraíbles, con una consola en la que se pueda configurar las políticas de seguridad en tiempo real. Permite la protección de datos fuera de la red en la que se encuentra la empresa, por medio de auditorías y monitorización Gracias a que las empresas tienen

directorios activos, para su mayor organización; cada una de las herramientas de sistema DLP, trabajan con ello, permitiendo asignar políticas a los usuarios y a ordenadores de acuerdo al grupo creado en los respectivos directorios.

Cada uno de los sistemas DLP llega a guardar los registros de actividad de todos los usuarios de la empresa, creando así un historial sobre el uso del dispositivo.

Si este sistema se aplicaría, se tendrá una gestión centralizada puesto que simplifica cada uno de los requisitos que se han pedido y una transparencia del usuario completa, debido a que la intervención del usuario es mínima y una productividad muy eficaz.

Las empresas en Ecuador, buscan soluciones que ofrezcan más por menor costo, por lo que un sistema DLP reduciría en gran medida el costo y la dificultad que se tiene en la protección de la información

ALCANCE

Al diseñar un modelo para la implementación de un sistema de prevención de pérdida de datos DLP, se ayudará a las empresas a descubrir, monitorear, proteger, administrar los datos que se dan a los usuarios de manera mucho más eficiente, ya que estas soluciones han tomado mucha relevancia que un sistema de prevención como un antivirus, antispyware o antispam o un firewall que la mayoría de las empresas han incorporado como un sistema de seguridad completo.

Lo primero es analizar la información que tiene una organización, dando énfasis en los elementos electrónicos, los cuales se va identificar y posteriormente clasificar la información más importante y sensible. Se realizará un análisis de toda la infraestructura tanto de hardware como software, obteniendo así los posibles problemas y el impacto generado en la empresa.

Al tener un resultado, se procederá con la creación de un modelo de prevención tomando en cuenta colocar políticas de seguridad, que ayuden a proteger la información de acuerdo a su prioridad. Se las podría definir de acuerdo a por qué fueron creadas, su principal uso, almacenamiento y posteriormente su destrucción.

Para la implementación de este diseño, se dará algunas soluciones tecnológicas que vayan de la mano junto a las políticas de seguridad anteriormente planteadas; entre estas se encuentran anti-spams, encriptación de la información, y la eliminación de la información que ya no sea de relevancia en la empresa. Se basará en el cuadrante de Gardner actualizado.

Se conoce que implementar estas soluciones ayuda a mitigar los ataques informáticos, pero también puede causar un poco de conflicto, ya sea por el costo o por la mala distribución de la información, es por eso que este diseño ayudará a las organizaciones tener conciencia de los riesgos a la que se encuentra expuesta si no tiene un debido sistema de protección de pérdida de datos.

JUSTIFICACIÓN

La información, para una organización, es totalmente indispensable debido a que sin está no se lograría el éxito de la misma. Por tal motivo no hay que evadir la protección de la información y de los sistemas que las desarrollan debido a que si se deja un punto sin seguridad, inmediatamente se vuelve vulnerable abriendo así una puerta a amenazas y ataques informáticos.

Fugas de información, han llegado a ser el tabú de las organizaciones, ya que las consecuencias son muy críticas. En los últimos tiempos, las políticas de seguridad que se han asignado a la información, no han sido muy eficaces siendo ignoradas tanto por los ejecutivos como por los empleados de empresas. Actualmente se tienen normas y leyes que regulan este tema, por

tanto las empresas tienen la capacidad de obtener, mediante los estándares internacionales y nacionales, grandes mecanismos de protección.

La mayoría de las empresas no tienen el conocimiento de que conlleva tener una eficaz seguridad de información, piensan que este proceso es muy complicado y que no se tendría buenos resultados, imaginan que aparte de ajustar estos mecanismos a las leyes y normas se tiene que ajustar al presupuesto que se tiene para este tipo de proyectos.

Es por esto, que al diseñar e implementar un sistema de prevención de datos DLP, ayudará a reducir notablemente la fuga de información permitiendo identificar las zonas sensibles donde se encuentran cada uno de los datos, monitoreando su proceso cumpliendo las políticas implementadas.

OBJETIVO GENERAL

- Desarrollar un modelo de seguridad para la prevención de pérdida de datos DLP, en empresas PYMES

OBJETIVO ESPECÍFICO

- Identificar las causas que conllevan a la perdida de datos.

- Realizar un análisis de las herramientas DLP usadas en el mercado.

- Desarrollar el método de prevención de pérdida de datos basados en la legislación ecuatoriana y en la norma mundialmente establecida ISO 27001 y 27002.

- Implementar el diseño elaborado en Wincha Tarqui (Ambato), de acuerdo con los requerimientos dados y resultados de los análisis obtenidos.

- Realizar un análisis de resultados y costos que se generó al implementar el sistema DLP.

TIPO DE METODOLOGÍA

En este proyecto se empleará una metodología de carácter descriptiva debido a que incluye investigación inductiva, deductiva y experimental. Se permite realizar un análisis de lo conlleva tener un sistema DLP endpoint en la empresa. Gracias a la metodología deductiva, se ayudará a identificar los posibles problemas y causas que enfrenta la empresa en seguridad de la información y su posterior pérdida de datos. Con la metodología inductiva se desarrollará un sistema de pérdida de datos basados en la legislación ecuatoriana y en las normas mundiales (ISO 27001 y 27002), para que se diseñe un sistema DLP apto para cada necesidad de la empresa. Con la metodología experimental se realizará la implementación del diseño antes modelado.

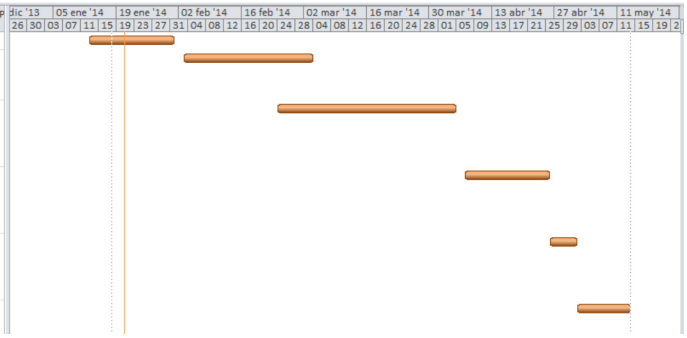
En el diseño se va a incluir herramientas de hardware y software. En la sección software, se va a implementar un sistema DLP endpoint previamente analizado, tanto en el servidor como en el cliente. En el lado del cliente ayudará a monitorear, controlar y prevenir que los usuarios no autorizados accedan, copien o transfieran información sensible; mientras que en el lado del administrador se regirán las políticas para clasificar, identificar, proteger y monitorear toda la información de la empresa pymes. En la sección hardware se utilizará una consola de políticas donde define y hace cumplir las políticas establecidas; además administrar los demás componentes que están vinculados a la herramienta endpoint. Un servidor con Windows Server 2008

R2 en el que se instalará el software DLP en el cual asigna las políticas y recoge las alertas, logs del usuario final, que se maneja mediante laptops o Workstation.

De acuerdo a lo planteado, se hará un análisis costo-beneficio que conlleva a tener esta herramienta de seguridad.

CRONOGRAMA DE ACTIVIDADES

	Nombre de tarea	Duración	Comienzo	Fin
1	Marco Metodológico	15 días	lun 13/01/14	vie 31/01/14
2	Tecnología DLP basado en la Legislación Ecuatoriana y normas ISO 27001 Y 27002	21 días	lun 03/02/14	lun 03/03/14
3	MODELO DE SEGURIDAD PARA LA PREVENCION DE PERDIDA DE DATOS EN LAS EMPRESAS PYMES	30 días	lun 24/02/14	vie 04/04/14
4	Implementación de solución para la administración de seguridad y prevención de pérdida de datos (DLP)	15 días	lun 07/04/14	vie 25/04/14
5	Análisis Costo-Beneficio de la solución para la administración de seguridad y prevención de pérdida de datos (DLP)	5 días	sáb 26/04/14	jue 01/05/14
6	Conclusiones y Recomendaciones	8 días	vie 02/05/14	mar 13/05/14



1 MARCO TEÓRICO Y REFERENCIA

En el capítulo presente se definen los conceptos que se utilizarán para el presente trabajo, así como el conocimiento de los tipos de información, los riesgos que conlleva en la susceptibilidad de la misma gracias a los ataques a los que son sometidos y las políticas de seguridad para el uso adecuado de la información en las empresas PYMES. Se define, también, que es una herramienta DLP, así como las características de cada una de ellas por medio del cuadrante de Gartner.

1.1 Conceptos

Generalmente los usuarios tienden a confundir los conceptos informáticos, sin embargo es necesario hacer una breve aclaración de los mismos.

Dato: Para poder definir este concepto, es necesario definirla desde la terminología general. En base a la definición de (Prisak, 1999); un dato es una unidad semántica y corresponde con elementos primarios de información que por sí solos son irrelevantes como apoyo a la toma de decisiones.

Pero en sí, el dato es una representación simbólica como algoritmos o números inclusive, es considerado como un atributo o característica de una entidad. Al no ser semántico, es decir que no tiene sentido, el dato recibe un procesamiento para la toma de decisiones.

Los datos pueden provenir de fuentes externas como internas, debido a que pueden ser almacenados en un espacio físico (DVD, CD) como virtual (nube electrónica), siendo así, de carácter objetivo, subjetivo, cualitativo o cuantitativo.

Al hablar de datos, hablamos de una clasificación de los mismos. Podremos tener datos para tomar decisiones o para archivarlos según sea su utilidad.

Las relaciones Públicas Jurídicas, en su publicación (Relaciones Públicas Jurídicas, 2012) - La protección de datos.pdf, los datos se pueden clasificar en dos maneras:

- Datos Públicos: Son datos que no tienen ningún tipo de restricción tanto para el personal como para el usuario. Un ejemplo son los datos que se muestran a través del internet, tales como redes sociales o páginas web.

- Datos Privados o Confidenciales: Son datos que tienen acceso restringido según las políticas de cada empresa. Pueden ser restringidos para cierto tipo de empleados o al usuario en general.

El conjunto de los datos, al ser contextualizados, corregidos, categorizados y condensados se convierte en información, que depende del grado de valor que se le añada, para que esta sea útil o no.

Información: La información se considera como un conjunto de datos precisos y coherentes que tienen un gran significado para el ser humano. Estos datos son procesados en un tiempo oportuno siendo de mucha utilidad para la toma de decisiones.

El conocimiento de la información que se tiene en una empresa, ayuda notablemente a clasificarla y ordenarla con la finalidad de proporcionar un nivel de seguridad adecuado. En base a lo que Gestiopolis publicó en su página web (Gestopolis, 2012), la información se la considera en base al Módulo de Administración y Dirección de Empresas, de la siguiente manera:

- Información Pública: Es aquella que se puede acceder libremente, siempre y cuando los integrantes de la empresa sepan cuál es la información que se está mostrando.

- Información Privada: Es aquella que tiene un acceso limitado. Este tipo de información puede ser manejada por una persona o un grupo que conforman la empresa. Puede llegar a ser datos personales o financieros.

Sistema: Un sistema es considerado a un conjunto de elementos (personas, actividades y recursos) que trabajan para la administración, procesamiento y organización de los datos de información para que puedan ser utilizados de manera óptima, llegando así a cumplir objetivos claros.

El principal objetivo de un sistema de información de una empresa es el ser productivos y llegar a ser un lugar de trabajo excepcional gracias al eficiente desarrollo de las actividades de la empresa.

Debido a esto, en la siguiente figura se define el tipo de sistema de información clasificado en torno a al usuario final, considerando como base un modelo jerárquico de una empresa PYMES.

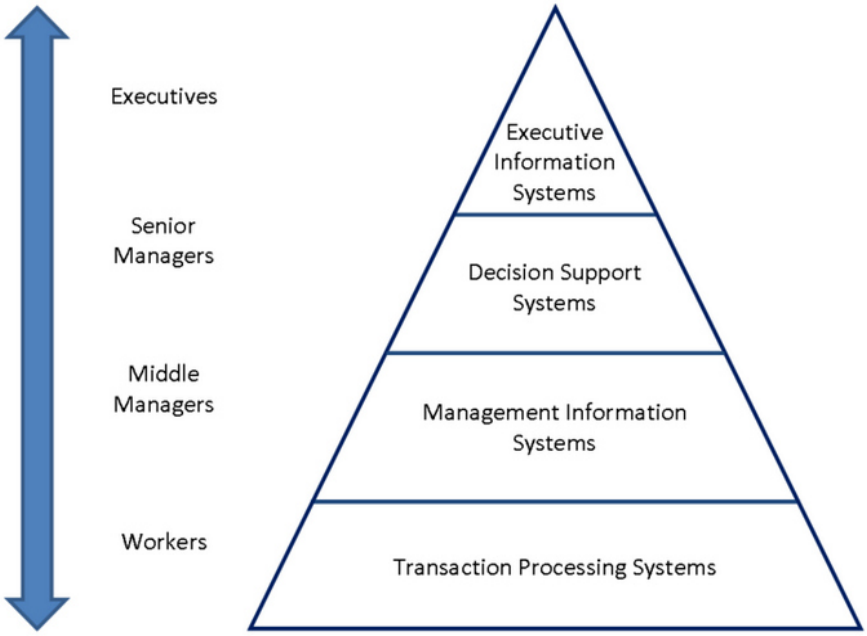


Figura 1. Tipo de Sistemas de Información
Tomado de (Wikimedia, s.f.)

- Sistema de información Ejecutiva (EIS): Este sistema maneja la información estratégica de la empresa en tiempo real, ayudando así, al desempeño y efectividad en la presentación de los datos. Es un sistema de inteligencia empresarial manejada netamente por los ejecutivos gerenciales.

- Sistema de Soporte de Decisiones (DSS): Este sistema se implementa al momento de que se haya realizado los respectivos sistemas transaccionales de la empresa ya que prácticamente estos sistemas constituyen la plataforma de información empresarial. Generalmente estos sistemas ayudan a formar un modelo de planeación financiera.

- Sistema de información Gerencial (MIS): Estos sistemas son formados por la interacción entre los usuarios, la tecnología y cada procedimiento de la empresa, es decir de los sistemas de información como tal. Se ayudan de otros sistemas que se usan en las actividades operacionales de la empresa.

- Sistemas de Procedimiento de Transacción (TPS): Es el primer sistema implementado en la empresa. La entrada y salida de la información es muy intensiva puesto que es el apoyo de las tareas a nivel operativo del trabajador final de la empresa.

Línea de tiempo de un Sistema de Información: Todo sistema de información tiene un ciclo de vida. En la siguiente figura se muestra el proceso de un Sistema de Información.

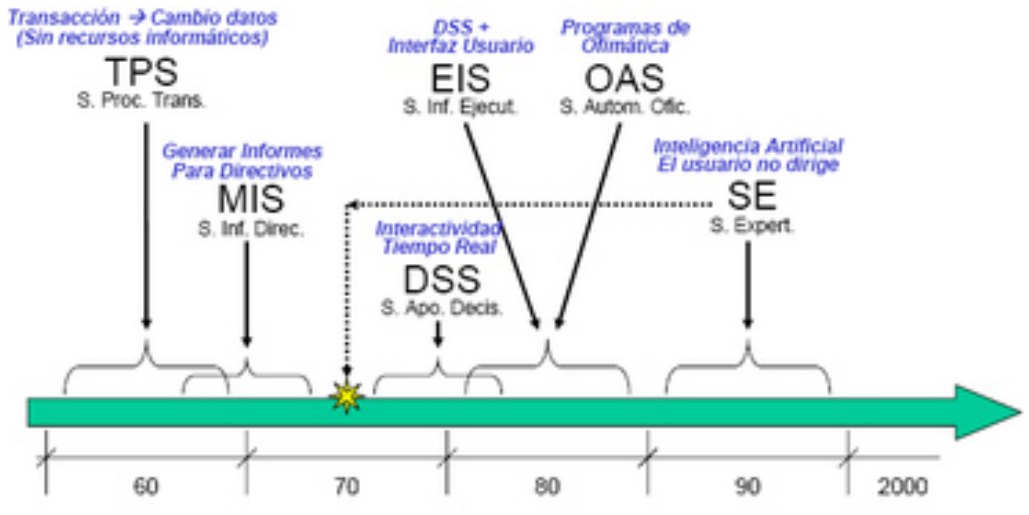


Figura 2. Línea de Tiempo de un Sistema de Información
Tomado de (Wikimedia, s.f.)

Sistema Experto (SE): Es aquel que el usuario no dirige, es netamente una inteligencia artificial ya que emula el comportamiento de un experto en un dominio.

- Sistema de Planificación de Recursos (ERP): Es el sistema que combina la interfaz del usuario, la información y el proceso de la empresa en un solo sistema.

- Sistema de Automatización de Oficina (OAS): Es considerada a las aplicaciones que maneja el usuario de la empresa.

1.2 Seguridad Informática

En la actualidad, los sistemas de información conforman una parte fundamental de cada empresa. Junto a los recursos de hardware y software, los datos que son almacenados y procesados en estos, necesitan estar protegidos.

Ataques, código malicioso, vulnerabilidad en la web e incidentes como el robo de la información, ha despertado en los últimos años la necesidad de preservar

la información. La seguridad es un mecanismo que permite el óptimo funcionamiento de cada sistema evitando que haya fallas en los mismos como la pérdida de la información.

La seguridad informática se considera como la protección de los recursos informáticos que hay en cada empresa, evitando la ejecución de procesos no autorizados sobre la red de información, así como el involucrar la autenticidad, confidencialidad de los datos de información.

Ayuda a mitigar y administrar los posibles riesgos que tiene la información, así como detectar las amenazas de seguridad de las empresas, ayudando en el correcto uso de las aplicaciones y recursos de los sistemas así como la recuperación del mismo en caso de que haya un suceso de inseguridad.

Hay que tomar en cuenta el cumplimiento del marco regulatorio que existe en cada una de las empresas y que cada uno de los usuarios tienen la obligación de cumplir con cada una de ellas, tales como controlar los accesos a la información y los archivos protegidos.

El cumplimiento de los requisitos y de los marcos legales impuestos por el cliente, es vital en la seguridad informática. Vigilar cada uno de los accesos de la información y de quien accede es responsabilidad de todo el personal, ya que en cada nivel se debe realizar las acciones necesarias para proteger de forma adecuada el uso de la información y recursos informáticos.

La seguridad informática debe ser concientizada a todo el personal de las empresas, realizando en cada una de las áreas de trabajo, las acciones necesarias para proteger de manera óptima el uso de los datos, la información y los recursos informáticos que se utilizan.

1.2.1 Alcance de la seguridad de información

Respecto al alcance de la seguridad informática, esta es definida por cada empresa. Se basa principalmente en la información que posee y el nivel de protección que se le quiere dar.

Panda Security, una empresa dedicada a soluciones de seguridad de la información, definió en su página web (Panda Security, 2009) que para que haya un buen alcance en la seguridad y que cubra todos los rubros debe seguir algunas características:

- Definir las políticas, procedimientos, estándares de la seguridad informática.

- Administrar a usuarios y recursos de cada sistema de comunicación e informático.

- Definir una seguridad de carácter interna de acceso a las aplicaciones.

- Definir normas y procedimientos en cada una de las operaciones del centro de cómputo de la empresa.

- Realizar procesos de copia de seguridad y recuperación de la información.

- Definir, desarrollar y mantener un plan de riesgo, en tal caso que haya una fuga de información.

- Implementar seguridades en cada uno de los sistemas físicos del centro de cómputo para evitar incendios o problemas eléctricos y electrónicos.

Los controles para una buena seguridad de la información se basan en los niveles de riesgos que hay en cada área que conforma la empresa. Los riesgos se los verá más adelante.

Cada uno de los controles se clasifica en tres clases:

- Físicos
- Técnicos
- Administrativos

Los controles físicos son aquellos que limitan el acceso a la información de manera somática con la conexión directa de los dispositivos a los equipos del centro de cómputo. Pueden consistir en alarmas, vigilantes, sistemas de detección de agua, humo, fuego incluso sistemas de alimentación de reserva como fuentes de alimentación (UPS) o baterías.

Los controles técnicos son los que se implementan en los ambientes lógico y físico de las empresas, evitando así la intervención de los usuarios en cada uno de ellos. En estos se incluyen antivirus, cifrado, herramientas de gestión de red, contraseñas, equipos inteligentes, huellas dátiles, entre otros.

Los controles administrativos son las políticas de seguridad que se dan en las empresas. Estas incluyen claves de acceso, aprobación para acceder a recursos, supervisión de las soluciones aplicadas, informes de auditoría, entre otras.

1.2.2 Riesgos

La Organización Internacional por la Normalización, define en su página web (International Organization for Standardization - ISO, 2014), “La probabilidad de que una amenaza se materialice, utilizando la vulnerabilidad existentes de un activo o grupos de activos, puede generar pérdidas o daños”.

Los riesgos se pueden encontrar en cada área de la empresa y cada sistema que ayuda a su funcionamiento. Cada uno de estos está conformado por procesos, que a su vez están creados por actividades que se pueden realizar de manera manual o automática, creando así una relación con un riesgo potencial.

Las empresas, frente a esta situación optan por la manera más fácil de traspasar los riesgos, sin tomar en cuenta que si se acepta la deficiencia se puede hacer algo para disminuir el evento del mismo.

1.2.2.1 Análisis y control de riesgos

Cada una de las empresas tiende a tener cada tipo de información distribuida en cada área y nivel de trabajo, pero no se dan cuenta que se encuentran en constante amenaza, debido a que no tienen un control necesario, llegando así, al robo de la misma y ocasionando un caos a nivel organizacional.

Al realizar un análisis de riesgo, ayuda notablemente a tener un conocimiento de las causas posibles de las amenazas y los daños que pueden producir. Es recomendable utilizarla como una herramienta de gestión para los sistemas de comunicación e información que hay en las organizaciones para el debido progreso de cada actividad realizada.

Ya que esto es una herramienta de gestión, debe seguir algunos procesos para que esto llegue a ser eficiente, los cuales son;

- Definir los sistemas de comunicación o informáticos que se van a analizar.
- Identificar las posibles amenazas que puedan dañar los sistemas.
- Determinar la agudeza de la amenaza.

- Determinar el impacto que puede generar a la organización, dando prioridad en cada una de ellas.

- Dar algunas recomendaciones para mitigar el riesgo.

- Documentar cada uno de los procesos.

Gracias a esto se podría determinar el riesgo y el impacto que pueda generar en cada empresa. El impacto se refiere directamente a la situación socio-económica que se puede dar.

Los riesgos que se producen en una empresa, generalmente van desde los medios físicos, controles de acceso hasta la protección de los datos y seguridad de la red implementada. Pero no se toma en cuenta algunos aspectos que también son complemento en la protección informática tales como:

- Asignación de responsabilidades.
- Políticas dadas a los usuarios.
- Marco legal de seguridad.
- Estándares de operación de los sistemas.
- Seguridad en cada uno de los sistemas.
- Plan de prevención de eventualidades.

Cada uno de los especialistas debe tomar en cuenta y abarcar todos estos aspectos para tener un análisis muy bueno y así presentar los resultados de acuerdo a lo que la empresa requiera.

Los riesgos a los que están sometidas las empresas se clasifican en 5 tipos en los cuales van desde la infraestructura hasta las interfaces usadas por cada colaborador, estas son:

- Riesgo de Integridad: Los riesgos de integridad incluyen a las acciones realizadas en las aplicaciones de las empresas, en estas están las autorizaciones, procesamientos y reportes de las mismas. Cada uno de estos riesgos se pueden visualizar en los siguientes componentes de cada sistema empresarial:

  - Interfaz de usuario: Se basan en las autorizaciones y restricciones al ejecutar funciones del sistema. También tiene que ver con los controles que se da para validar y completar la información introducida.

  - Procesamiento: Están relacionados con el control y balance preventivo y correctivo de la información que se ha introducido. También incluye los riesgos que se dan con la exactitud y totalidad de cada informe para obtener resultados y tomar las mejores decisiones.

  - Procesamiento de errores: Son los riesgos que se dan si los errores del sistema no son capturados y corregidos correctamente.

  - Interface: Estos riesgos se basan con los controles preventivos y correctivos de la información que ha sido procesada y enviada por medio de las aplicaciones empresariales.

- Riesgos de Relación: Son los que se producen por el uso de la información en una aplicación de manera pertinente. Este riesgo está directamente relacionado con la toma de decisiones.

- Riesgos de Acceso: Se basan en el acceso inapropiado a cada sistema de la empresa, están afiliados con el acceso a la información que están en las bases de datos y su debida confidencialidad. Se puede dar en los siguientes niveles de seguridad:

- Nivel Físico: Se da en los elementos físicos y su apropiado acceso tales como dispositivos biométricos, contraseñas que se dan en los equipos, entre otras.

- Redes: Se da gracias al acceso inadecuado al entorno de la red y cada uno de los procesos que hay en ella.

- Entornos de procesamientos: Se da por el acceso inapropiado a las interfaces de los programas y la información empresarial.

- Aplicaciones: Es el riesgo que se da en cada mecanismo de seguridad que se provee a los trabajadores para realizar su trabajo.

- Riesgo en Infraestructura: La mayoría de las empresas no poseen una estructura tecnológica para futuras necesidades, por lo que el riesgo es eminente. Estos riesgos están en netamente complementados con el desarrollo, operación y mantenimiento de cada proceso empresarial y sus respectivas aplicaciones.

- Riesgo en seguridad de infraestructura y entorno: Este tipo de riesgo se basa en riesgos eléctricos tales como altos voltajes, riesgos de radiaciones, incendios y mecánicos

1.2.3 Políticas de Seguridad

Hoy en día, la seguridad informática es un punto clave para cada empresa puesto que cada una de ellas incrementa o mejoran su esquema informático así como las plataformas colocadas.

Cada empresa ha puesto el acceso a la información de manera más amplia y de forma distribuida dando ventajas para el negocio, tales como:

- Reducción de Costo: A través de mecanismos de acceso a la red y la integridad de los procesos, la reducción de costos es notable, debido a que al ser más efectivo en las comunicaciones entre los clientes y los socios de cada empresa, ayuda en sí al incremento de las ventas.

- Alto Rendimiento en las ocupaciones de la empresa: Al tener un acceso seguro a la información corporativa desde cualquier lugar, cada uno de los empleados aumentan la productividad de su trabajo, ayudando así al crecimiento socio-económico de la empresa.

Gracias a los beneficios que brindan las conectividades, también estas generan problemas y riesgos ya que cada una ellas están expuestos a spams, virus, entre otros que pueden introducirse en los sistemas de información de la empresa.

Las políticas de seguridad son un conjunto de normas y procedimientos que ayudan a definir las guías de trabajo y los métodos de seguridad que deben ser establecidos a nivel institucional con el fin de establecer, estandarizar y normalizar la seguridad del usuario y de los sistemas tecnológicos.

Los ámbitos en los que se definen las políticas de seguridad son las humanas y tecnológicas. El ámbito humano tiene que ver con la integración de actividades y responsabilidades de todos los clientes y personal de la empresa; mientras que el ámbito tecnológico, se basa en el funcionamiento de las telecomunicaciones, software, hardware entre otros sistemas informáticos que existen en la empresa.

Para la elaboración de las políticas de seguridad se debe de tomar en cuenta 2 aspectos:

- Requisición de las políticas: Cada una de las políticas que se implementan en las organizaciones tienen conexión directa con la cultura

organizacional definida. Al integrar personas que tengan conocimientos de seguridad e ir preparando el documento que definirían cada política, ayuda notablemente a la aplicación y cumplimiento de las mismas.

- Elaboración de las políticas de seguridad: Para producir las políticas, es necesario saber cómo está estructurada la empresa y cómo se está efectuando cada uno de los procesos. A partir de esto se evalúa que la seguridad empiece a proceder así como poder detectar los puntos que estén en total vulnerabilidad.

Cada una de las políticas debe ser concisa y enfocada a la realidad de la empresa. Es responsabilidad de cada uno de los líderes empezar a apoyar este tipo de proyectos, para que la empresa siga creciendo no solo en negocio sino en TICS.

1.3 Perdida de datos en empresa Pymes

Empresas PYMES o pequeñas y medianas empresas; son el conjunto de empresas que de acuerdo a país establecido, el número de trabajadores, niveles de producción, años de vida y el volumen de venta originado desde un capital, tienen características de igual magnitud en su crecimiento.

Basados en el documento investigativo “Las Pymes en Ecuador” proporcionada por la Universidad Salesiana del Ecuador, (Universidad Politécnica Salesiana, 2014); en Ecuador, las empresas PYMES son aquellas en las que su volumen de venta está entre los 15.000 y 200.000 anuales. Son esenciales para el país puesto que contribuyen en su economía debido a que generan casi el 100% de los servicios que una persona utiliza diariamente como por ejemplo las tiendas de barrio, papelerías o servicio de transporte. Al no tener una gran cantidad de activos, son capaces de adaptarse a los cambios que sufre la economía ecuatoriana diariamente.

La fragilidad que tienen las empresas PYMES en el país, es muy notoria, la falta de conocimiento empresarial, la falta de liquidez para crecer, insuficiencia en materiales y equipos de tecnología para ayudar a incrementar los procesos contables y administrativos ayuda a tener una fuerte competitividad con las grandes empresas en el mercado.

Uno de los más grandes inconvenientes que tienen este tipo de empresas, es el uso inadecuado de la información, cada día se ve que la fuga de información va incrementándose ayudando a desvanecer la empresa, debido a que la información se puede enviar por medios electrónicos tales como correos o mensajería instantánea (IM), inclusive se la puede obtener por medio de dispositivos extraíbles tales como CD´S o USB´S.

La pérdida de datos se la considera como un error en los sistemas de información implementados, ya que la información se llega a deshacer o simplemente fugarse por el descuido en la transmisión, procesamiento y almacenamiento de la misma. Esto llega a suceder por el motivo de que no se valora adecuadamente la información, sin saber que cada atributo que tiene cada una de ellas, se las considera como activos informáticos.

Fred Cohen, en su libro “Virus Informáticos: teoría y experimentos” (Cohen, 1984) considera que al hablar de activo informático, se está denotando la economía de la información, la cual comprende una preocupación en la cantidad de información procesada en una empresa, mediante la interacción de sus integrantes para la toma correcta de decisiones.

En el artículo “Fuga de Información en las organizaciones” (Calvo, 2009), explica que todas las empresas usan dispositivos tales como celulares inteligentes que permiten el acceso a correo, almacenamiento de información, sincronización de la misma por medio de conexiones tales como wireless o redes móviles, que si bien facilita el trabajo de los empleados, representan un riesgo en la perdida de la confidencialidad, integridad y disponibilidad de la

información, si no se tiene en claro las consecuencias de incorporar nuevas tecnologías y los posibles mecanismos que se pueden implementar para proteger la información.

1.3.1 Valor de la información

La información es esencial para la toma de decisiones de cada empresa. Su valor está relacionado en la situación en la que se va a usar y quien la está manejando. Esta constituye un bien que en la mayoría de los casos no se valora como se debe ya que es consideraba intangible.

Este está asociado directamente con la creación, almacenamiento, retención y administración de la información, así también el valor esencial que esta tiene al momento de haber sido utilizada.

1.3.2 Motivos para la fuga de información

Los motivos que se podría considerar para la fuga de información, se debe a la falta de conocimiento del valor de la misma por los usuarios, ya que puede ser difundido en perímetros que no están asociadas a la empresa. Inclusive la falta de formación y buenas prácticas de las empresas a los empleados, y la falta de políticas y procedimientos son elementos suficientes para desencadenar un incidente de fuga de información.

Los códigos malware son las causas o motivos más comunes para el robo de la información, debido a que este permite automatizar y controlar una parte de los procesos que tiene la información de la empresa que se quiere despojar. Gracias al diseño de estos códigos, pueden pasar desprevenidos mientras obtienen y envían la información pertinente.

El acceso no autorizado a los sistemas e infraestructura de las empresas es otro motivo para la fuga de información. Se han vuelto una palestra en los

incidentes de seguridad más peligrosas mostrando un déficit de nivel de seguridad. Cada sistema, para no convertirse en un sistema obsoleto, requiere actualizaciones, y por este medio puede obtenerse la información sensible provocando un daño considerable para la empresa.

1.3.3 Riesgo de información sensible y consecuencias

En la actualidad, las empresas han invertido para proteger su información en centro de datos, debido a que la movilidad y portabilidad de la misma ha ido evolucionando. La información se está manejando y distribuyendo por medio de dispositivos móviles tales como telefonía celular, dispositivos extraíbles y equipos portátiles. Pero cada una de estas aún no es consciente del valor que tiene su información y los daños que podrían suceder si es que esta llegara a manos indebidas.

Los puntos de fuga son la parte esencial para que esto ocurra, es por eso que para su mejor entendimiento, se las clasificó de la siguiente manera:

- Redes Sociales: En la actualidad, esta herramienta es vital para la humanidad, debido a su flexibilidad de comunicación y velocidad en la trasmisión de mensajes, pero, cada una de ellas representan un riesgo para la confidencialidad de la información ya que al ser poder ser la información de la empresa publicada, puede causar severos inconvenientes.

- Robo de equipos portátiles y dispositivos móviles: Cada empresa otorga los recursos necesarios para que el trabajador pueda realizar su trabajo, es así que proporcionan la mejor tecnología para que este sea efectivo; sin embargo, no tienen ningún mecanismo de protección por lo que el obtener datos confidenciales es muy sencillo.

- Malware, Virus: Este es uno de los puntos de fuga de información más comunes, debido a su sencilla difusión en el medio informático y su difícil percepción.

SANS Institute, publicó en el artículo “Fuga de información en empresas” (SANS Institute, 2009); explica que los activos más importantes de toda organización es la información ya que esta contiene datos secretos y confidenciales. También considera que uno de los atacantes principales es el empleado, ya que son personas que tienen todo el acceso a las instalaciones y el control de la información.

Un estudio realizado por Lumesion, “2014 Data Protection Maturity Survey”, explica que el 59% de las empresas han perdido información sensible por medio de dispositivos móviles y extraíbles. Este tipo de pérdidas se asocia directamente con los trabajadores de cada empresa ya que esta no tiene políticas adecuadas para el manejo de la información sensible.

Ahora, las empresas tienen una gran duda de cómo cubrir la perdida de dispositivos si no se tiene los mecanismos de control para la protección de los datos que tiene cada dispositivo, así también como definir adecuadamente un nuevo proceso ante un nuevo evento de pérdida de información en una situación en la que no se puede controlar y como desenlace delimitar si las políticas de protección establecidas son las correctas.

1.4 Qué es un DLP

Data Loss Prevention (DLP) es considerado un término de seguridad informática refiriéndose a un sistema que identifica y supervisa la protección de los datos estáticos, en movimiento y en uso. Estos sistemas inspeccionan y analizan el contenido de la información así como la seguridad de cada transacción como por ejemplo el tiempo en el que se envía la información al destinatario y el marco de gestión que se genera de manera centralizada.

Están diseñados para localizar y prevenir el uso y transmisión de la información confidencial.

En la siguiente figura se explica brevemente el esquema de un Sistema de Prevención de Perdida de datos:

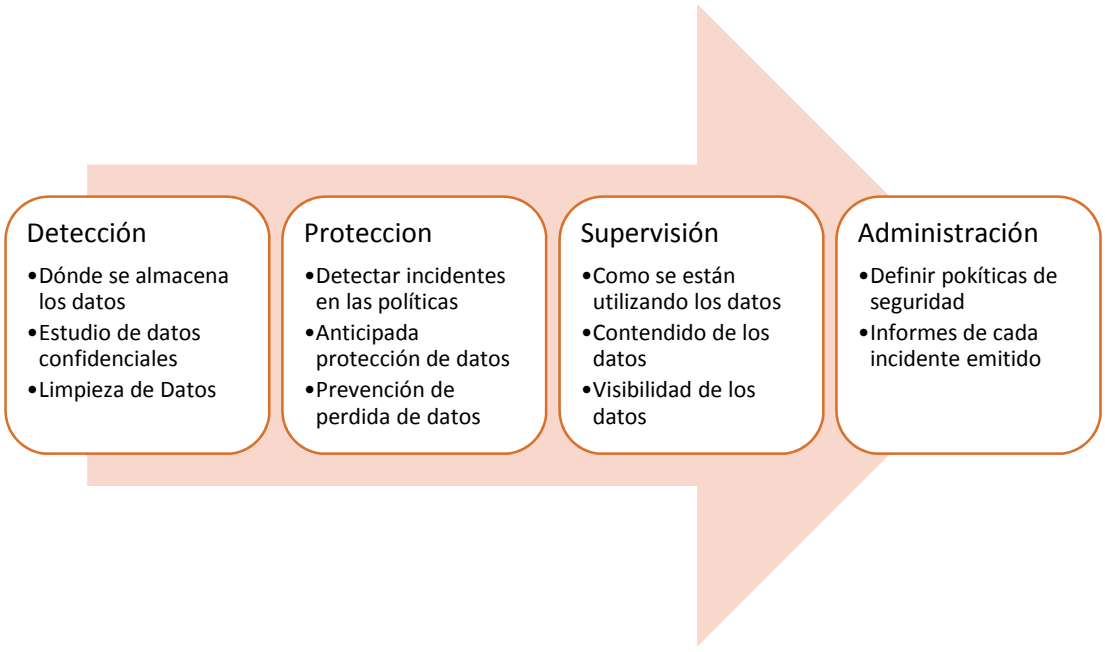


Figura 3. Esquema de un DLP

Tomado de (Steffens, s.f.)

En la fase de detección se descubre en donde están almacenados cada uno de los datos y la información de la empresa, por lo que esta fase es esencial para poder determinar en dónde pueden ser colocados cada uno de los datos y la información manejada de preferencia en un repositorio centralizado.

En la fase de protección se define cómo se están utilizando los datos en la empresa con la finalidad de detectar los incidentes que se van provocando debido a su mal uso; por lo cual se proporciona una seguridad proactiva en el uso de estos y así poder prevenir la fuga de información sensible de la empresa.

En la fase de supervisión, se da un seguimiento en tiempo real del manejo de los datos y la información sensible gracias a la herramienta Endpoint colocada en los equipos de los usuarios de la empresa. Con esto se puede determinar las medidas necesarias que ayudarían a prevenir la fuga de información, y otras acciones que pueden ocurrir si esta no ha sido controlada a tiempo, tales como cancelar los procesos de transmisión de la información o bloquear cada evento por medio de las políticas asignadas en la herramienta de seguridad.

En la fase de administración se definen las políticas de seguridad que se van a utilizar en la empresa con el fin de mitigar el robo y fuga de información y así poder generar informes de cada incidente que se ha presentado.

1.4.1 Función de un DLP

La función de un sistema de prevención de pérdida de datos (DLP) es la de detectar, identificar, supervisar y prevenir la fuga de información de carácter sensible para cada una de las empresas. Estos procesos se realizan mediante herramientas estables protegiendo los datos mediante un ciclo de vida de la herramienta.

Los aspectos que se toman en cuenta para la prevención de pérdida de datos se basan de acuerdo a los tipos de datos obtenidos:

- Datos en Reposo: Son aquellos datos sensibles que se verifica su almacenamiento en medios de respaldo en donde está cada contenido. Un ejemplo claro de esto es el uso de la herramienta DLP para indagar los documentos colocados en un servidor que contengan los datos de las utilidades emitidas en el presente año. Si el servidor no tiene autorización para tener ese tipo de información, el registro puede ser encriptado o removido, siempre y cuando se avise al propietario del mismo.

- Datos de Movimiento: Estos datos son los que están en constante observación desde el tráfico de la red mediante el Proxy de manera pasiva o en línea. Estos datos pueden ser la mensajería instantánea, emails o código fuente emitido por la web de carácter sensible.

- Datos en Uso: Son los datos que son manipulados por el usuario y que son monitoreados por medio de las soluciones al punto final. Un ejemplo clave es la extracción de la información sensible por medio de dispositivos extraíbles tales como USB´s o discos.

1.4.2 Características de un sistema DLP

La característica básica de un sistema DLP es la que ayuda netamente a las empresas a entender mejor el verdadero significado de cada uno de los datos que tienen, así como el clasificar y administrar cada uno de ellos generando comunicados para el correcto manejo de la información que está siendo utilizada.

Al realizar un análisis profundo del contenido de información que tiene la empresa, se toma en cuenta también el buen desempeño de la herramienta seleccionada ya que el trabajo de esta depende como se encuentre la información, así como las técnicas empleadas para el manejo de la misma.

En la actualidad, cada solución de prevención de pérdida de datos, trabajan bajo un servidor central en la cual se administra la ejecución y la detección, asimismo la creación de cada punto que gestiona las políticas y los flujos de trabajo con la presentación de informes a tiempo real.

Gracias a los sistemas DLP se logra reducir la transmisión de los datos confidenciales en el centro de datos empresariales y los equipos de los usuarios finales, además ayuda con la identificación de cada proceso que está en mal estado y que va transmitiendo la información sensible.

Logra supervisar y resguardar las comunicaciones con contenido confidencial que van a la web gracias a la definición e implementación de políticas de seguridad de carácter general en la empresa.

1.4.3 Políticas

Las políticas es el núcleo principal de un DLP, sin ellas no se vería la marcada diferencia entre los datos sensibles y los de acceso público. Cada una de las políticas se basa en las especificaciones propias de cada empresa, pero también de entornos muy fuera del ambiente laboral tales como las interconexiones de componentes intermedios (PCI) o los sistemas de seguridad digital (DSS).

En esta etapa es importante tomar en cuenta las políticas que ya han sido creadas en la empresa y discutir con las personas encargadas de manejar los datos, para poder realizar una adecuada identificación, clasificación y protección de los mismos. Estas políticas se convierten en reglas que el sistema DLP debe cumplir durante su periodo de funcionamiento. Tomemos como ejemplo la clasificación de los códigos fuente de los sistemas financieros que son considerados como un activo sensible de la empresa, los cuales están desarrollados mediante un lenguaje de programación JAVA. Estos deben ser almacenados en repositorios y máquinas desarrolladas en JAVA. Si un usuario quisiera modificar el código fuente en otro lugar, el sistema DLP se encarga de bloquear la solicitud debido a que está cumpliendo con la política definida.

Las políticas regulares que son establecidas en la empresa se logran convertir en reglas del sistema DLP. Estas reglas son desplegadas en los agentes del punto final, que están en los equipos de los trabajadores y en la red que va desde el centro de administración DLP hasta el usuario final.

En la siguiente figura se tiene una visión más clara de cómo las políticas son esenciales en los sistemas DLP.

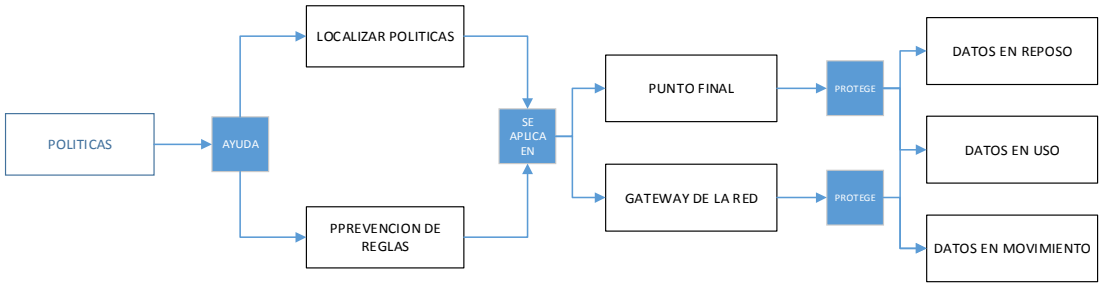


Figura 4. Visión de las políticas en un Sistema DLP

Tomado de (Revista Dintel, s.f.)

1.4.4 Herramientas DLP

Las herramientas de prevención de pérdida de datos tienen como fin cuidar la información sensible de cada empresa y garantizar el cumplimiento de cada una de las políticas definidas, cuyo objetivo principal es el de proteger los datos sensible en cualquier lugar que estén ubicados como por ejemplo en espacios físicos, puntos terminales o en la nube.

Esta tecnología identifica la información sensible ya definidas por la empresa y por medio de algoritmos que hay en la herramienta, esta encuentra coincidencia con las políticas establecidas, generando así el cumplimiento de las mismas. La mayor parte de estas herramientas ven los datos en movimiento, como se explicó anteriormente ya sea por vía web, correo electrónico o los datos copiados en medios extraíbles; pero también pueden observar los datos en reposo que están almacenados a lo largo de la red empresarial.

1.4.4.1 Análisis de cada herramienta dlp basado en cuadrante de Gartner

El cuadrante de Gartner es una herramienta exclusiva para el análisis de mercado que analiza y evalúa a los principales proveedores de cada mercado en el ámbito tecnológico evaluando varios puntos tales como: fortalezas, debilidades y sus capacidades para crecer en un futuro.

El cuadrante está segmentado en cuatro partes en dónde se distribuyen las principales compañías que dan las herramientas de prevención de pérdida de datos (DLP) en función de su tipología y sus productos. En la siguiente figura se muestra los cuadrantes de Gartner:

Figura 5. Modelo del Cuadrante de Gartner
Tomado de (Gartner, s.f.)

El eje X, se define como la integridad de visión o “completes of visión”, en la que representa el conocimiento de los proveedores para saber aprovechar el momento en el que está el mercado en tiempo real con el fin de generar un valor para ellos y para los clientes. El eje Y, se trata en la capacidad de ejecutar o “ability to execute”, es la que trata de medir la habilidad de los proveedores para ejecutar la visión del mercado de una manera exitosa.

Los dos ejes dividen al cuadrante en 4 sectores que son los líderes (leaders), visionarios (visionaries), aspirantes (challengers) y jugadores del nicho (nicho players).

Los líderes son aquellos que tienen una puntuación elevada al combinar el potencial de visualizar el mercado y la forma como ejecuta el proceso de venta, soporte de sus productos y servicios dados al usuario final. Los aspirantes son aquellos que ofrecen una calidad en funcionabilidad así como la cantidad de instalación del producto. Los visionarios son los que ofrecen una buena gestión de contenido empresarial (ECM), de manera propia en base a alianzas estratégicas con otros socios, lo cual permite una integridad en las plataformas y programas, inclusive se anticipan a las necesidades del mercado. Y para finalizar los jugadores del nicho que son los que se enfocan en determinadas áreas de la gestión de contenido empresarial, pero no tienen un paquete de programas completos.

Al medir cuál de los productos DLP es el más eficaz para realizar la gestión se basó en el documento definido el 14 de marzo del 2014 gracias a la empresa Gartner, quien definió las principales marcas que ayudarán a las empresas a tener un buen sistema de prevención de pérdida de datos.

En el siguiente gráfico se puede ver las principales empresas para que tratan este tema.

Figura 6. Cuadrante de Gartner para Plataformas de Endpoint Protection
Tomado de (Gartner, s.f.)

Este cuadrante se formó en base a la eficiencia y rendimiento de los anti-malware, así como el rendimiento y calidad de gestión en otras plataformas distintas a Windows, como por ejemplo Macintosh o Linux.

En la siguiente tabla se demuestra las principales fortalezas y debilidades de cada uno de los proveedores en herramientas DLP.

Tabla 1. Fortalezas y Debilidades de Proveedores de la Herramienta DLP

PROVEEDOR	FORTALEZAS	DEBILIDADES
Arkon Neetwork Security	• Capacidad entendible EPP (Endpoint Protection) en la que integra las capas de seguridad. • Se tiene firewall personal, encriptación y control de dispositivo con licencia Avira. • Fácil configuración en las políticas para minimizar la superficie de ataques. • Encriptación de discos y cifrado de carpetas en la que incluyen archivos de carácter sensible tanto en dispositivos fijo como en móviles.	• No es conocido en el mercado. • No ofrece una amplia gama en protección malware. • Al no ser conocido en el mercado no está en ninguna prueba en protección Endpoint. • Es compactible solamente con plataformas Windows. • Tiene dependencia en la marca Avira, puesto que tiene un equipo mínimo en investigación.
Beyond Trust	• Su consola administrativa es basada en flash, combina la protección endpoint y análisis de vulnerabilidad. • Permite la eliminación de derechos de administrador y el manejo de privilegios de manera seleccionada. • Dispone de una gama de licencias anti-malware de Norman que proporcionan un buen soporte técnico y monitoreo de archivos. • Da un acuerdo de servicio de 48 horas sobre vulnerabilidades fuertes. • Ofrece Retina Mobile, que proporciona análisis y monitoreo de las vulnerabilidades en dispositivos Android, IOS y Blackberry.	• Es poco conocido en el mercado. • No tiene capacidad de obtener y recoger información personalizada, puesto que debe ser definido y programado con anticipación. • No participa en pruebas industriales y no demuestra la eficacia de su colección tecnológica. • Solo se apoya en escritorio Windows y plataformas de servidores mediante un sistema integrado web. • El agente anti-malware funciona en host virtualizado en Windows, sin embargo no está optimizado para entornos virtuales.

PROVEEDOR	FORTALEZAS	DEBILIDADES
BitDefender	• Gravity Zone proporciona una gestión de Endpoint físicos, virtuales y móviles fácil de usar. • Permite implementaciones en la nube gracias a Cloud Security for Endpoints. • La mayor parte de funcionalidad de antivirus se realiza en un servidor central, teniendo solo un cliente en el punto final. • La seguridad para servicios móviles está disponible en la interfaz de gestión ya que proporciona protección anti-malware, control de acceso a la web y encriptación.	• Es poco conocido en el mercado • La consola administrativa carece de evaluación de los estados de seguridad de la información. • Cliente importantes tales como Exchange. • Aún no tiene en la consola administrativa consolidada.
Check Point Software Technologies	• Se destacan por tener “software blades”. Estas son arquitecturas de seguridad flexibles para cualquier tipo de empresa debido a que incluyen cortafuegos personales, anti-malware de licencia Kapersky Lab, control de acceso a red y VPN integrado. • Tiene una interfaz de usuario final de fácil acceso y navegación. • Los administradores son capaces de personalizar las políticas para cada usuario desde varios dispositivos. • Se gestiona en dispositivos móviles ya que incluye MDM siendo compactible con Android y IOS. • Gestiona la sincronización con correo Exchange.	• El agente no tiene la capacidad de análisis de contenido iniciales y se basa en la puerta de entrada por lo que no se puede lograr una efectiva monitorización de la información en tiempo real. • . El escaneado en red se centra principalmente en sólo el tráfico HTTP por lo que casos de uso de la nube no son actualmente soportados. • Todavía se encuentra en una etapa en la que no hay aún soporte para la búsqueda exacta de los datos.

PROVEEDOR	FORTALEZAS	DEBILIDADES
Kapersky Lab	• Tiene gran reputación en la detección de malware. • El tablero de instrumento llamado Microsoft Management Console (MMC), tiene advertencias de vulnerabilidad e informa los problemas que presenta el cliente. • Al tener un control en las aplicaciones, esta tiene una base de datos para el mejor desempeño de las mismas. • Tiene varias soluciones para el cliente final, tales como VMware vShield, que se encarga en la detección de intrusos en tiempo real.	• El colocar parches produce que haya problemas en las aplicaciones del cliente final. • Las funciones desarrolladas internamente en la consola MMC, necesita hacer más pruebas antes de su lanzamiento al usuario. • Los productos de seguridad para Exchange estaña en servidores independientes, por lo que produce que no estén integrados en su totalidad con los demás productos.
McAfee	• La plataforma de Endpoint proporciona una gestión flexible, presentando informes y flujos de trabajo en tiempo real. • Su plataforma es de carácter abierto ya que da la oportunidad de manejar 120 aplicaciones externas. • Su herramienta es capaz de dar un análisis de riesgos de la seguridad que se dan en el momento así como la detección de malware.	• Complejidad en el manejo de la plataforma. • El ciclo de seguridad que proporciona la herramienta no está alineada a un buen flujo de trabajo.

PROVEEDOR	FORTALEZAS	DEBILIDADES
Microsoft	• Su plataforma SECP (System Center 2012 Endpoint Protection de Microsoft) se encuentra ya en todas las licencias de Microsoft. • Trabaja con las licencias CAL (Core Client Access License) que son aplicables tanto en el servidor con en el cliente final. • Ha mejorado en la limpieza de archivos infectados, ya que son reemplazados con una versión confiable que se encuentra en la nube de Microsoft.	• A pesar de ser un producto de gran capacidad, esta es solamente ara sistemas Microsoft, por lo que no es compactible con otros sistemas operativos. • El manejo de la plataforma debe ser administrado por usuarios Windows, o que puede inhabilitar de manera errónea al cliente. • No ofrece el control de datos en Sharepoint y en aplicaciones MDM excepto Exchange.
Symantec	• Fue el pionero en dar soluciones de seguridad a través de la nube. • Tiene herramientas que ayudan a la depuración y eliminación de infecciones en tiempo real. • Trabaja en entornos virtualizado ya que el costo de ellos es mucho más accequible.	• El manejo de la plataforma es fácil para el que maneja en el área de administración de la plataforma pero para el usuario es complicado por algunas interfaces gráficas. • Es un sistema que si no se tiene un administrador no se lo puede manejar a cabalidad.

Para determinar cuál es la herramienta que será de utilidad para la realización de este proyecto, se basó en cada uno de los aspectos de la tabla 1, así como en la decisión de cada uno de los integrantes de la empresa definiendo a la herramienta proporcionada por McAfee, como el mecanismo ideal para la implementación piloto.

1.4.5 Aplicaciones

Las organizaciones deben de tomar en cuenta algunos aspectos tales como el detectar los datos que se tienen que vigilar y ser controlados continuamente, también el saber tomar las medidas adecuadas para reducir la fuga de información y que a la par sea muy rentable.

En el mercado de tecnologías en Data Loss Prevention, divide a este sistema en una herramienta y en una solución.

La solución es aquella que incluye en su totalidad la creación de las políticas, el monitoreo y protección de los datos sensibles. Las interfaces de funcionalidad y de usuario final se complementan de tal manera que pueden solventar los problemas técnicos y de negocio con el fin de proteger todo el contenido que se tiene.

Las herramientas de prevención de pérdida de datos se dedican a proteger los datos y contenido que tenga la empresa ya que incluyen algunas características de los productos de Endpoint.

Es bueno saber que cada una de ellas cumple con su principal función de poder prevenir y solventar los problemas que generen que de una u otra manera son estas son causadas por el mal manejo de las unidades de negocio o el administrador de la herramienta.

Para la mayoría de las empresas, todas las políticas de seguridad son altamente sensibles para ser manejada por cualquier persona, es por eso que los líderes del negocio son los encargados principales para que puedan controlar cualquier inconveniente en el manejo de la información, es por eso que el desarrollo de la metodología de sistema de prevención de pérdida de datos es una solución dedicada para este segmento.

1.5 Elemento de Amenazas

La pérdida de datos se da de distintas maneras debido a que existen elementos o mecanismos que pueden facilitar con éxito la fuga de información. Los elementos pueden ser organizativos que son los trabajadores ya que no tienen el conocimiento del correcto uso de la información; o los ámbitos técnicos, que son errores de hardware o daños en el software que se van

generando debido a los ataques informáticos como virus, troyanos o también por catástrofes naturales, en los cuales la infraestructura tecnológica de la empresa llega a perderse. Es por eso que para saber cada uno de estos elementos, se ha clasificado en pérdida de datos accidental y en ataques externos e internos que se van desarrollando en cada una de las empresas.

1.5.1 Perdida de datos accidental

Este es uno de los casos que más se suscita en una compañía, aquí están relacionados directamente los trabajadores y las políticas que son conocidas supuestamente por ellos. Los usuarios no conocen en su totalidad las políticas que hay, por lo que no reconocen que cada documento en el que trabajan que de una u otra manera tienen caracteres sensibles o confidenciales. Los casos más comunes son:

- Carga de documentos a través de la red, como por ejemplo carpetas temporales, en la que todos los empleados tienen acceso libre.

- Enviar documentos de carácter confidencial, sin ser encriptados.

- Guardar los documentos con información sensible en dispositivos extraíbles, tales como USB, disco duros, entre otros.

1.5.2 Ataque Interno

Este tipo de ataques son aquellos en que existe un intruso que saben la arquitectura de la red empresarial, así como administradores de la misma. Son considerados los más comunes, de acuerdo al FBI en el año 2012 estos son los más peligrosos ya que corresponden del 60 al 80% de incidentes reportados. Esto se da por la suplantación de identidad incluso se puede hacer una captura, interpretación y almacenamiento de todos los paquetes de datos que viajan por la red, para su posterior análisis y desciframiento, a este proceso

de “escuchar” todo lo que circula por la red se llama sniffing, los cuales realizar un cifrado a los datos y la información de la empresa de una manera oculta. El robo de la información más común, como se ha visto con anterioridad se da por medio de virus, troyanos y gusanos que pueden traer los usuarios.

1.5.3 Ataque Externo

Estos ataques tiene con objetivo obtener la información de la compañía por medio de personas que son ajenas a la empresa, estas son los hackers o piratas informáticos, los cuales violan la seguridad informática para destruir la información o hacerla inutilizable cambiando la forma de acceder a la misma, y así lograr su objetivo principal de obtener toda la información sensible de la misma y con eso poder tener algún beneficio propio o monetario. Esto, generalmente se suele realizar a través de la red Internet o Intranet y también de servidores que son paralelos a las empresas, es decir servidores de acceso por marcado.

2 TECNOLOGÍA DLP BASADA EN LA LEGISLACIÓN ECUATORIANA Y NORMAS ISO 27001 Y 27002

Gracias a que la tecnología ha ido avanzado, y la información ha sido utilizada, transmitida y receptada a través de sistemas digitales, ha hecho que la población requiera de servicios eficientes para su beneficio, sin embargo, la necesidad de protección de la información que requiere el usuario, es elevada, por lo que buscan una protección adecuada contra el posible uso equivocado de la información sin que haya una limitación o restricción de los beneficios que los sistemas tecnológicos ofrecen.

En el presente capítulo se habla de las legislaciones ecuatorianas relacionadas con la prevención de perdida de datos, así como las normas internaciones ISO 27001 Y 27002, ayudando con mejores prácticas y tecnología aplicada a las empresas PYMES.

2.1 Ley internacional relacionada con la prevención de perdida de datos

En los últimos años, las leyes relacionadas con la protección de información han sido creadas y reformadas para que los nuevos procedimientos electrónicos sean productivos, así como para los ataques y fraudes que se han ido derivando mientras ha ido avanzando la tecnología, sean mitigados.

En la siguiente tabla se verá algunas de las leyes más importantes acerca de la fuga de información.

Tabla 2. Leyes de la Fuga de información

PAÍS	LEY	DESCRIPCIÓN
Estados Unidos	Ley SOX06	Prohíbe prestar a los clientes de auditoría, servicios de contabilidad y otros relacionados con la preparación de cuentas información y datos.
España	Ley Orgánica de Protección de Datos de Carácter Personal	Se sanciona con pena de prisión y multa la obtención o violación de la divulgación de datos privados, estafas electrónicas, hacking, la introducción de virus, entre otras; siempre y cuando es hecho con intención dolosa o cuando es cometido por un funcionario público.
Inglaterra	Ley de Abusos Informáticos (Computer Misuse Act)	Se castiga con cinco años de cárcel o multas ilimitadas a cualquier intento exitoso de alterar datos informáticos.

La ley que está más acorde a este proyecto es la ley SOX (Sarbanes-Oxley), de Estados Unidos debido a que está se aplica en empresas que contribuyen con la bolsa americana. Esta ley regula en su totalidad las funciones financieras como contables y auditorías, penalizando de manera fuerte el crimen que afecte netamente a la corporación. Limita en su totalidad a los servicios de auditoria prestar servicios de cuentas anuales, implementación de sistemas financieros, auditorías internas, consultoría de inversiones, entre otras, a los clientes, que en este caso son las empresas.

Además de las leyes informáticas, también se han ido creando y modificando algunas normas o también llamadas “Buenas Practicas”, las cuales se pueden definir como modelos a seguir para trabajar de manera efectiva, ordenada y segura toda la información personal o de empresas.

En la siguiente tabla se mostraran las principales normas a nivel internacional:

Tabla 3. Principales Normas Internacionales

NORMAS BUENAS PRÁCTICAS	DEFINICIÓN
ISO/IEC	Es un conjunto de estándares desarrollados por la ISO(International Organization for Standardization) y la IEC (International Electrotechnical Commission), los cuales facilitan el manejo del marco de gestión de seguridad de la información que puede ser utilizada para todo tipo de organización, pública o privada
COBIT	Se aplica en los sistemas de información de empresas, en las que se incluyen dispositivos electrónicos tales como computadores, telefonía y ambientes de carácter distribuido.
ITIL	Está formado con mejoras de carácter administrativo que se utilizan en los distintos procesos de las empresas con el fin de mejorar el servicio dado.
COSO	Son informes que detallan los puntos de control interno que maneja cada empresa.

Para este proyecto, se tomara como base la norma ISO/IEC 27000, 27001 Y 27002 que se encuentran dentro de la familia de normas ISO/IEC.

2.1.1 ISO 27000

La Organización Internacional de Normalización, define a la norma ISO/IEC 27000 como un conjunto de estándares que están desarrollados por la ISO e IEC que trabajan para dar un marco de gestión de seguridad de la información utilizable por cualquier tipo de organización sea público o privado.

Tiene la finalidad de proveer un modelo que tiene como base crear, implementar, revisar, monitorear, mantener y mejorar los Sistemas de Gestión de Seguridad de la Información, la cual su diseño e implementación dependerá

de las necesidades, objetivos, requerimientos y procesos que tiene cada una de las empresas.

2.1.1.1 Estructura ISO 27000

La familia de la norma ISO 27000 tiene como objetivo principal dar soporte a las organizaciones grandes, medianas o pequeñas, en la implementación, operación, monitoreo del Sistema de Administración de Seguridad de Información.

En la siguiente tabla se explica cada una de las normas que corresponden a la familia ISO 27000.

Tabla 4. Normas correspondientes a la familia ISO 27000

NORMA	DEFINICIÓN
ISO/IEC 27000	Facilita una visión general de los Sistemas de Gestión de Seguridad de la Información, una explicación a brevedad del proceso Planificar, Realizar, Revisar y Monitorear así como los términos y definiciones que se usan en la familia 27000
ISO/IEC 27001	Es la norma principal para requerir cada uno de los procesos del Sistema de Gestión de Seguridad de la Información, está se certifica por medio de los auditores externos de este sistema en cada una de las empresas.
ISO/IEC 27002	Describe cada uno de los controles y sus objetivos que se recomiendan en cuanto a seguridad de la información
ISO 27003	Es una guía de buena práctica que está en desarrollo. Tendrá la información del uso del modelo PDCA (Plan-Do-Check-Act) así como la guía de implementación del sistema de gestión de seguridad de la información
ISO 27004	Es una norma que está en fase de desarrollo en la cual especificará cada una de las métricas y técnicas aplicables para determinar la eficacia de los sistemas de gestión de seguridad de la información. Se usara para medir cada uno de los componentes de la fase Do de la PDCA
ISO/IEC 27005	Apoya los conceptos generales de la norma ISO/IEC 27001 ayudando a establecer las directrices para la gestión de riesgo que hay en la seguridad de la información
ISO/IEC 27006	Determina cada requisito que se necesita para la certificación de los sistemas de gestión de seguridad de la información y de cada firma de auditoría
ISO 27007	Es una buena práctica que está en desarrollo. Se basará para mostrar una guía de auditorías para el Sistema de Gestión de Seguridad de la Información
ISO/IEC 27011	Es una guía de implementación del Sistema de Gestión de Seguridad de Información, así como una guía de información del modelo PDCA para el área de las Telecomunicaciones
ISO 27031	Está en fase de desarrollo. Hará referencia a una guía para la cyberseguridad.
ISO 27033	Es una norma basada para el área de redes en la cual consistirá de siete partes: Diseño e implementación de seguridad de redes, seguridad en las comunicaciones de las redes mediante VPN´S (Virtual Protocol Network), arquitectura de la seguridad de la red, diseñar escenarios de redes, protección de las comunicaciones que hay entre las redes mediante las puertas de acceso (Gateways), acceso remoto y gestión de la seguridad de la red.
ISO 27034	Está en fase de desarrollo en la que consistirá en dar una guía de seguridad para aplicaciones a usuarios finales

Con cada una de las normas fomentan un enfoque claro y conciso de los procesos de cada empresa durante su implementación, desarrollo y continua mejora de los Sistemas de Administración de Seguridad de la Información.

La eficiencia de cada una de las empresas se tiene que ver con la identificación y la gestión de varias actividades que se relacionan entre sí, debido a que cada uno de los procesos formados se constituye directamente en elemento del siguiente proceso. Adicional al tener interacción y gestión entre los procesos de cada una de las empresas, ayuda a la misma en comprender cada requerimiento de seguridad de su información y la necesidad de establecer objetivos y políticas necesarias para garantizar una fiable seguridad de la información organizacional.

Es importante tener en cuenta que en la operación e implementación de los controles que se aplicaran para la administración de los posibles riesgos que haya en la empresa estén alineados con los posibles riesgos que tenga el negocio en las diferentes áreas, y así con un efectivo monitoreo y revisión de cada proceso haya una mejora de los mismos y así poder crear oportunidades favorables para la empresa.

En la siguiente figura ilustra el Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27000. La figura muestra como el Sistema de Gestión de Seguridad de la información toma como base los requerimientos que la empresa tiene para mantener segur su información, así como las posibles soluciones para satisfacer cada uno de los requerimientos de la empresa.

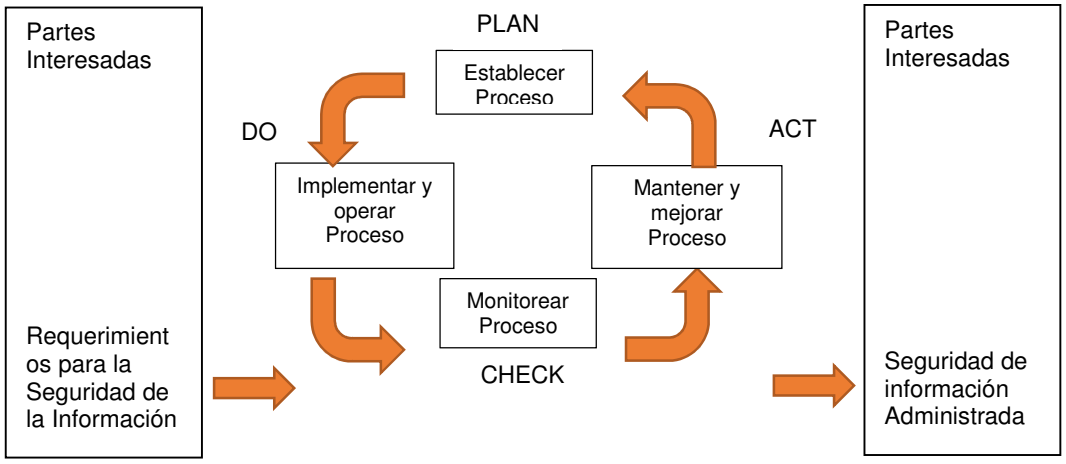


Figura 7. Sistema de Gestión de Seguridad de la Información

Tomado de (International Organization for Standardization - ISO, s.f.)

2.1.2 ISO 27001

La norma ISO 27001 garantiza la implementación, operación y gestión de la implementación de un Sistema de Gestión de Seguridad de la Información. Es considerada la norma más completa que hay para la implantación de los controles, indicadores y métricas que establecen un marco óptimo para la gestión de la seguridad de información de las empresas.

2.1.2.1 Antecedentes y características de la norma

La norma BS7799 empieza desde 1995 con el objetivo de ayudar a las empresas a nivel mundial en las certificaciones de gestión de seguridad de la información por medio de auditorías internas y externas. Las leyes gubernamentales de Gran Bretaña se aplicaron a todas las compañías británicas con el fin de que utilicen esta norma como cumplimiento de la Ley de Protección de la Información. Existió la primera fase en la que se estableció la guía de buenas prácticas, pero no se definió una certificación; en la segunda fase existió la auditoria y certificación de las empresas que han optado por un Sistema de Gestión de Seguridad de la Información (SGSI). Cada una de las partes fue revisada en 1999, la cual la primera se adoptó por la ISO con el

nombre ISO7799. En el año 2000 fue aceptada por más de 80.000 empresas a nivel global y en el 2005 la segunda parte se publica adopta en la ISO, con lo que se publica bajo la norma 27001.

Desde el año 2006, la BSI publicó la BS7799-3:2006 que se centra netamente en la gestión de riesgo de los sistemas de información, con esto ayudará en un futuro a la ISO 27001:2005.

La ISO 27001 está compuesta por procesos que ayudan a evaluar, implementar, mantener y administrar un sistema de gestión de seguridad de la información y un conjunto de controles que ayudan a realizar mejores prácticas en el tema de seguridad de la información.

Con la implementación de esta norma ayudará a cada empresa a definir el sistema de gestión de seguridad de la información así como el mantenerlo ya que facilita la administración de los riesgos y la protección de los activos de información.

Como se mencionó anteriormente la gestión de un sistema se basa en el modelo PDCA (Plan-Do-Check-Act), el cuál es fundamental para el funcionamiento del sistema de gestión de seguridad de la empresa.

En la siguiente figura se muestra cada una de las fases de la gestión de sistema.

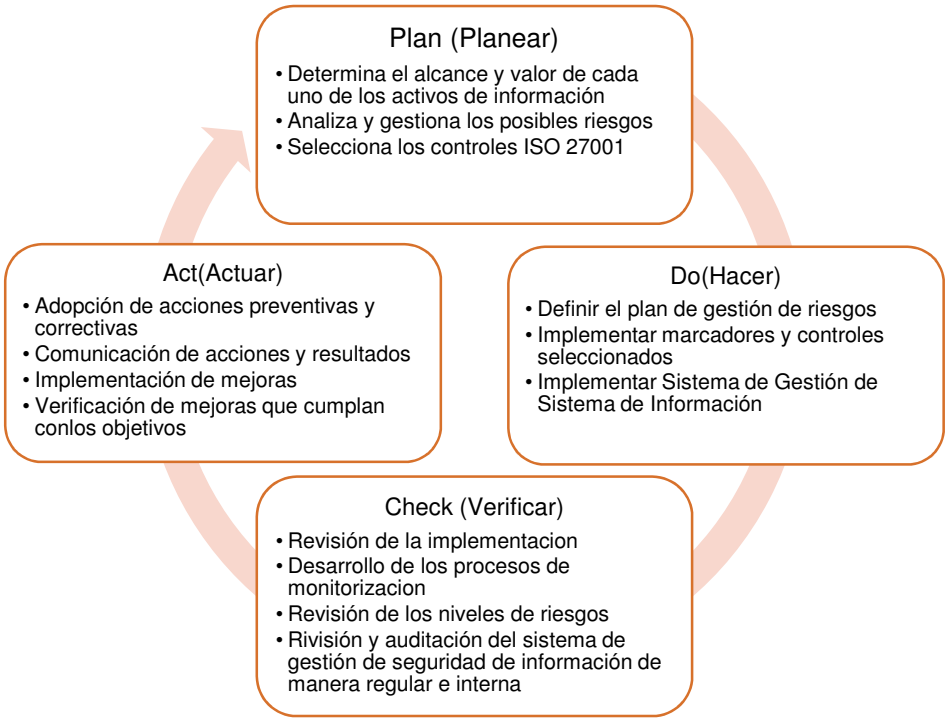


Figura 8. Fases de la Gestión de Sistemas de Información

Tomado de (Tüv Süv Iberia, s.f.)

Fases de la Gestión de Sistemas

Plan: Establecimiento del Sistema de Gestión de Seguridad de la Información.

Para establecer un sistema de gestión de seguridad de Información se debe definir el entorno en el que se manejará el SGSI debido a que toma en cuenta las características de la empresa así como la ubicación de la misma y la información que se tiene que proteger. También se debe definir cada una de las políticas de seguridad a implementar ya que deben estar alineados con los objetivos de la empresa ya que se busca determinar el posible riesgo que puede resultar el que haya fuga de información confidencial. Al tener la política de seguridad ya definida así como el grado de seguridad que se quiere en la empresa, se llega a definir las áreas con más riesgo que necesitan ser administradas definiendo todos los controles a implementar documentándolos para su establecimiento formal.

Do: Implementación y Operación del Sistema de Gestión de Seguridad de Información.

En esta etapa se realiza un plan de tratamiento de riesgo, el cuál identifica todas las responsabilidades, prioridades y acciones que se deben de tomar en cuenta para administrar los posibles riesgos en la seguridad de la información. Al implementar los objetivos de control el saber cada una de las responsabilidades se puede dar cumplimiento de cada uno de ellos. Los programas de entrenamiento a las empresas son necesarios ya que deben saber cómo opera el sistema de gestión de los sistemas de información que se requirió, con esto se llega a implementar procedimientos de detección de los incidentes de seguridad así como su posible tratamiento.

Check: Mantenimiento y constante verificación del Sistema de Gestión de Seguridad de la Información.

En esta etapa se definen los procedimientos de monitoreo ya que se detecta los errores que están en el sistema, se identifica los incidentes y debilidades y se va comprobando el cumplimiento de las actividades de seguridad que han sido asignadas a cada uno de los usuarios o las que estén implementadas a través de la tecnología de la información con el fin de determinar en qué puntos se deben actuar para mitigar las brechas de seguridad.

Otro punto es de verificar la efectividad cada una de las actividades del Sistema de Gestión de Seguridad de la Información, basándose en los resultados de auditorías, incidentes, sugerencias de los distintos elementos que actúan en el sistema.

Se hace una comparación entre el riesgo residual y el nivel de riesgo aceptable para la empresa tomando en cuenta los cambios que se han ido efectuando en la empresa tales como: objetivos, procedimientos en las áreas de negocio, amenazas, tecnología que puedan afectar directamente al SGSI.

Gracias a las auditorías internas se mide la no conformidad del sistema, lo cual permite verificar el estado de no cumplimiento de todos los requerimientos que se han planteado en el proceso.

Act: Mantener y mejorar al Sistema de Gestión de Seguridad de la información.

En esta etapa se hace la implementación de las mejoras tomando las acciones preventivas y correctivas. Se llega a informar a las partes interesadas, todos los resultados, acciones y acuerdos tomados para asegurar que el mejoramiento se apunte a los objetivos planteados al inicio Se registra las posibles acciones que puedan afectar el rendimiento y la efectividad del Sistema de Grsyion de Seguridad de Información debido a que se permitirá observar los puntos débiles que se den a medida que vaya transcurriendo el tiempo.

2.1.3 ISO 27002

Es una guía de buena práctica de seguridad de información en la que muestra muy gran variedad de series de controles de seguridad. Ayuda a resolver los problemas de seguridad de la infraestructura tecnológica y llega a hacer una aproximación a la perfección en la seguridad de la información de cada empresa debido a que va a abarcando a todas las funcionalidades y áreas de las mismas.

2.1.3.1 Antecedentes y características de la Norma

Desde el 01 de Julio del 2007, la ISO 17799:2005 recibe el nombre de ISO/IEC 27002:2005. Fue publicada por primera vez como IS/IEC 17799:2000 en el año 2000 y tras un periodo constante de revisión, en el año 2005, se actualizó el documento como ISO/IEC 17799:2005.

La ISO 27002 se basa en el conjunto de controles de seguridad y de una guía para la implementación del Sistema de Gestión de Seguridad de la Información.

Al igual que en la ISO 27001 este está compuesto por 11 dominios, los cuales se centran en un aspecto de la seguridad de la información, 133 controles de seguridad y 39 objetivos de seguridad.

En la siguiente figura se muestra la distribución de los 11 dominios así como los aspectos de seguridad.

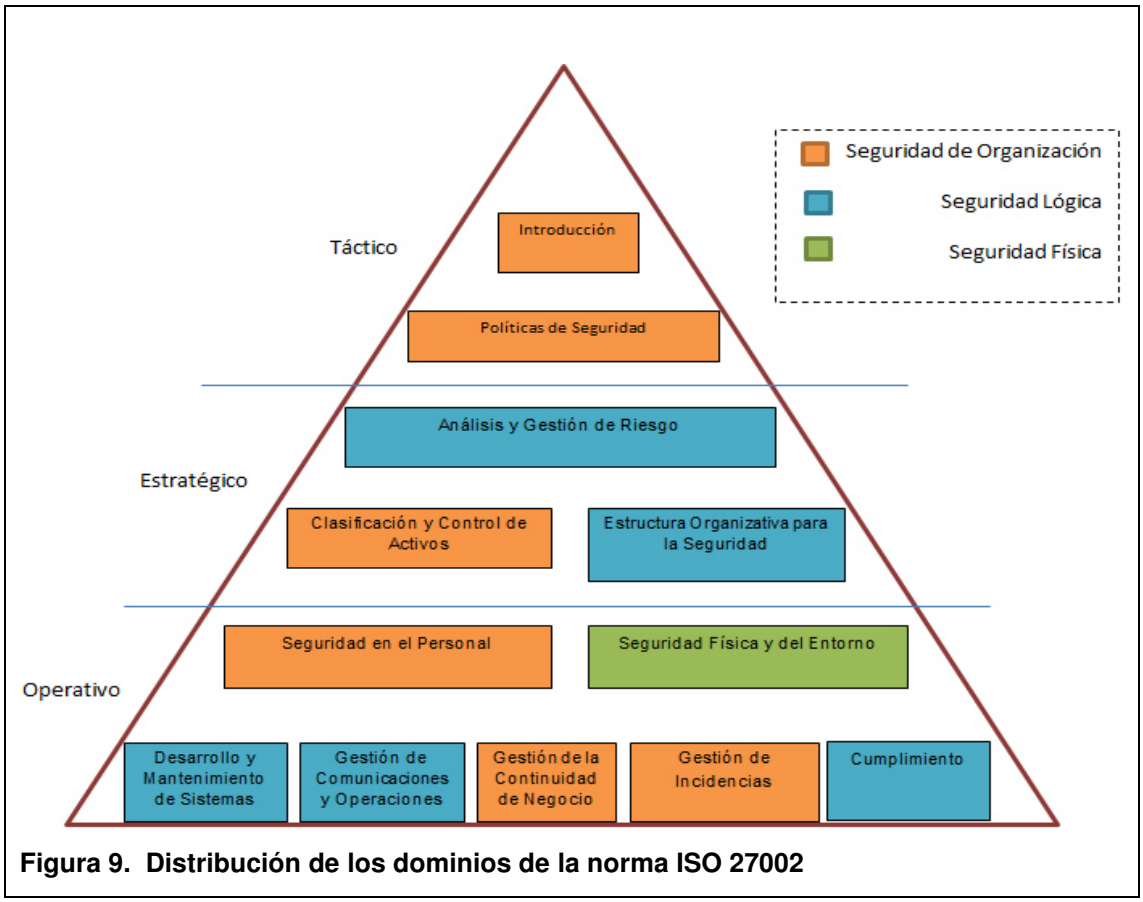


Figura 9. Distribución de los dominios de la norma ISO 27002

Análisis y Gestión de Riesgo: Se identifica cuantifica y prioriza cada uno de los riesgos.

Políticas de Seguridad: Son las políticas de cada empresa, que deben estar bien definidas para que se regule el trabajo de cada área en lo que seguridad de información se refiere.

Estructura Organizativa para la Seguridad: Define cómo se va a tratar la seguridad de información dentro de la empresa con el personal y externamente con clientes y proveedores.

Control y Clasificación de Activos: Se debe tener un control del inventario de los activos que tiene la empresa, así como su clasificación y el responsable de cada uno de ellos.

Seguridad en el Personal: Especificar los límites que se tiene en el acceso y manipulación de la información así como las responsabilidades del personal de la empresa.

Seguridad Física y del Entorno: Consiste en tener instalaciones y ambientes adecuados para mantener en correcto estado la seguridad de información.

Gestión de Comunicaciones y Operaciones: Garantiza la correcta operación de cada uno de los procesos que se han creado, así como toda la comunicación de la empresa. En este domino se ve la división de cada uno de los ambientes de prueba, operación y desarrollo con el fin de evitar problemas futuros en las operaciones del sistema.

Control de Acceso: Se toma en cuenta todas las medidas que se deben tomar para el acceso adecuado de la información, dar autorización a las personas correctas mediante autenticaciones, contraseñas o métodos seguros para el control de acceso a la información sensible.

Desarrollo y mantenimiento de los Sistemas de Información: Consiste en tomar la mejor decisión en adquirir nuevos sistemas, siempre y cuando estén dentro los estándares de calidad así como un eficiente mantenimiento de los mismos.

Gestión de incidentes en la seguridad de la información: Cada una de las empresas deben de tener registros para identificar cada uno de los

responsables de cada incidente que ocurra, así como las posibles soluciones y técnicas de aprendizaje.

Gestión de la Continuidad del Negocio: Cada una de las empresas debe de tener planes de acción alternativos para evitar que los incidentes que puedan sucedes no detenga las operaciones de cada área por largos periodos de tiempo.

Cumplimiento: Este dominio debe hacer cumplir cada una de las políticas, reglamentes, derechos de confidencialidad, entre otros, para que el sistema de gestión de seguridad de información tenga un productivo funcionamiento.

2.2 Legislación ecuatoriana relacionada con la prevención de pérdida de datos

En este punto se definirá y se dará a conocer cada una de las leyes que son aplicables en la república del Ecuador en base a la pérdida de datos y su prevención. En el artículo 81 de la Constitución Política de la República, del Ecuador garantiza el derecho a acceder a las fuentes de información, como mecanismo para ejercer la participación democrática respecto del manejo de información pública y privada, es por eso que en los siguientes puntos se verá la información más detallada de cada una de las leyes de acuerdo a la prevención de perdida de datos.

2.2.1 Ley orgánica de trasparencia y acceso a la información pública

La ley orgánica de transparencia y acceso a la información pública (Información Transparente, 2010); consideran a la Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP), que el acceso a la información pública es un derecho de las personas garantizadas por el estado.

En el Art. 6 muestra que esta ley pertenece a todas las ecuatorianas y los ecuatorianos que son ciudadanos gozando de los derechos establecidos en la constitución ecuatoriana. La nacionalidad ecuatoriana es el vínculo político y jurídico con el estado, son que haya un perjuicio que tenga alguna nacionalidad indígena que hay en el Ecuador plurinacional. La nacionalidad de obtiene por nacimiento por naturalización.

El objetivo de esta ley se establece en el Art. 2 en la que norma y garantiza el ejercicio fundamental de derecho de los ciudadanos ecuatorianos a la información conforme a las garantías colocadas en la constitución política de la república de Ecuador; así como el Pacto Internacional de Derechos Civiles, la convención Interamericana de Derechos Humanos y demás instrumentos internacionales que están en vigencia, que estén signatarios a Ecuador.

Esta ley, según el Art. 3 en el ítem e; es aplicable para las corporaciones, fundaciones y organismos no gubernamentales (ONG), aunque tengan carácter privada y sean encargadas de la administración de bienes o servicios públicos, que mantengan convenios, contratos con instituciones públicas u organismos internacionales, siempre y cuando tenga la finalidad pública.

En el Art. 18 de la nueva Constitución especifica que todas las personas en forma individual y colectiva tienen derecho a buscar, recibir, intercambiar, producir y difundir información verdadera que esté verificada acerca de los hechos, acontecimientos y procesos de interés; así como acceder libremente a la información dada en entidades públicas y privadas que manejan funciones del Estado.

En el Art. 5 define a la ley de información pública a todo los documentos de cualquier formato, que se encuentren en poder de las personas jurídicas e instituciones públicas que se refieran a esta ley, así como contenidos creados o que se hayan producido con recursos del Estado.

2.2.2 Ley de comercio electrónico, firmas electrónica y mensaje de datos

En esta ley se define las regulaciones de los mensajes de datos, así como las firmas electrónicas, certificaciones, contrataciones telemáticas y electrónicas, prestación de servicios a través de las redes de información, comercio electrónico y protección del usuario que utilice estos sistemas.

La seguridad en el área de comercio electrónico así como la red de internet debe proteger la seguridad física de los elementos de hardware y periféricos; que pueden ser afectados por acciones equivocadas incluso calamidades naturales. También debe de proteger los sistemas de información utilizados y el contenido de los mismos que pueden ser mal utilizados u alterados por personas externas o de la empresa.

La protección de los entornos que utiliza las empresas es esencial ya que se puede delimitar áreas de Intranet e Internet como tal, protegidas con cortafuegos los cuales realizan tareas de vigilancia y control de acceso. La protección de los mensajes y comunicaciones se basa en técnicas y soluciones para dar la respectiva seguridad de la información transmitida y receptada.

La ley de Comercio Electrónico del Ecuador en su disposición número nueve se define como toda transacción comercial realizada en parte o en su totalidad a través de redes electrónicas. Esta ley abarca todo tipo de acceso a la información comercial y digital, así como transacciones electrónicas, contratación pública entre otras.

Los objetivos de esta ley en el Ecuador son:

- Proteger al usuario que utilice este servicio, ayudándole con la protección de su identidad del aceptante y ofertante que avale los desarrollos tecnológicos sobre seguridad en materia de comercio electrónico.

- Dotar de un marco jurídico en operaciones y transacciones tengan como escenario el Internet.

- Homologar los documentos digitales dentro de la red que son considerados con el mismo valor jurídico que los documentos escritos.

- Introducir o modificar las infracciones que pueden originarse de las operaciones virtuales dentro del comercio electrónico.

En Ecuador se adoptó como esquema de seguridad las claves públicas basadas en la Ley Modelo UNCITRAL de las naciones unidas para el comercio electrónico, la que toma como prioridad firmas electrónicas y entidades de certificación.

Esta ley contempla ocho secciones las cuales son tratadas a continuación, en las cuales se tomaran en cuenta 4, debido a que estas se enfatizan en los objetivos del proyecto:

Sección Primera – Objetivo de la Ley:

De las Firmas Electrónicas.- Se define lo que es firma digital, así como los requisitos para que sean válidos y su duración. *Artículos del 13 al 19.*

De los Certificados de Firma Electrónica.- Define cada uno de los puntos que se toman en cuenta para obtener los certificados de firma electrónica, así como su reconocimiento a nivel internacional. *Artículos del 20 al 28.*

De las Entidades de Certificación de Información.- Define cada una de las obligaciones y responsabilidades que cada una de ellas deben de tener en cuanto a la protección de los datos de sus contratantes, tomando en cuenta cada uno de los servicios que ofrecen al cliente y su funcionamiento. *Artículos del 29 al 35.*

De los organismos de promoción y difusión de los servicios Electrónicos, y de regulación y control de las entidades de certificación acreditadas.- Define los organismos de promoción, difusión, regulación, registro y control de los servicios y comercio electrónicos. Además se toma en cuenta la autorización, registro, y regulación de las entidades de certificación acreditadas en el Ecuador. *Artículos del 36 al 43.*

Sección Tercera-Servicios Electrónicos

De los Servicios Electrónicos.- Establece el cumplimiento de la Ley en cualquier tipo de actividad financiera, transaccional, entre otras que ocupen redes electrónicas. *Artículo 44.*

De la Contratación Electrónica y Telemática.- Se establece la validez de los contratos electrónicos, así como su apertura y relación con el contrato electrónico. En caso de litigio se establece las normas para su proceso. *Artículos del 45 al 47.*

De los derechos de los usuarios o Consumidores de servicios electrónicos.- Se establece derechos y obligaciones de los usuarios que utilizan los diferentes servicios electrónicos. *Artículos del 48 al 50.*

De los Instrumentos Públicos.- Reconoce la validez jurídica de los mensajes de datos autorizados o expedidos por la autoridad competente y firmada electrónicamente. *Artículo 51.*

Sección Cuarta- De las Pruebas

De la Prueba.-Se definen los diferentes medios de prueba así como la impugnación de certificados y firmas electrónicas, Se establece procedimientos para que se pueda efectuar la prueba requeridas para los procedimientos.

Sección Quinta- De las infracciones informáticas

De las Infracciones Informáticas.- Son aquellos que definen sanciones por cualquier delito informático en el Ecuador en lo que tiene que ver con robo de información, mal uso de datos sensibles como claves de accesos, obtención no autorizada de información, falsificación electrónica, daños a la infraestructura tecnológica. *Artículos del 57 al 64.*

Efectos de la Ley: Reconoce como fuerza jurídica y validez de los mensajes de datos, de cualquier tipo de forma en la que estén, así como la información que éstos contengan teniendo igual valor jurídico que los instrumentos públicos y privados.

Firma Electrónica o digital.- La firma digital es usada de manera prioritaria dentro de las redes como Internet y el comercio electrónico en Ecuador ya que el ambiente en el que se maneja es seguro.

La ley establece que el mecanismo utilizado para la firma digital debe ser criptográfico, de modo que utiliza una Infraestructura con 2 claves diferentes: una para cifrar y otra para descifrar.

Entidades de Certificación.- Son las empresas unipersonales o personas jurídicas que emiten certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica El certificado es muy importante ya que es respaldo de la firma digital.

Por la importancia de los servicios que prestan las entidades de certificación la Ley ha puesto especial énfasis en que dichas personas naturales o jurídicas: cumplan estrictamente los siguientes requisitos:

- Encontrarse legalmente constituidas, y estar registradas en CONATEL.

- Proceder de forma inmediata a la suspensión o revocatoria de certificados electrónicos previo mandato del Superintendente de Telecomunicaciones, en los casos que se especifiquen en esta ley.

- Mantener una publicación del estado de los certificados electrónicos emitidos.

- Demostrar solvencia técnica, logística y financiera para prestar servicios a sus usuarios.

- Garantizar la prestación permanente, inmediata, confidencial, oportuna y segura del servicio de certificación de información.

- Mantener sistemas de respaldo de la información relativa a los certificados.

- Proporcionar a los titulares de certificados de firmas electrónicas un medio efectivo y rápido para dar aviso que una firma electrónica tiene riesgo de uso indebido.

Protección a los usuarios del Comercio Electrónico

La Ley de Comercio Electrónico garantiza los derechos de los usuarios que realizan transacciones de cualquier tipo en la red, así como el comercio electrónico que ellos realicen Art. 39

2.2.3 Ley de Propiedad Intelectual

Gracias al SICE (Sistema de Información sobre Comercio Exterior), la ley de propiedad intelectual maneja 3 secciones, que se las puede ver en su artículo y son los siguientes.

- Derecho de autor y los derechos conexos: Este punto hace referencia a las obras artísticas o científicas, tales como diseños arquitectónicos o sistemas informáticos. Su funcionalidad es ayudar que los derechos sobre sus interpretaciones o ejecuciones sean de su auditoria.

- Propiedad industrial: Se refiera a la inclusión de invenciones, patentes, marcas, entre otros en cada proyecto que ayude a la industria ecuatoriana.

- Variedades vegetales. Esta es una ley de carácter internacional, la cual tiene como finalidad expandir los derechos de autor fuera de su país y así ayudar a la comunidad global.

Según el Art. 289 de la Ley de Propiedad Intelectual del Ecuador, se podrá demandar:

- La cesación de los actos violatorios.

- El comiso definitivo de los productos u otros objetos resultantes de la infracción, el retiro definitivo de los canales comerciales de las mercancías que constituyan infracción, así como su destrucción.

- El comiso definitivo de los aparatos y medios empleados para el cometimiento de la infracción.

- El comiso definitivo de los aparatos y medios para almacenar las copias.

- La indemnización de daños y perjuicios.

- La reparación en cualquier otra forma, de los efectos generados por la violación del derecho.

- El valor total de las costas procesales.

2.2.4 Ley Especial de Telecomunicaciones

Se resume a la última reforma de la ley especial de Telecomunicaciones aplicada por el Consejo Nacional de Telecomunicaciones en los siguientes puntos:

Artículo 6. Son servicios finales de telecomunicaciones aquellos que proporcionan la capacidad completa para la comunicación entre usuarios, incluidas las funciones de equipo terminal y que generalmente requieren elementos de conmutación.

Artículo 15. Las redes privadas serán utilizadas únicamente para beneficio de un solo usuario y no podrán sustentar, bajo ninguna circunstancia, la prestación de servicios a terceros. Las redes privadas no podrán interconectarse entre sí, ni tampoco con una red pública.

Artículo 39. Toda conexión o interconexión entre redes de telecomunicaciones debe efectuarse de manera eficiente, en concordancia con los principios de igualdad de acceso y trato no discriminatorio, para lo cual todo concesionario deberá ofrecer las mismas condiciones técnicas, económicas y de mercado a quien solicite la conexión o interconexión con la red operada.

La Ley Especial de Telecomunicaciones considera que es conveniente proveer a los servicios de telecomunicaciones de un marco legal que vaya acorde a la importancia, complejidad, magnitud, tecnología y especialidad de dichos servicios, con los que puedan desarrollar criterios de gestión empresarial y beneficio social; asegurando, así una adecuada regulación y expansión de los sistemas radioeléctricos y servicios de telecomunicaciones a la comunidad y mejorar permanentemente la prestación de los servicios existentes, de acuerdo a las necesidades del desarrollo social y económico del país.

2.2.5 Constitución de la república (Habeas Data)

Es la constitución que garantiza la defensa de los derechos humanos, en lo que refiere a agresiones o amenazas desde la difusión de datos personales que están en las nuevas tecnologías de la información como base de datos, correos electrónicos, redes sociales, entre otros.

El Habeas Data permite a cualquier persona de carácter jurídico o natural conocer, acceder, autorizar, actualizar, anular la transmisión de los datos a otras personas que trabajen en determinadas bases de datos (Artículo 92).

Su finalidad es garantizar que no haya una pérdida de datos y no se vulnere los derechos de libertad tales como el derecho de la integridad personal y familiar o el derecho al honor y al buen nombre que se encuentran formalizados en los artículos 3, 7, 18, 19, 20 y 66 de la República del Ecuador.

3 MODELO DE SEGURIDAD PARA LA PREVENCION DE PERDIDA DE DATOS EN LAS EMPRESAS PYMES

3.1 Identificación de la información

Para realizar el modelo de prevención de pérdida de datos se debe tener en cuenta la información de la empresa que se va a dar la solución.

La empresa escogida para realizar la implementación del presente trabajo es Winchas Tarqui Ecuador debido a que es una empresa líder en el mercado ecuatoriano en dar asistencia técnica vehicular en consecuencia de algún tipo de falla mécanica o daños generados mediante accidentes de tránsito a clientes de empresas nacionales como Ecuasistencia. En la actualidad no cuenta con una buena gama de seguridad informática, tanto en infraestructura lógica como física, por lo que al hacer un estudio previo se logró definir las áreas que más vulnerabilidades han generado a través de los años las cuales son el área de Logística, Sistemas y Finanzas.

3.1.1 Identificación y clasificación de la información

La información que tiene la empresa debe de ser identificada y clasificada para tener en cuenta las necesidades, su grado de prioridad y la protección que requiere, es por eso que en base la ISO 27000 y 27001 se realiza la primera fase de identificación y planificación de la información que ha sido proporcionada por la empresa.

Se inicia con la identificación de las áreas funcionales de la empresa así como cada información que manejan y la interacción que tiene con otras áreas; de igual manera se tiene una descripción el tipo de información que se está utilizando y el motivo por el cual están interactuando con las otras áreas de la empresa. Cada una de las tablas mostradas a continuación tiene su desarrollo en el anexo A del presente trabajo.

En la siguiente tabla se muestra las áreas funcionales de la empresa que fueron electas, así como la interacción que tiene cada una de ellas.

Tabla 5. Áreas Funcionales, de interacción de la empresa

Área Funcional	Áreas de Interacción	Tipo de Información	Descripción del tipo de información
Recursos Humanos			
Finanzas			
Logística			
Sistemas			

El área funcional es cada uno de los grupos de trabajos que existen en la empresa y de los cuales hace como tal la organización. El tipo de información es aquel donde se nombra todos y cada uno de los tipos e información que son utilizados en las áreas funcionales de la empresa. En las áreas de interacción se describe que se tiene en común con el tipo de información colocada y las áreas que se pueden tratar. La descripción del tipo de información ayuda a conocer con más detalle la función que cumple la información en las áreas de la compañía.

Una vez que se tiene identificadas las áreas de la empresa así como los tipos de información que tienen, se determina el valor que tiene la información para la empresa, se debe tomar en cuenta que la información que se utilice en 2 áreas diferentes se debe de tomar con valores individuales ya que puede ser más valiosa para un área que para otra.

Para tener una valoración efectiva se debe de tomar en cuenta la justificación que se da a cada tipo de información tales como la frecuencia que se utiliza y su recepción.

En la siguiente tabla se tomará en cuenta la tabla definida anteriormente con los parámetros mencionados anteriormente.

Tabla 6. Áreas funcionales de interacción en base a la frecuencia de uso de la información de la empresa

Área Funcional	Áreas de Interacción	Tipo de Información	Descripción del tipo de información	Frecuencia de Uso	Valor para la Empresa	Recepción	Ranking
Recursos Humanos							
Finanzas							
Logística							
Sistemas							

La frecuencia de uso se determina en base a cuanto se ocupa la información en las áreas de la empresa. El valor será tomado en una escala de 1 a 5 siendo 1 el de menos frecuencia y 5 el de mayor frecuencia.

La recepción es considerada como recibe la información de la empresa los usuarios que trabajan en la misma como colaboradores externos, la cual se basa en los siguientes aspectos:

- TEC: terceros, empleados y contratistas.
- SA: socios y asociados.
- C: Clientes.

El valor de la empresa será tomado en una escala de 1 a 5 en la cual se demostrará la importancia en beneficios y otros puntos para la compañía en un futuro.

El ranking ayuda a definir los niveles que tiene la información de acuerdo al valor crítico definido por la empresa, se tomará en una escala de 1 a 5 siendo 1 la de menos importancia y 5 a de mayor importancia.

Al definir los valores de la información de manera correcta, esto ayudará a definir los posibles riesgos a las que está expuesta y poder determinar la seguridad que esta necesita.

3.2 Infraestructura Tecnológica

La empresa consta con algunos aspectos tecnológicos para el buen desempeño de la misma, las cuales fueron estudiadas y verificadas entorno a la fase operativa en la seguridad física de la ISO 27002, así como la ley de comercio electrónico del Ecuador en la que la protección de la infraestructura de cada empresa es esencial así como la seguridad de los datos de la misma. En los siguientes puntos se determinará la infraestructura tanto de hardware como de software de la empresa.

3.2.1 Infraestructura de Hardware

La empresa consta con un servidor de red el cual trabaja con Windows Server 2008 R2, colocado de manera virtual por medio de WMWARE PLAYER, colocado en una máquina portable HP. En base al Control y Clasificación de Activos de la ISO 27002, la clasificación de cada uno de los equipo que manejan los usuarios, incluido el servidor están definidos por equipos HP modelo 2570p.

En la siguiente tabla se determinan las características de los equipos que maneja la empresa.

Tabla 7. Características y especificaciones técnicas de equipos empresariales

Elementos	Característica
Procesados	Intel I5
Memoria RAM	8GB
Tarjeta Gráfica	Intel
Tipo de Pantalla	LED
Conectividad	Puerto Ethernet Puerto USB 2.0 Puerto USB 3.0
Conectividad Inalámbrica	4G Bluetooth Wi-Fi

3.2.2 Infraestructura de Software

Teniendo en cuenta la fase de Desarrollo y Mantenimiento de los Sistemas de Información de la ISO 27002; en la que se verifica si cada uno de los sistemas cumplen con los estándares, se comprobó que cada uno de los equipos que se manejan en la compañía tienen el Sistema Operativo Windows 7 Enterprise, así como herramientas ofimáticas tales como Microsoft Office 2010 y antivirus McAfee otorgado por medio de licencias.

3.2.2.1 Aspecto de la Herramienta DLP seleccionada

La herramienta escogida gracias al cuadrante de Gartner, vista en capítulos anteriores, es de la corporación McAfee. McAfee DLP Endpoint Protection, es una herramienta implementada para ayudar a las empresas a proteger la información sensible o confidencial, permitiendo que el manejo de la información pueda ser controlado mediante políticas. La herramienta que se proporciona a la empresa se dirige entono a los estándares de la ISO 27001 Y 27002, tomando en cuenta las fases de políticas de seguridad así como el control de acceso a la información.

El Host DLP Endpoint Protection, es el núcleo para administrar la información, la cual está alimentada por el software ePO (McAfee EPolicy Orchestrator). Con este sistema se analiza, ajusta e informa el uso de los datos en uso, en reposo y en movimiento. Los datos en reposo son los que se encuentran almacenados en los servidores, los datos en uso son aquellos que están en cada una de las actividades diarias de los usuarios y los datos en movimiento son los que se envían a través de la red.

Para la comunicación directa entre la herramienta McAfee EPolicy Orchestrator y la herramienta McAfee DLP Endpoint, es indispensable tener el servicio McAfee WFC (Windows Communication Fundation), ya que podemos obtener la base de datos de los clientes así como la conectividad de la misma.

McAfee DLP Endpoint Protection, es la herramienta de punto final que inspecciona el contenido de cada usuario de la empresa, así como su estación de trabajo. Utiliza tecnología de descubrimiento avanzado para identificar el contenido de cada información. Incorpora también la gestión de cada dispositivo externo previniendo la transmisión de los datos sensible, evitando el uso no autorizado de dispositivos de medios extraíbles.

3.3 Riesgos

La empresa no posee un sistema para proteger los datos de sus clientes, así como de la información de cada uno de los empleados. La información puede ser vista por todas las personas alineadas a la empresa, así como externas; lo que ha provocado que la información sea vista de manera general. En el tema financiero, la información sensible está expuesta para ser visible con cada uno de los usuarios de la compañía, por lo que el riesgo en términos generales, es bastante alto. En los siguientes puntos se realizará un análisis de cada una de las vulnerabilidades técnicas y el nivel de gestión de seguridad que se necesitan con la que se cumplen los puntos la segunda fase Do (hacer) de la ISO 27001 analizadas en el capítulo 2 del presente trabajo.

3.3.1 Análisis de vulnerabilidades técnicas

Al tomar en cuenta todo el conocimiento de la infraestructura física y lógica de la empresa, y basándonos en la ley de comercio electrónico, firmas electrónicas y mensaje de datos, así como en la ley especial de telecomunicaciones y la ley orgánica de trasparencia y acceso a la información pública de Ecuador, las cuales trabajaron conjuntamente con la fase de Análisis y Gestión de Riesgo de la ISO 27002, se logró determinó la siguiente tabla en la que se definió cada uno de los elementos que fueron puestos a revisión y su vulnerabilidad en el medio de la empresa.

Tabla 8. Elementos de revisión de la empresa y vulnerabilidades

Elementos de Revisión	Vulnerabilidad
Físico	La empresa está establecida en una propiedad privada, con instalaciones eléctricas nuevas. Consta con un cetro de datos pequeño que está inhabilitado, ya que quieren costear el precio del mismo implementado un sistema virtual.
Lógico	La empresa no consta con un sistema de servidores, por lo que la información está almacenada en el equipo de trabajo de cada usuario, la administración de la información es compartida por la mayoría de los usuarios, por lo que la información sensible está con un riesgo máximo.
Seguridad	La empresa tiene un buen sistema de seguridad física, por lo que los equipos físicos no tienen ningún inconveniente de que sean extraviados, lo que se refiere a la información la vulnerabilidad es alta por lo que la empresa ha tomado medidas para que esto se disminuya en un gran porcentaje.

3.3.2 Nivel y Gestión de Seguridad

Al momento de haber realizado la identificación y el análisis de las áreas funcionales de la empresa, así como de la información y la valoración de cada una de ellas y sus vulnerabilidades, que son muy altas. Se toma en cuenta el TAO (Tasa Anual de Ocurrencia); la cual se calcula con la relación de los incidentes registrados en la empresa de un año anterior, que está estimada por cada jefe de cada área con el número total de la información almacenada.

Con esto se puede determinar la gestión de los incidentes dados y determinar un riesgo real anualmente. También se establece el impacto generado y que se materializan en los empleados, contratistas o terceros, así como los clientes y los socios-accionistas de la empresa.

El TAO está definido por la siguiente ecuación:

$$TAO(\%) = \frac{Número\ de\ incidentes\ registrados\ en\ el\ año\ anterior}{Número\ Total\ de\ información\ almacenada} x100 \qquad \text{(Ecuación 1)}$$

En la siguiente tabla, se mide como se podrá obtener un mayor control en el análisis de riego obtenido de la empresa.

Tabla 9. Control de análisis de riesgo de la empresa

Área	Tipo de Información	Riesgo	% TAO	Impacto (1 al 5)			Total	%+-
				ECT	C	SA		

Para trabajar en la gestión de los incidentes de seguridad, se debe de tomar en cuenta la información que puede resultar ser expuesta y que pueden ser dañados de alguna manera. Para esto, en la siguiente tabla se observa los registros de estos incidentes y el impacto generado en la empresa.

Tabla 10. Registro de incidentes e impacto generado en la empresa

Identificador de Seguimiento	Incidente	Área	Tipo de Información	Impacto (1 al 5)			Solución	Observación
				ECT	C	SA		

3.4 Políticas y Procedimientos

Para llevar una correcta protección de la información de la empresa se definió las políticas y procedimiento en base a las fases de Políticas de Seguridad, Estructura Organizativa para la Seguridad, Seguridad en lo Personal y Control de Acceso de la ISO 27002 debido a que en cada uno de ellos ayudará considerablemente a todo el ciclo de la información es decir desde su creación, uso, almacenamiento y eliminación de la misma.

Los acuerdos de confidencialidad es uno de los elementos más importantes ya que se define la información sensible que se pueda manejar por medios electrónicos, también es necesario definir las políticas y responsables del

manejo de la misma, ya que cualquier mala manipulación de la misma se dará sanciones internas de la empresa así como externas.

En la empresa donde se ejecutó este proyecto; se definieron las políticas de la empresa que se dan a los usuarios entrantes, para que no haya ningún tipo de inconveniente en un futuro.

Cada uno de los usuarios que ingresa a la empresa debe de firmar un documento en el cuál acepta todas las políticas y procedimientos de la misma.

La empresa tiene la difusión de las políticas de seguridad por media de correo electrónico, así como boletines y en la página web de la misma; por lo que la concientización al usuario está sobre las expectativas.

3.4.1 Ciclo de vida de la información

En este punto se observa el ciclo de vida que toma la información obtenida con anterioridad; así como definir algunas políticas y procedimientos en la creación, uso, almacenamiento, destrucción de la misma.

3.4.2 Creación y uso de la información

Se define tomando en cuenta como punto de partida el área de recursos humanos ya que se vio los roles y responsabilidades de cada empleado, así como contratistas y terceros. Cada uno de ellos tiene acceso a la información sensible al firmar un acuerdo de confidencialidad de la misma, así como derechos de propiedad intelectual. Todos los sistemas de información están a la disposición de cada uno de ellos; siempre y cuando tengan el debido acceso y gestión de los activos de la empresa.

La información se crea y se maneja únicamente en los equipos autorizados de la empresa; por lo que al definir cada perfil de cada empleado, nos ayuda a

establecer políticas de permisos y restricciones de acuerdo al área en la que se esté trabajando.

3.4.3 Condición de uso

En la siguiente tabla, el departamento de Recursos Humanos define cada uno de los permisos otorgados para el manejo de la información así como los niveles de los mismos, los cuales fueron definidos en base a las fases de Gestión de Continuidad del Negocio, Control de Acceso de la ISO 27002.

Tabla 11. Permisos otorgados a usuarios para manejo de información

Código Empleado	Nombre	Cargo	Área Funcional	Tipo de Información	Permisos	Nivel de Seguridad

3.4.3.1 Monitoreo de Seguridad y Gestión de Derechos de la Información

En base a la etapa de verificación de la ISO 27001, se debe definir un área responsable de monitorear y validar la seguridad de la información, es este caso se asignó el área de Sistemas; ya que ellos están vinculados directamente con la validación de cada una de las actividades de seguridad así como la ejecución de las mismas en base a las políticas de seguridad de la información.

La empresa determinó que era necesario colocar las siguientes políticas de información para el monitoreo a realizarse por el área de sistemas, las cuales se fundamentaron en la fase de Gestión de Comunicaciones y Operaciones así como la Gestión de Incidentes en la seguridad de la información de la ISO 27002.

- Se deben realizar un reporte donde se registren todos los intentos de acceso a la red así como de todos los eventos ocurridos.

- El reporte debe constar de los siguientes puntos

  - Registro de eventos claves ocurridos (hora, fecha y ubicación).

  - Tipo de evento ocurrido.

  - A que archivos se tuvo acceso.

  - Registrar los intentos de acceso fallidos y rechazados.

  - Cambios efectuados en la configuración del sistema.

  - Quienes están involucrados en el evento (cuenta de usuario o dirección IP).

  - Registro de fallas repostadas por los usuarios relacionadas con la información.

Cada uno de los empleados, así como sus clientes finales conocen todas las políticas establecidas en la empresa las cuales se definen en el manejo correcto del correo electrónico corporativo, el uso de las herramientas de comunicación y la protección de los datos corporativos y personales que están en cada uno de los dispositivos de la empresa. Este conocimiento se establece por medio de inducciones capacitaciones del área de sistemas que se da y su posterior entrega de documentos de políticas informáticas, así como protección de los datos, con el objetivo de evitar el mal uso de la información y así generar pérdidas y fugas de la misma.

Cada una de las áreas de la empresa clasificó la información de acuerdo a su relevancia que son: pública, privada, confidencial y restringida; así como el número de usuarios que pueden tener acceso a la información.

3.4.4 Almacenamiento de la Información

La empresa consta con un servidor virtualizado en el cuál toda la información está almacenada; pero no se deja a un lado el posible almacenamiento de la información en dispositivos externos que cada área tiene; por lo que en los siguientes puntos se define la distribución de la información así como el control de los accesos y el manejo de los respaldos.

3.4.4.1 Distribución de la Información

La información está clasificada en base a las áreas funcionales de trabajo así como su tipo y las fases de Control de Acceso y Estructura Organizativa para la seguridad de la ISO 27002, por lo que la restricción de los accesos es una de las prioridades de cada una de ellas.

Almacenar la información en dispositivos extraíbles y la protección de la información receptada y emitida por medio del correo electrónico, es una de las políticas que solicitó la empresa realizar, ya que en años anteriores se han encontrado una gran cantidad de falencias y fugas de información por este medio. En caso de incumplir con las políticas, se aplicarán las sanciones establecidas por la misma en la que se ven afectados los usuarios involucrados. Estas incluyen suspensiones que van de 1 a 2 semana, multas de infracción económicas que son medibles dependiendo de qué cantidad de información se perdió. Las multas económicas van desde 100 a 200 dólares americanos en el caso de que la información sensible haya sido emitida a la competencia, previa investigación, se aplicará el despido intempestivo con visto bueno por la empresa.

En la siguiente tabla, cada una de las áreas de la empresa definirán los equipos de trabajo y dispositivos extraíbles a utilizar.

Tabla 12. Utilización de equipos de trabajo y dispositivos extraíbles

Nivel de Información Analizada	Área	Tipo de Información	Usuario	Equipo	Dispositivo

3.4.4.2 Control de accesos y el manejo de los respaldos

La empresa consta con políticas de control de accesos tanto físicos como lógicos implementados en función a la ISO 27002 en sus fases de Control de Acceso y Seguridad Física y del Entorno. Los accesos físicos están colocados sistemas de ingreso a la empresa; así como equipos contra incendios en el área de sistemas, las condiciones ambientales en las que están los equipos también están definidas. Sólo se permite el acceso al personal autorizado y al personal que haya sido previamente aprobado para ingresar.

El control de acceso lógico se basa en la creación de las cuentas de los usuarios tanto empleados como externos, en donde se controlan los privilegios en el acceso a la información; las contraseñas dadas a los usuarios deben ser únicas e intransferibles para cada uno de los usuarios.

La protección de la información en las redes de cómputo de la empresa están en buenas condiciones ya que cada procedimientos y responsable para la gestión de equipos remotos está a cargo el área de sistemas, ya que tiene controles en redes públicas e inalámbricas para la protección de la integridad y confidencialidad de cada uno de los datos transmitidos.

El respaldo de la información debe estar almacenado en aquellos equipos de cómputo en los que tengan la funcionalidad del almacenamiento del mismo. Cada uno de los usuarios en sus equipos consta con este sistema ya que se debe salvaguardar la información de tal forma que garantice la continuidad del negocio.

Cada una de las áreas definió el tipo y nivel necesario de respaldo de la información, pidiendo que cada usuario sea responsable de realizar un respaldo interno de la información que está creando y/o utilizando dentro de la empresa. En caso de que la información respaldada sea critica o confidencial se debe proteger por medio de una seguridad.

Los respaldos realizados por los usuarios se llevaran a cabo cada 15 días, por lo cual el área de Sistemas es el único que tiene todo el control a la información y es el único en autorizar en caso de ser necesario la instalación de algún respaldo de información previamente solicitado por algún usuario.

En la siguiente tabla se identificará el control de los respaldos que se realizan en cada una de las áreas funcionales de la empresa.

Tabla 13. Control de Respaldos

Responsable	Área	Tipo de Información	Medio de Respaldo	Autorización	Fecha

3.5 Eliminar la Información

La empresa definió las políticas que se tiene que aplicar en relación a la seguridad de la información cuando algún usuario termina su relación laboral con la empresa o sus actividades dentro de esta cambian, con el único fin de evitar el mal uso de la información a la cual ya no deberán acceder. De igual manera se definió cada una de las políticas para la correcta entrega de la información de manera segura.

En caso de que algún empleado deje de trabajar para la empresa o sea asignado a una posición nueva, se debe retirar los equipos asignados para su trabajo, hacer un respaldo de la información correspondiente a la empresa, dar de baja al usuario en carpetas y documentos compartidos así como sistemas que controlaba. El área de sistemas tendrá un manejo del historial de la

información, si es que se necesite en futuras ocasiones poder dar a la persona que sea responsable o asignada para la información. Cada perfil de usuario que esté configurado en el equipo será eliminado para evitar su acceso en futuras ocasiones.

3.5.1 Destrucción de la información en modo seguro

Cada uno de los procedimientos que van relacionados al borrado seguro y destrucción de medios, la empresa requirió para garantizar que la información confidencial sea mal utilizada por medio de una eliminación o el reutilización de los dispositivo de almacenamiento.

Los equipos en la cual la vida de depreciación es mayor a 3 años, se prepara a subasta del mismo o destrucción, por lo que el área de sistemas tiene que hacer una valoración de la información que hay en cada dispositivo para su posterior eliminación, en tal caso de que la información este en vigencia se respalda en un disco duro externo por el lapso de tiempo de 1 año. En el caso de reutilización de los mismos hará un borrado seguro de sistema operativo de la empresa. Este borrado se realiza con un programa llamado Blancco, el cual da de baja todo el sistema operativo de la empresa, permitiendo la instalación de un sistema operativo comercial fuera de compañía.

3.6 Bosquejo de Implementación de tecnología DLP

Para completar el ciclo gestión de un sistema informático, basándose en la cuarta etapa de la ISO 27001 en la siguiente figura; se encuentra el bosquejo de implementación de la tecnología DLP en la empresa.

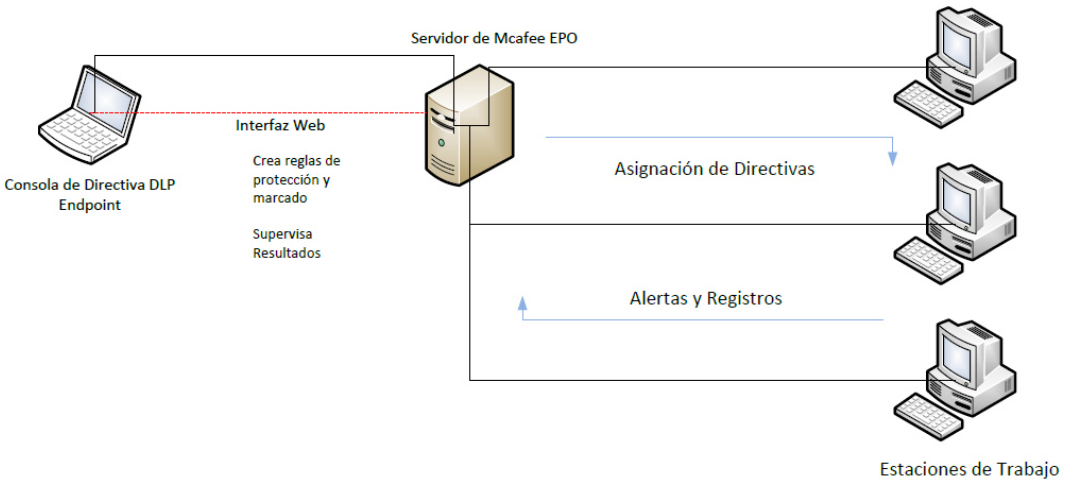


Figura 10. Bosquejo de la Implementación de tecnología DLP

La consola de directivas DLP Endpoint es la interfaz que administra y aplica las políticas y directivas de seguridad de información en la empresa. En la consola se accede al sistema McAfee EPO en la cual asigna las directivas a las 3 estaciones de trabajo a implementar.

3.6.1 Solución para la administración de seguridad y DLP

La tecnología en la que se fundamenta la implementación de la herramienta de prevención de pérdida de datos, fue tomando forma gracias a las 11 fases del dominio de la ISO 27002, vistas en el capítulo 2 de este trabajo, las cuales van protegiendo la información de la empresa a lo largo de su ciclo de vida para su mejor utilización y manejo ya que va generando perfiles de acuerdo al área de trabajo generando así permisos y restricciones de la información a utilizar.

Se garantiza la cobertura completa del sistema ya que se puede administrar de manera eficaz la información desde su creación hasta la eliminación de la misma, es por eso que la solución DLP ofrecida en este trabajo, da a conocer o describir cada uno de los datos de información, los cuales definen que tipo de dato es sensible o confidencial, ya que al controlar cada una de estas actividades se permite realizar un análisis mucho más efectivo de la

información. También permite monitorear los datos sensibles que hay en la empresa, se sabe qué tipo de información se está trabajando con el fin de evitar las fugas de información en los puntos finales como dispositivos extraíbles, en este proceso se definen las políticas de identificación de quién envía la información, donde se la envía, gestionando así, el cumplimiento de las políticas y normativas definidas por la empresa.

La protección de los datos es la parte esencial de la solución DPL, ya que define qué tipo de protección se debe de dar a los datos sensibles como notificaciones, bloqueos, cifrados, para que al momento de prevenir se llegue a cumplir cada una de las normativas que protege la información en medios externos.

3.6.1.1 Establecer flujo de trabajo y administración

Al establecer esta solución DLP, se vio la necesidad de realizar informes así paneles para tomar medidas en el caso de que haya una mala utilización de la información con cada uno de los usuarios; estos informes se crearon apoyándose en base a la fase de Gestión de Incidentes en la seguridad de la información de la ISO 27002.

Esta solución DPL cuenta con herramientas de reportes a tiempo real que detecta, registra y monitorea los datos que están utilizados de manera normal, así como los datos en riesgo. Cada uno de estos reportes o informes analiza los incidentes que se tengan con el fin de tener datos casi precisos para fines de auditorías.

4 IMPLEMENTACIÓN DE SOLUCIÓN PRA LA ADMINISTRACIÓN DE SEGURIDAD Y PREVENCIÓN DE PÉRDIDA DE DATOS (DLP)

4.1 Implementación Piloto

Para empezar con la implementación de la herramienta; verificar el estado y funcionamiento del servidor; es uno de los puntos fundamentales. Este consta con el software de Windows Server 2008, el cual tiene implementado las siguientes funciones.

- Active Director: Este servicio es el encargado de administrar el inicio de sesión de los usuarios y grupos de los mismos, que están conectados en la red; así como las políticas creadas y asignadas. El dominio con el que se trabajó es con wtarqui.com.ec

- Servicio de DNS o Servicio de Nombres de Dominio: Es el encargado de asignar los nombres a los equipos y servicios de red de los clientes de la empresa. La IP utilizada es de clase C y es la 192.168.58.140

- Servicio de DHCP o Protocolo de Configuración Dinámica: Es el encargado de asignar automáticamente a los usuarios un rango de IP´s para la conexión directa sin necesidad de estar haciéndolo de manera manual. Los rangos en el cual se basa es desde la IP inicial 192.168.58.141 hasta la IP final 192.168.58.250.

- Cada una de las máquinas pueden ser conectadas a través de la conexión a Escritorio Remoto, lo cual es factible ya que no se necesita tener los equipos físicos para la administración de los mismos.

Para la implementación de la herramienta se basa en las configuraciones del servidor, y tomando como usuarios de prueba a un total de 3, los cuales están en los grupos de Logística, Finanzas y Sistemas; se consideraron estas áreas

ya que son las más afectadas en la pérdida de información, esto se basa en el estudio de información realizada con los ejecutivos de la empresa.

Por medio de conexión remota, se procede a tener el acceso total del servidor en el cuál se inicia la instalación de la herramienta McAfee E-Policy Orchestrator, versión 4.68., ya que va monitorizando en tiempo real los programas de seguridad implementados, en este caso se el programa asignado es McAfee DLP Endpoint Protection 9.22.0.

Al instalar el sistema EPO, se procede a realizar la instalación del Servicio WFC (Windows Communication Foundation), el cual es el encargado de hacer la comunicación de la herramienta de administración con la del cliente.

Hay que tomar en cuenta que en cada una de las herramientas antes mencionadas, se escoge el dominio en el que se está trabajado, en este caso es wtarqui.com.ec y que usuario es el que va a administrar cada uno de los permisos, el cuál es Administrador.

La herramienta como se mencionó anteriormente, es un aplicativo web en la que se tiene que ingresar con permisos administrativos, en este hay que colocar las extensiones de la herramienta McAfee DLP Endpoint y las extensiones de los agentes. Esto es importante ya que se puede hacer la respectiva monitorización en tiempo real de cada uno de los usuarios, así como el generar las políticas requeridas por la compañía para la seguridad de la información.

En las siguientes figuras tenemos las vistas generales de la herramienta instalada en el servidor del usuario.

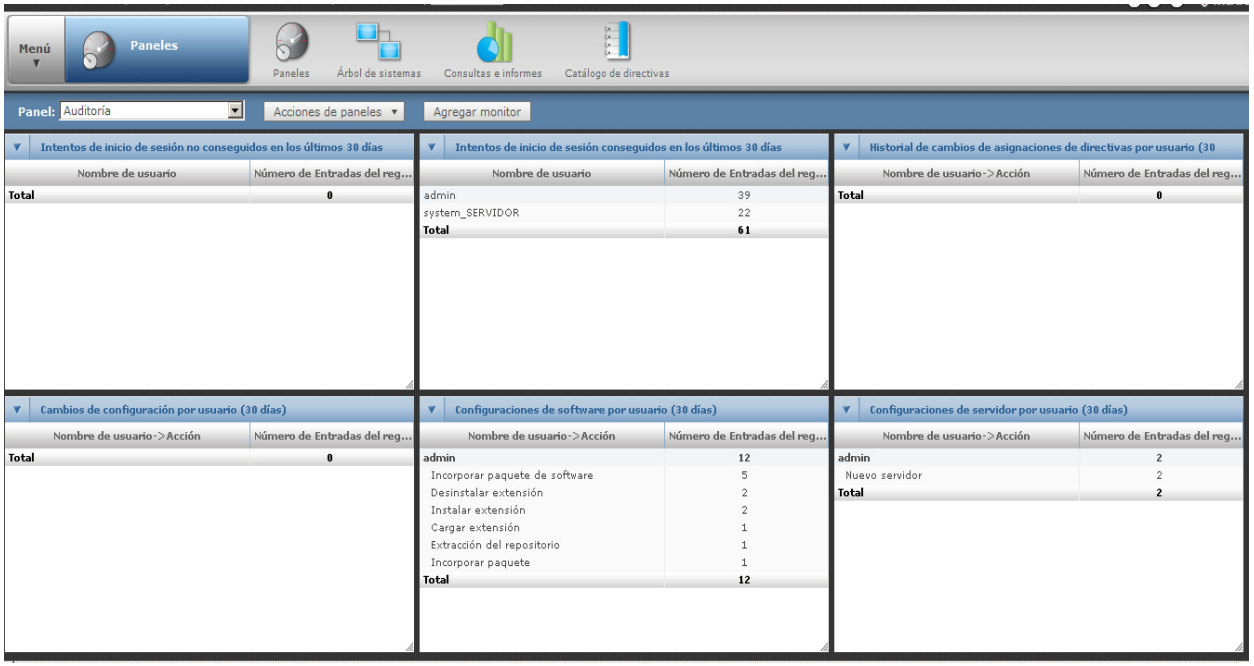


Figura 11. Esquema General de McAfee E-Policy Orchestrator

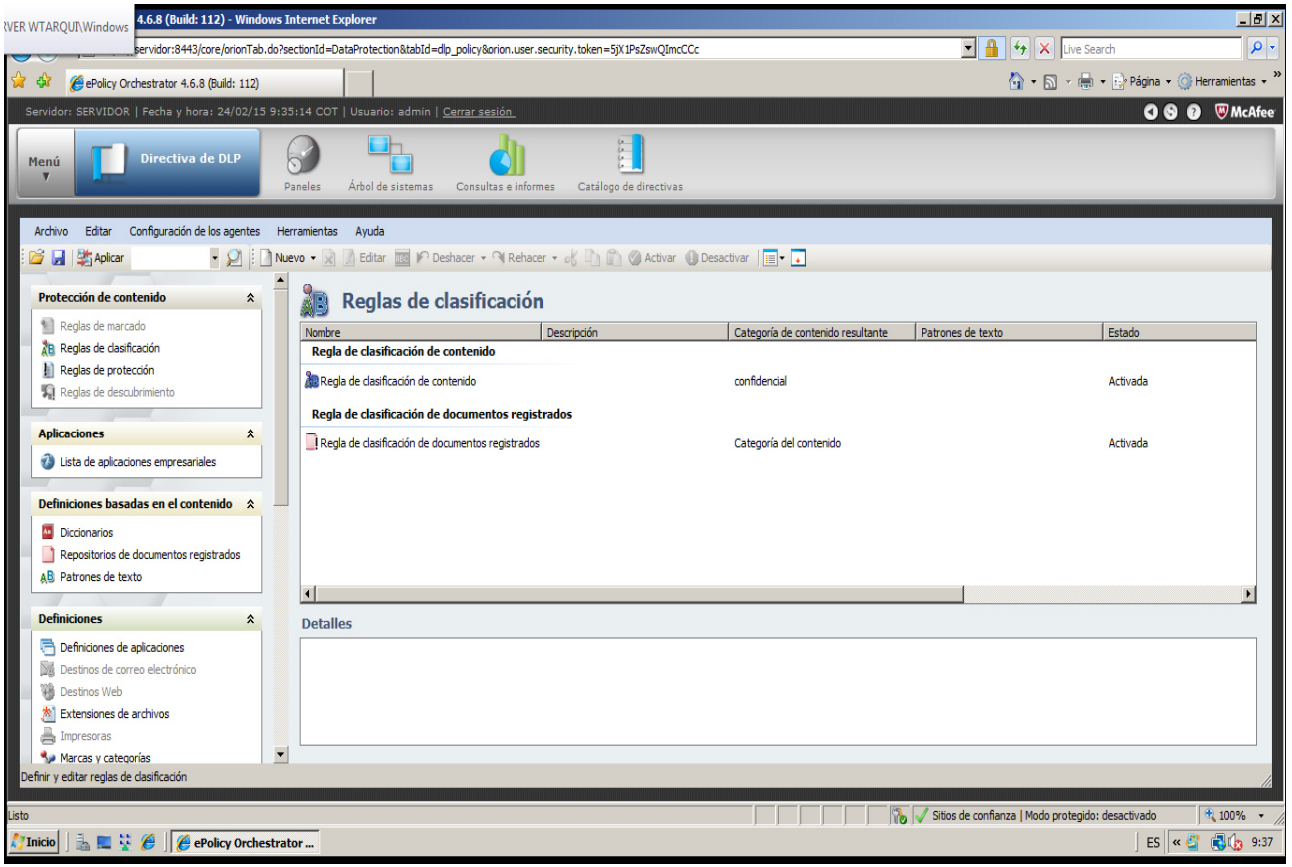


Figura 12. Esquema General de las Directivas DLP

Para que exista una sincronización con el active directory del servidor, se tiene que hacer una sincronización en los árboles de sistemas, ya que estos tienen toda la información de los usuarios y las máquinas que están trabajando, así mismo el control para la instalación del agente en cada uno de ellos. En los siguientes gráficos se puede ver el árbol del sistema y la activación del McAfee Agent en el cliente.

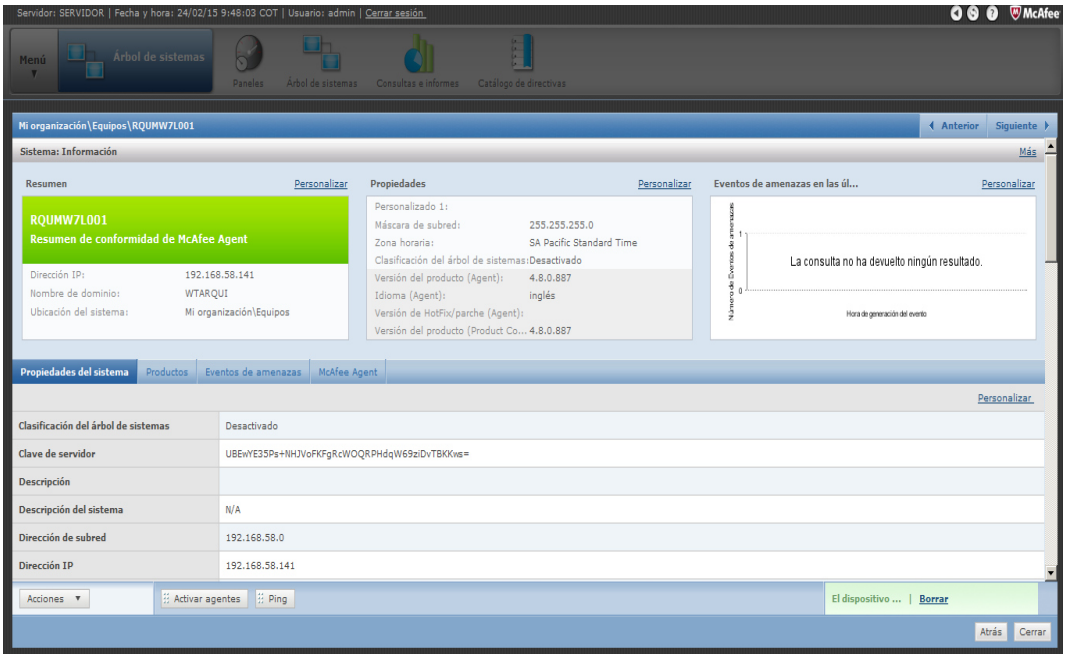


Figura 13. McAfee Agent para los clientes desde el Servidor

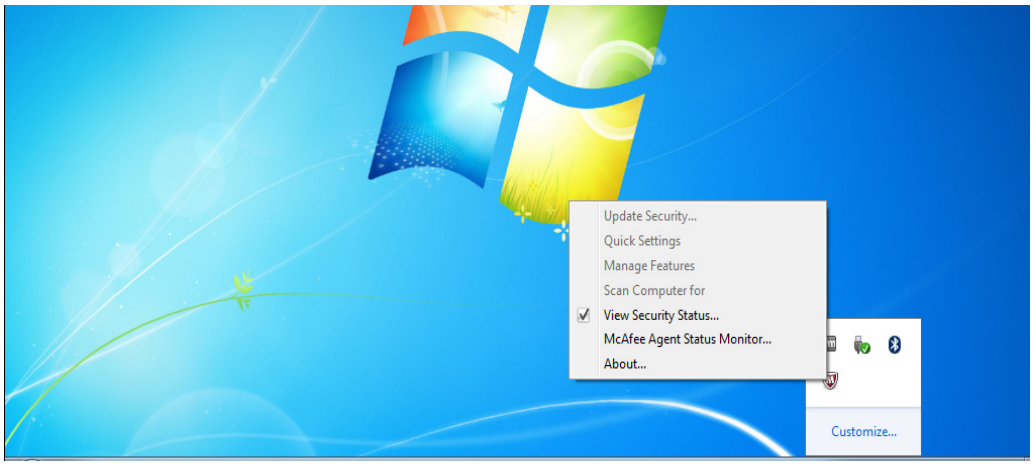


Figura 14. McAfee Agent para los clientes desde el equipo del usuario

Al tener instalada la herramienta tanto en el servidor con el cliente se procede, a realizar las reglas de clasificación, asignación de dispositivos para el control de la fuga de información.

A ver que se tiene una sincronización a tiempo real, desde la herramienta ubicada en el servidor y las máquinas de cada uno de los usuarios, la implementación resultó ser exitosa; sin embargo existen riesgos y una evaluación más profunda que se verá en los siguientes puntos del proyecto.

4.2 Riesgos y Amenazas de la implementación

Los riesgos que se obtuvieron se basaron en 2 matrices tomando en cuenta la probabilidad de riesgo e cada una de ellas, la primera antes de la implementación y la segunda después de la misma vista anteriormente.

En la siguiente tabla se define el impacto de la fuga de información, tomando en cuenta 5 niveles con sus respectivos rangos y probabilidades.

Tabla 14. Definición de impacto de fuga de información

Nivel	Rangos	Porcentaje de Fuga
1	Bajo	1%
2	Menor	2 al 10%
3	Intermedio	10 al 20%
4	Mayor	20 al 30%
5	Superior	Mayor al 30%

Además se tomó en cuenta el escenario de riesgos estudiado en base a las posibles vulnerabilidades que tiene el sistema.

En la siguiente tabla se muestra el escenario:

Tabla 15. Escenario de riesgos en base a posibles vulnerabilidades

ESCENARIO	PROBABILIDAD		IMPACTO GENERADO	RESULTADO GENERADO
Uso de Software Inseguro	NULA	1	1	1
Enlaces de Comunicación	NULA	1	1	1
Abuso de Privilegios en el manejo de servidor	POSIBLE	3	2	6
Pishing en Base de Datos	NULA	1	2	2
Daños en el control de acceso	NULA	1	2	2
Suplantación de Identidad para el manejo del servidor	CASI NULA	2	1	2
Problemas de confidencialidad de la información y falencia en el control del acceso a la misma	POSIBLE	3	3	9
Copias de seguridad en servidores y base de datos	NULA	1	3	3
Uso de software inseguro en dispositivos móviles	CASI NULA	2	2	4
Robo de información entre usuarios de la empresa	CASI SEGURO	4	5	20
Falsificación de documentos, virus para robar la información	CASI SEGURO	4	5	20
Robo de Información de las áreas en archivos compartidos, base de datos	POSIBLE	3	5	15
Robo de Información en Estaciones de trabajo	SEGURO	5	5	25
Robo de información en correo corporativo	SEGURO	5	5	25
Robo de Información por dispositivos externos de medios extraíble	SEGURO	5	5	25

Las probabilidades se definieron en base a un análisis con las personas del área de sistemas en las que, especificaron las probabilidades de cada una de ellas. Este análisis permitió hacer distintos escenarios para un mejor estudio de la clasificación de la información.

En las siguientes matrices define los riesgos que se dan antes de la implementación del sistema y después de la misma, tomando en cuenta los escenarios que se mencionó anteriormente.

Tabla 16. Matriz de riesgos antes de implementar la metodologia aplicando un sistema DLP

Probabilidad	Valor	Tabla de Impacto de Fuga de Información				
		1	2	3	4	5
Nula	1	• Uso de software Inseguro. • Enlaces de Comunicación.	• Phishing en Bases de Datos • Daños en control de accesos	• Copias de seguridad en servidores y base de datos		
Casi Nula	2		Suplantación de identidad para manejo del servidor	Uso de software inseguro en dispositivos móviles		
Posible	3	Abuso de privilegios en el manejo del servidor	Problemas de confidencialidad de la información y falencia en el control del acceso a la misma			Robo de Información de las áreas en archivos compartidos, base de datos
Casi Seguro	4			Robo de información entre usuarios de la empresa	Falsificación de documentos, virus para robar la información	
Seguro	5					Robo de Información en Estaciones de trabajo Robo de información en correo corporativo Robo de Información por dispositivos externos de medios extraíble

Tabla 17. Matriz de riesgos después de implementar la metodologia aplicando un sistema DLP

Probabilidad	Valor	Tabla de Impacto de Fuga de Información				
		1	2	3	4	5
Nula	1	• Uso de software Inseguro • Enlaces de Comunicación	• Phishing en Bases de Datos. • Daños en control de accesos. • Robo de Información por dispositivos extraíbles, archivos compartidos. • Robo de Información por correo corporativo.	• Copias de seguridad en servidores y base de datos. • Falsificación de documentos.		
Casi Nula	2	Abuso de Privilegios	Suplantación de identidad para manejo del servidor. Falencias en control de accesos. Suplantación de identidad	Uso de software inseguro en dispositivos móviles		
Posible	3	Abuso de privilegios en el manejo del servidor	Problemas de confidencialidad de la información			Robo de Información de las áreas en archivos compartidos, base de datos
Casi Seguro	4			Robo de Información en Estaciones de trabajo.		
Seguro	5					

Tabla 18. Matriz de Probabilidad vs Valor sin aplicar la herramienta

ANTES DE LA IMPLEMENTACIÓN DLP	Probabilidad	# de Riesgos en base al impacto de fuga				
		1	**2**	**3**	**4**	**5**
	Nula	2	2	1	0	0
	Casi Nula	0	1	1	0	0
	Posible	1	2	0	0	1
	Casi Seguro	0	0	1	2	0
	Seguro	0	0	0	0	3
	Total de Riesgos	3	5	3	2	4
	% de Riesgos	18%	29%	18%	12%	24%

Tabla 19. Matriz de Probabilidad vs Valor Aplicando DLP

DESPUÉS DE LA IMPLEMENTACIÓN DLP	Probabilidad	# de Riesgos en base al impacto de fuga				
		1	**2**	**3**	**4**	**5**
	Nula	2	4	2	0	0
	Casi Nula	1	3	1	0	0
	Posible	1	1	0	0	1
	Casi Seguro	0	0	1	0	0
	Seguro	0	0	0	0	0
	Total de Riesgos	4	8	4	0	1
	% de Riesgos	24%	47%	24%	0%	6%

Las matrices se basaron en la probabilidad que el escenario se de en base al riesgo que se genere en su fuga. Se contabilizó cada uno de ellos en las tablas de riesgo antes mencionadas.

Al ver las matrices e identificar cada uno de los riesgos antes de la implementación y después de la misma, se definieron los siguientes puntos:

- Hay una disminución en los riesgos en los rangos superior y medio alto del impacto de la fuga de información llegando a un porcentaje nulo y casi nulo, por lo que la implementación fue efectiva al dar políticas y restringir dispositivos externos, en donde fácilmente pueden extraer la información sensible de la misma.

- Cada uno de los riesgos que hubo un aumento de porcentaje en sus rangos, lo cual define que la perdida de información va a ser casi nula al haber implementado la herramienta.

Al clasificar la información proporcionada por cada área de la empresa, hubo discrepancias en la sensibilidad de la información, por lo que se optó por tomar los datos de los años 2013 y 2014, para que al momento de definir las políticas se tenga una mejor distribución de los datos.

4.3 Resultado Final

Después de haber desarrollado el modelo de seguridad para la implementación piloto de la herramienta DLP se realizó una evaluación en la que se tomó distintos parámetros, para definir el resultado final que proporciono haber implementado la herramienta del proveedor McAfee.

En la siguiente tabla se identifica una matriz comparativa que la herramienta proporcionó al cliente; en la cual se ve la efectividad de la misma.

Tabla 20. Matriz Comparativa de la Herramienta McAfee DLP

MATRIZ COMPARATIVA DE LA HERRAMIENTA MCAFEE DLP ENDPOINT PROTECTION	CUMPLE	NO CUMPLE
Controla el almacenamiento de archivos sensibles en medios extraíbles (CD, USB, discos duros, etc).	X	
Supervisar que un documento confidencial no puede ser enviado a través de correo electrónico.	X	
Supervisar que una porción tanto del archivo como de una base de datos determinado no pueda ser impreso.		X
Registra y controla o el cifrado de información sensible.	X	
Integración de herramienta con la infraestructura de la compañía o empresa.	X	
Instalación Remota.	X	
Integración con el Directorio Activo.	X	
Cuenta con paneles de identificación y monitoreo de en el uso de la información.	X	
Se pueden exportar los incidentes generados a otro tipo de archivos para tener un reporte más claro.	X	
Genera notificaciones de bloqueo y monitoreo al usuario	X	
Los usuarios cumplen con la compactibilidad del sistema y sus versiones Windows (XP, Vista y 7, 32 y 64 bits).	X	
Definir los recursos que son utilizados en los equipos Endpoint.	X	
El cliente cuenta con seguridad para que el administrador tenga acceso al control de sus equipos.	X	
Se encuentra alineado con las normas y estatutos cumpliendo con los requisitos de la compañía.	X	

En las siguientes figuras se ve cada uno de los puntos antes mencionados, en el cual se evaluó la herramienta en la empresa.

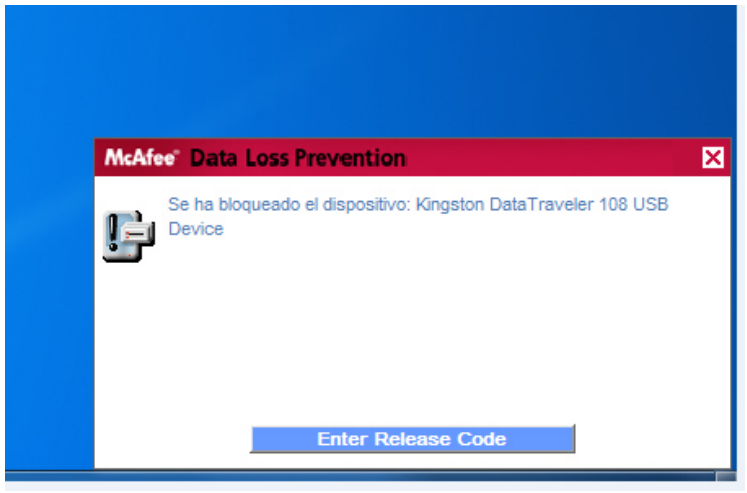


Figura 15. Control del Almacenamiento de Información sensible en dispositivo extraíble

En la figura 15 se identifica que el dispositivo USB de la marca Kingston no puede ser utilizado en los equipos de los usuarios ya que por políticas este producto no es utilizado en la empresa, para el manejo de la información.

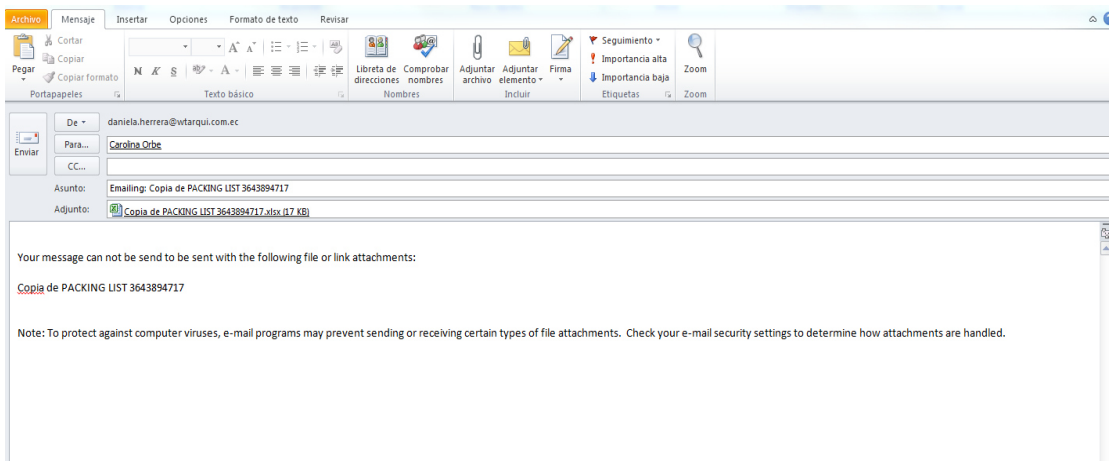


Figura 16. Supervisión de envió de información sensible por correo electrónico

En la figura 16 el usuario no puede enviar un correo electrónico con un documento adjunto, ya que el mismo es de carácter confidencial para la empresa ya que son lista de productos en base a la segmentación de los clientes que se manejan.

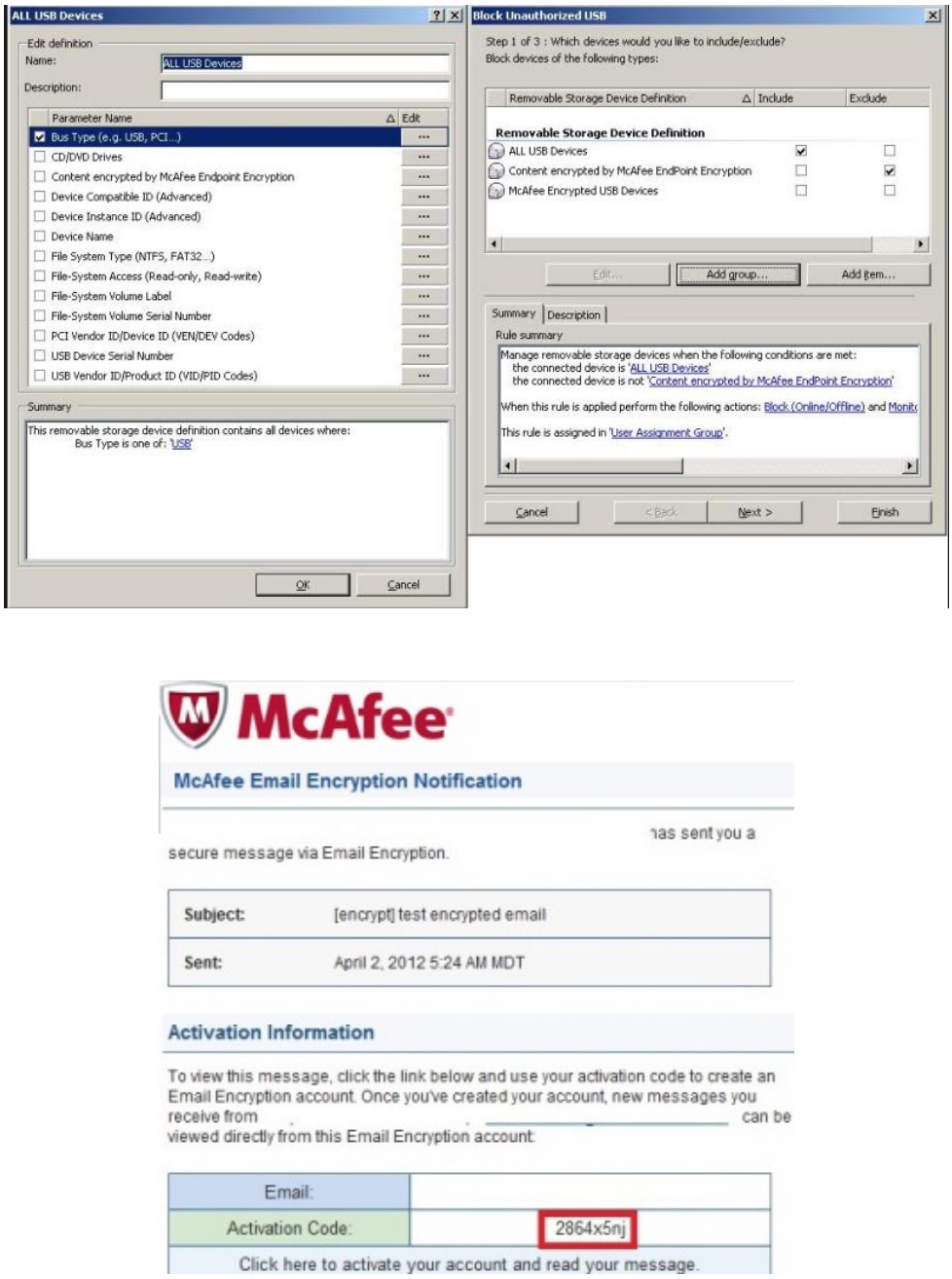


Figura 17. Registra y controla o el cifrado de información sensible

En la figura 17 se observa que al registrar y controlar la información sensible, está no puede ser vista ni modificada si es que el agente administrador no envía un código de activación, el cual tiene que ser colocado al momento de que la información haya llegado al destino.

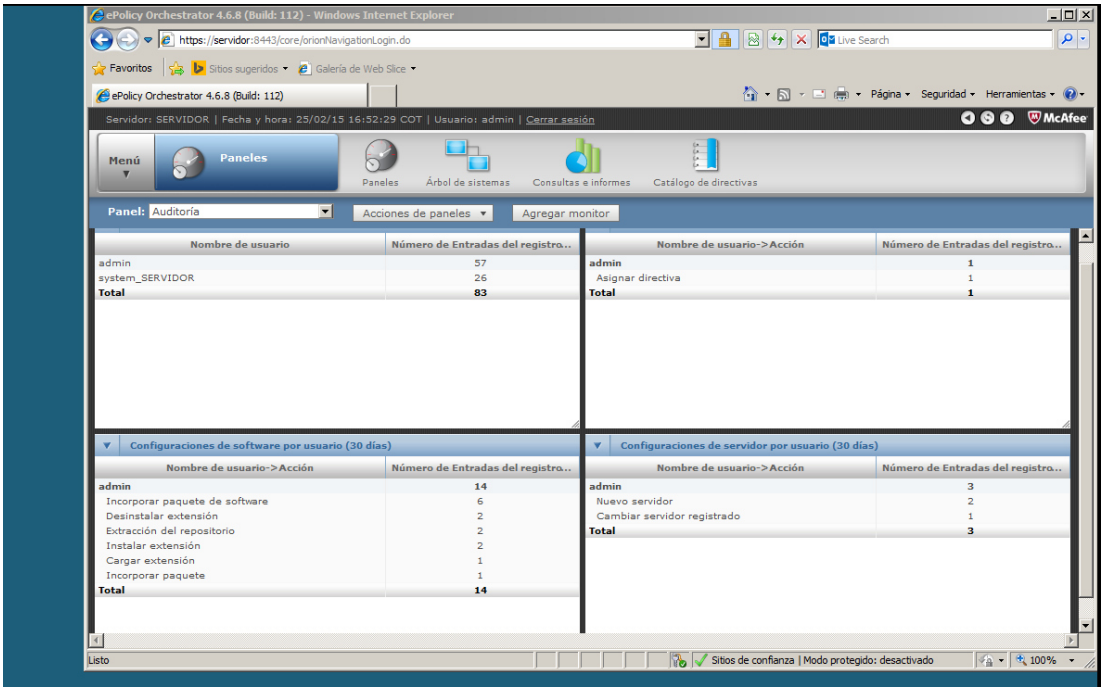


Figura 18. Integración de herramienta con la infraestructura de la compañía o empresa

La figura 18 muestra como la herramienta está integrada con el servidor de la compañía en la cual muestra todos los procesos que se han dado con respecto a las máquinas de los usuarios, con esto se lleva un mejor control de tiempo real de la utilización de la herramienta.

A

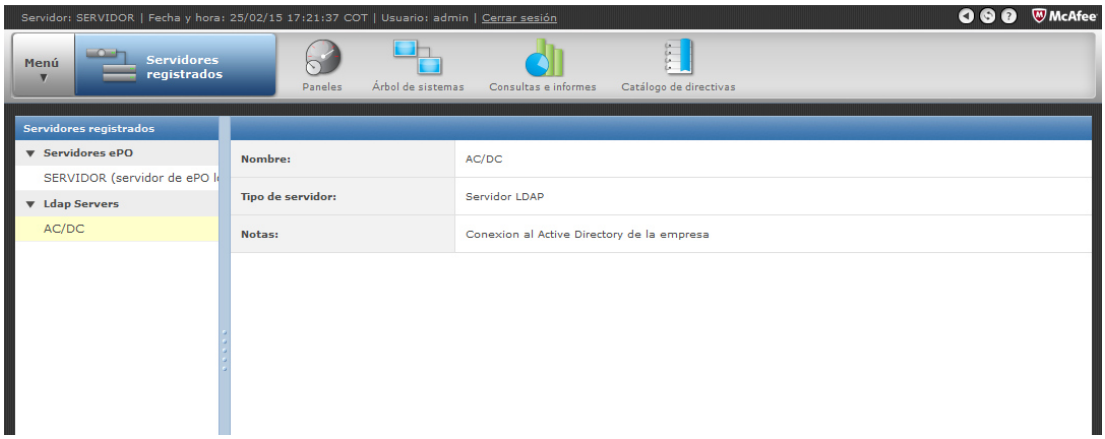


Figura 19. Integración con el Directorio Activo de la Empresa

La figura 19 muestra que la herramienta funciona en perfecto estado con el Active Directory de la compañía ya que con esta se hace la conexión para el uso de la misma en las máquinas de los usuarios.

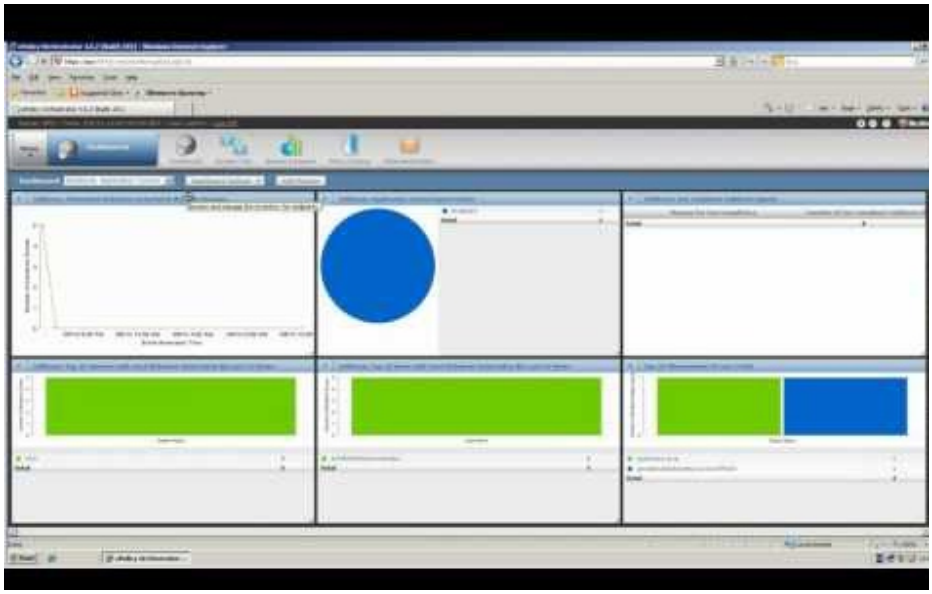


Figura 20. Paneles de identificación y monitoreo en el uso de la información

En la figura 20 se observa cómo se está utilizando la información de la empresa. Los segmentos de color verde es la información que ha sido

correctamente utilizada, mientras que los segmentos azules, es la información que se debe verificar en que ha sido utilizada para determinar el inconveniente que haya causado un error.

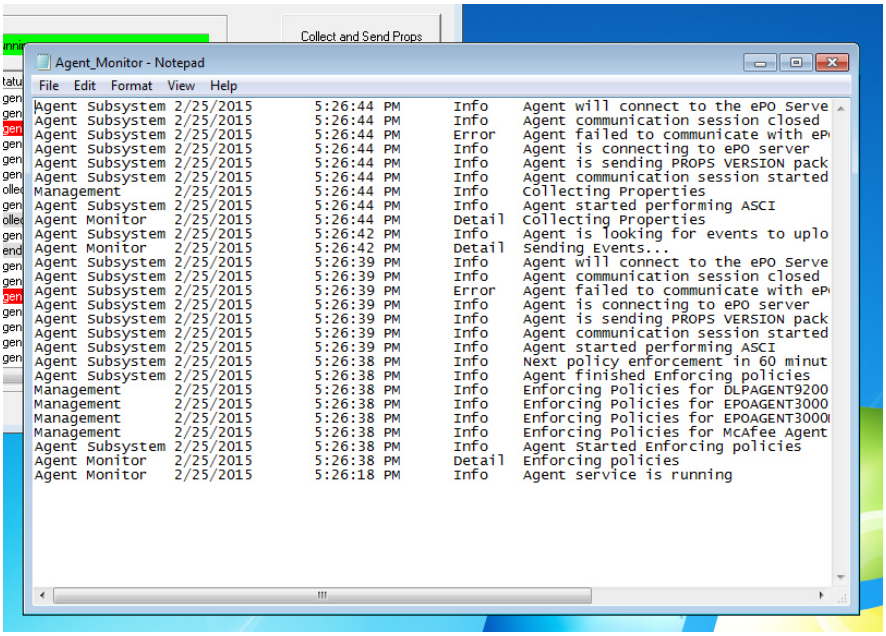


Figura 21. Exportar eventos generados a otro tipo de archivos

Para los agentes que manejan la consola, es bueno tener una información detallada de lo que la herramienta hado supervisando en cada una de las máquinas de la compañía, así ayudará a dar un detalle más proporcionado a las cabezas de la empresa para la toma de decisiones.

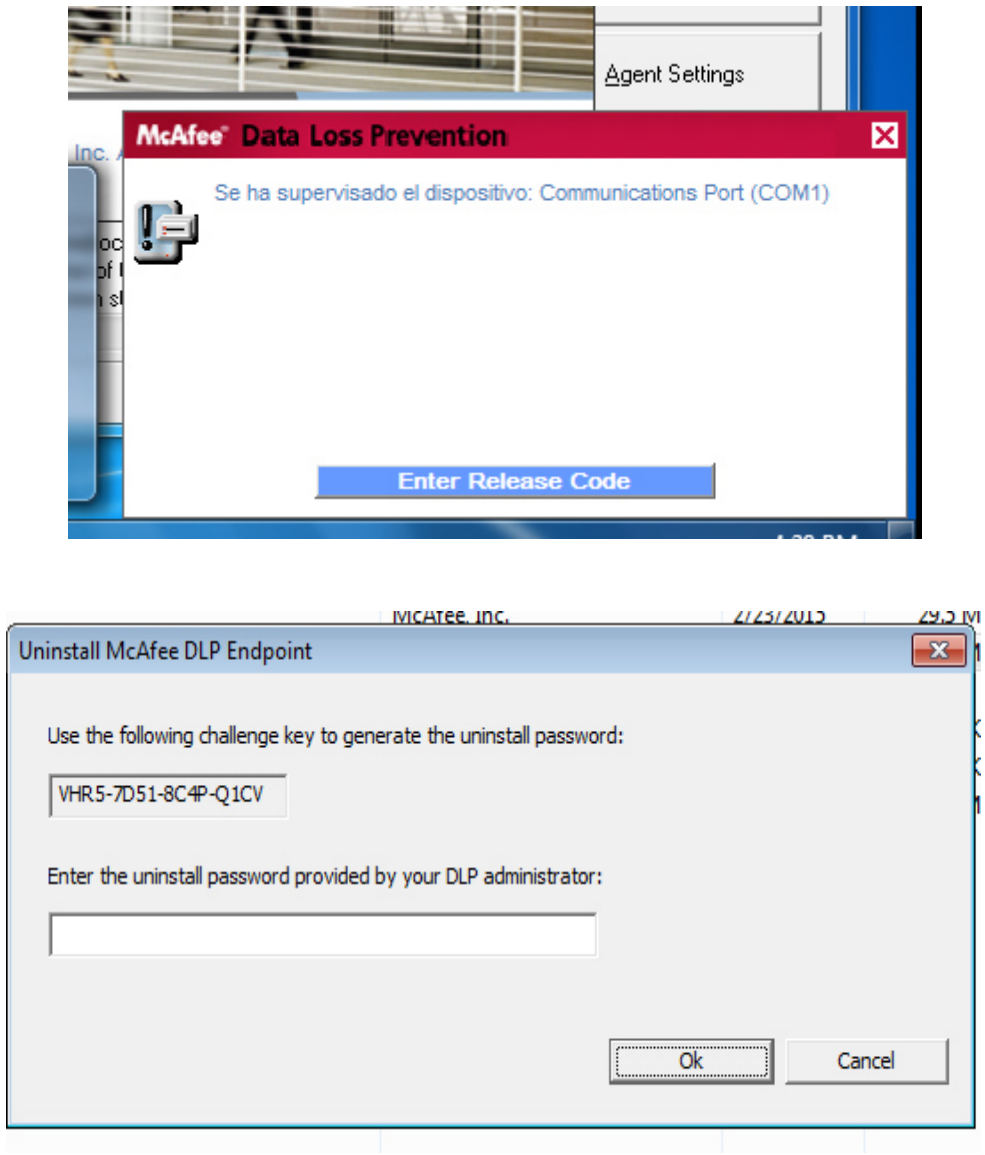


Figura 22. Genera notificaciones de bloqueo y monitoreo al usuario

Cuando un usuario quiera ingresar algún tipo de dispositivo que no está autorizado para su manejo, este genera una notificación al usuario, el cual pide que este pida autorización a los administradores para poder ser utilizado, en el caso de que sea netamente corporativo.

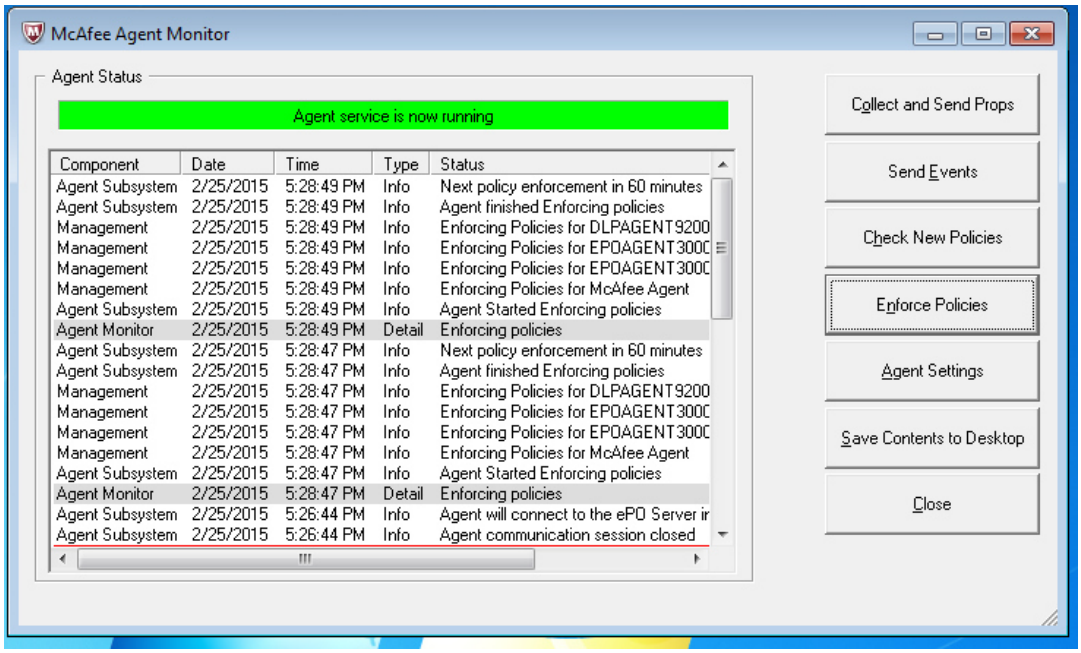


Figura 23. El cliente cuenta con seguridad para que el administrador tenga acceso al control de sus equipos

Cada una de las máquinas son gestionadas por un Agente DLP, el cuál puede ayudar a generar, actualizar, enviar eventos de los usuarios, para monitorizar de manera más efectiva el uso de la información.

En la matriz identificamos que la implementación de la herramienta de prevención de perdida de datos ha sido efectiva en un 94%, por lo que se cumplió con la mayoría de los puntos requeridos por la empresa.

4.4 Evaluación del sistema DPL

El sistema permitió gestionar de manera automatizada y centrada las políticas y normas colocadas por la empresa; así como seguridad de información en los puntos finales.

Se hizo la prevención de acceso no autorizado y robo de la información; así que en el momento que ocurra un evento de esta magnitud, los datos que puedan ser hurtados sean inútiles y difícil de descifrar.

Con esta herramienta da la protección contra robo y divulgación accidental de datos confidenciales, lo cual fue el principal objetivo de este proyecto. Es una protección de datos integrada y completa de puntos terminales, ya que controla la manera en que transfiere datos en la red y las que copia en dispositivos de almacenamiento portable.

Al tener un control centralizado desde el servidor, se puede manejar cada una de la definición de las políticas por cada grupo que este en el Active Directory de la empresa.

Con el sistema de McAfee que se utilizó en la implementación del modelo DLP se comprobó cada uno de los procesos que hay en el sistema de gestión de seguridad ISO 27000, los cuales fueron estudiados en el capítulo 3 del presente trabajo.

En la fase de planificar se realizó un análisis de tallado en los que se establecen los límites del sistema así como las políticas de seguridad en función de los recursos tecnológicos, características del negocio y la estructura de la empresa. Se identificó los riesgos, amenazas y vulnerabilidades que tiene la información en la empresa, en el cuál se determinó el impacto que estos generan en el negocio.

En la fase de implementación o hacer se definió la política de seguridad de la información en base a la gestión de documentos, seguridad física, control de acceso, gestión de incidentes ocurridos. Se realizó la evaluación de cada riesgo encontrado en la empresa implementando los marcadores y controladores seleccionados para cada información frágil.

En la fase de verificación se midió el desempeño del proceso de monitorización de la información de la empresa en base a las políticas establecidas anteriormente; por lo que al ver que la herramienta DLP podía realizar algunos puntos más como por ejemplo el marcado exclusivo de los documentos,

realizando algunos cambios en la misma y se reportó a los líderes de la empresa los beneficios que se obtuvieron para su revisión.

En la fase de actuar se aportó con una buena gestión preventiva correctiva al supervisar cada evento que realiza el usuario, en cada documento corporativo, en un menor tiempo y de manera eficaz.

5 ANÁLISIS COSTO-BENEFICIO DE LA SOLUCIÓN PREVENCIÓN DE PÉRDIDA DE DATOS (DLP)

La implementación del sistema DLP en la empresa generó algunos puntos de vista, los cuáles sirvieron para realizar el siguiente análisis. Estos puntos son:

- Genero resultados positivos en el tiempo de la gestión de contingencia.
- Generó resultados positivos sobre el costo del proceso de gestión de los riesgos generados de la herramienta.
- Generó resultados positivo en el rendimiento del proceso de gestión de los riesgos generados de la herramienta.

Al saber las opciones que se tuvo para el tratamiento de los riesgos, se vio que la mitigación de los mismos se debe al cambio de los procesos de la empresa, así como el almacenamiento de su información.

5.1 Costo

Se hizo un análisis de los costos que se han venido dando en la empresa por motivos de fuga de información obteniendo los siguientes resultados:

Tabla 21. Costos por fuga de información

Motivo para la fuga de información	% de Perdida de Información	Costo por cada Item	Costo Total
ROBO DE EQUIPOS	52%	$ 520,00	$ 1.000,00
ROBO DE DISPOSITIVOS EXTRAIBLES	22%	$ 220,00	
PERSONAL QUE SALIÓ DE LA EMPRESA	26%	$ 260,00	

Al tener la herramienta de prevención de pérdida de datos unificada da un costo favorable para la empresa que se hizo la implementación piloto de la

misma, debido a que McAfee brinda la oportunidad de manejar paquetes que brindaron una seguridad en tiempo real contra los peligros que ingresaban así como los que salían de la empresa. La consola manejada así como la herramienta del cliente reduce en un gran porcentaje el CAPEX (Gasto de Capital) así como el OPEX (Gasto Operativo), ya que la unificación de todos los sistemas en su infraestructura, proporcionó gran visibilidad de lo que sucede con la seguridad de la información.

Los costos que se desarrollaron al implementar la herramienta DLP se segmenta en el costo de desarrollo del software, costo de equipo para el desarrollo, y costos adicionales como entrenamiento a usuarios y administradores del sistema.

Para que este proyecto sea aceptado se tomó en cuenta algunos puntos tales como el valor neto actual (VAN) y la tasa interna de retorno (TIR). La relación costo/beneficio define la ganancia dada por la inversión emitida en el proyecto. Esta relación se mide de acuerdo a la siguiente ecuación:

$$\frac{B}{C} = \frac{\sum_1^N VAN}{INVERSION\ INICIAL} \qquad \text{(Ecuación 2)}$$

Dónde:

- B/C: Relación Beneficio-Costo
- VAN: Valor actual neto
- N: Número de años para realizar el proyecto

Considerando la información emitida por la empresa se llegó a establecer algunos parámetros de medición para realizar el análisis respectivo.

El costo de los equipos es un punto muy importante para este análisis; se tomó en cuenta las características del equipo en el que se realizó la implementación

piloto de la herramienta DLP. En la siguiente tabla se da una proforma del costo del equipo.

Tabla 22. Proforma costo de equipo principal

Item	Cant.	Descripción	Valor unitario	Subtotal
1	1	Computadora HP 2570P	$ 650,00	$ 650,00
2	1	1 Monitor 23 pulgadas HP LA2306X	$ 230,00	$ 230,00
			Suma Subtotal	$ 880,00
			IVA 12%	$ 105,60
			TOTAL	$ 985,60

También se tomó el costo y realización de toda la implementación de la herramienta. En las siguientes tablas se muestra el costo de elaboración de la implementación así como el costo general del mismo.

Tabla 23. Costo de elaboración para la implementación

Item	Cantidad en horas	Descripción	Valor unitario	Subtotal
1	100	Levantamiento de información	$ 3,00	$ 300,00
2	110	Clasificación de la información	$ 3,00	$ 330,00
3	60	Diseño y programación de equipo	$ 3,00	$ 180,00
4	25	Elaboración de planes de mantenimiento	$ 3,00	$ 75,00
			TOTAL	$ 885,00

Tabla 24. Costo de licencias software

Item	Cantidad	Descripción	Valor unitario	Subtotal
1	1	Licencia McAfee ePO	$ 49,30	$ 49,30
2	1	Licencia McAfee DLP	$ 92,20	$ 92,20
3	1	Licencia Windows Server Datacenter 2008	$ 362,00	$ 362,00
4	1	Capacitación herramienta McAfee	$ 65,00	$ 65,00
			TOTAL	$ 568,50

Al definir cada uno de los costos definidos para la implementación se realizó un cálculo de rentabilidad, en la que se hizo la suma total de todos los costos tanto de equipos, como los de implementación dando un resultado muy factible para la empresa. En la siguiente tabla se muestra el costo final total.

Tabla 25. Costo final total

Item	Rubro	Costo
1	COSTO DE EQUIPO	$ 985,60
2	COSTO DE ELABORACIÓN DE PROYECTO	$ 885,00
3	COSTO GENERAL DE IMPLEMENTACIÓN	$ 568,50
	COSTO FINAL	$ 2.439,10

Para la corroboración de los datos se hizo un análisis de utilidad neta tomando en cuenta la diferencia que se dio entre el ingreso anual asociándose directamente con los gastos proporcionados con lo cual el flujo de costos van a estar proyectados a 1 año y el primer trimestre del año 2. Con este análisis se ve que la inversión que se realizó no representa un costo excesivo, por lo que puede ser cubierto con facilidad en un corto tiempo debido a que en este periodo de tiempo se ve un ingreso positivo en base a la inversión colocada inicialmente.

En el siguiente cuadro está el cálculo de la utilidad neta así como el valor neto actual, la tasa interna de retorno y la relación beneficio-costo. La inversión que se dio fue el costo generado por la fuga de información de la empresa, que es del $ 1000.

Tabla 26. Análisis costo beneficio

		1 AÑOS				2 AÑO
MODIFICADORES	**0**	**1 TRIMESTRE**	**2 TRIMESTRE**	**3 TRIMESTRE**	**4 TRIMESTRE**	**1 TRIMESTRE**
AHORRO EN PERDIDA DE INFORMACIÓN		$ 1.000,00	$ 1.000,00	$ 1.000,00	$ 1.000,00	$ 1.000,00
ACTUALIZACIÓN DE LICENCIAS MCAFEE						$ 92,10
MANTENIMIENTO DE SERVIDOR		$ 35,00	$ 35,00	$ 35,00	$ 35,00	$ 25,00
DEPRECIACIÓN DE EQUIPOS					$ 328,53	
UTILIDAD ANTES DEL IMPUESTO		$ 965,00	$ 965,00	$ 965,00	$ 636,47	$ 882,90
UTILIDAD SRI A EMPRESAS (28%)		$ 270,20	$ 270,20	$ 270,20	$ 178,21	$ 247,21
UTILIDAD NETA		$ 694,80	$ 694,80	$ 694,80	$ 458,26	$ 635,69
FLUJO NETO	$ (2.439,10)	$ 694,80	$ 694,80	$ 694,80	$ 786,79	$ 635,69
TIR	12%					
VAN	$ 154,32					
BENEFICIO/COSTO	0,063271					

En base a lo calculado en el cuadro anterior, se puede demostrar que los beneficios son superiores a los que se invirtió. El proyecto es viable y rentable porque genera aportes económicos y sociales a la empresa, por lo cual las cabezas de la empresa ven que se pueden realizar algunos cambios positivos en la organización. El tener una relación beneficio/ costo positiva del 0.063271, se ve un retorno por cada dólar invertido; lo que a la empresa les resultó muy bueno.

5.2 Beneficio

El beneficio adquirido por la compañía se ve en las utilidades netas de la misma por un periodo de un año puesto que ese es el tiempo que definió la empresa para medir el beneficio adquirido al implementar el sistema. Se puede observar una reducción en el valor que ha ido generando la fuga de la información en los años 2013 y 2014.

Se puede observar el beneficio en el valor de la inversión del proyecto, ya que, esta implementación libera un porcentaje de capital positivo para que la empresa pueda utilizarlo en otros procesos que generen valor, los cuales como especificó la compañía son las capacitaciones a todos los usuarios y a los administradores del sistema que trabajan en la empresa, con el fin de ayudar a mitigar la fuga de información.

Debido a que la empresa no contaba con procesos, ni con la documentación acerca del correcto uso de la información; cada uno de los datos sensibles estaban dispersos en cualquier equipo tecnológico de uso público, por lo que todas las personas podían tener acceso a la información financiera, comercial y estratégica de la empresa. Con el desarrollo de la metodología de prevención de pérdida de datos y la implementación de la misma, se creó y se dio a conocer con más profundidad y exactitud cada uno de los procesos que se van a utilizar en la compañía en relación al manejo de la información sensible y confidencial por parte de los usuarios.

Al haber realizado una metodología que tuvo la finalidad de prevenir la perdida de datos y en la que los principales factores que se manipularon son de carácter lógico y tecnológico, como el análisis de la información y los equipos informáticos de la empresa; se pudo definir cada uno de los puntos débiles en el manejo de la información del negocio y la causa principal que los provocaba, por lo que al realizar la implementación de la herramienta que administra todo los procesos que realizan los usuarios en tiempo real, se pudo optimizar de manera eficaz la administración de la fuga de información y su prevención en una sola consola que es ejecutada en el servidor principal de la empresa.

La empresa, al ver que el sistema que proporciona McAfee es muy dinámico y fácil de utilizar, ayuda a instruir a los administradores de la herramienta con el objetivo de monitorear y evitar que intrusos accedan a la información de la empresa. Si se da una buena administración del sistema, el robo y la fuga de información dejarían de existir, generando así un ahorro en tiempo y económico para la empresa.

Facilita en un 100% la protección de los datos con el cumplimientos de las normativas, que al ser colocadas en la herramienta de manera directa, está se despliega en cada uno de los usuarios de manera automatizada; sin la necesidad de que se esté trabajando en cada máquina.

Detecta de manera precisa cada uno de los usos de la información y más aún si es sensible que están almacenados en los equipos de los usuarios así como el servidor; por lo que al supervisar continuamente los datos ayuda que la fuga se mitigue en un gran porcentaje.

Al minimizar los gastos de administración en la perdida de información, así como en una amplia infraestructura, la empresa ya no está en la necesidad de cubrir esos gastos, sino en capacitaciones y conciencia a las personas que trabajan en la compañía.

La capacitación que se le dio a toda la empresa fue un punto favorable para desarrollar un ambiente de trabajo más productivo, evitando así que haya dubitaciones en el manejo de la información.

6 CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

Al realizar una investigación de las posibles causas que pueden generar la pérdida de información en las empresas Pymes del Ecuador, definiendo 2 elementos principales para este problema: el tecnológico y el humano. Con el desarrollo del modelo de prevención de pérdida de datos se logró mitigar favorablemente en el aspecto tecnológico tener una herramienta que gestione todo el seguimiento de la información clasificada en tiempo real y en el aspecto humano tener el suficiente conocimiento de lo que implica el perder la información.

En el mercado actual, las empresas de soluciones tecnológicas han puesto en su plataforma seguridad de la información; por lo que uno de sus objetivos principales es el de ser el mejor. En este trabajo no solo se tomó en cuenta quien es el líder en el mercado, sino que se estudiaron otros factores como las fortalezas y calidad que tiene la herramienta pero a su vez las debilidades que estas pueden generar. Gracias al cuadrante de Gartner se pudo definir que la herramienta proporcionada por la empresa McAfee es la más óptima para la implementación piloto de este proyecto; ya que es una herramienta enfocada a medianas y grandes empresas, lo que ayuda a que el cliente pueda tenerla de manera sencilla.

Evitar la pérdida de información y cumplir con las leyes y normas establecidas internacionalmente así como nivel nacional, ya es un tema que está siendo tratado en el Ecuador; por lo que al desarrollar el modelo de pérdida de información propuesta tomando en cuenta algunos indicadores y elementos ayudó a que la empresa seleccionada sepa manejar la información sensible de clientes, proveedores, usuarios de manera correcta y así poder evitar sanciones legales. La información de la empresa fue debidamente clasificada para poder general políticas de información en la herramienta a instalar.

Con el desarrollo del modelo de prevención de datos se procedió con la implementación piloto del mismo, el cual inicialmente generó conflictos en el momento de la instalación de las herramientas tanto del cliente como del servidor, debido a que los paquetes de Microsoft Visual C++ no estaban debidamente colocados en las máquinas de la empresa. También no se tomó en cuenta la nueva actualización de la herramienta por lo que el estado de los agentes que manejan la herramienta no podía ser visible, generando conflictos a momento de tener reportes de actividades que solicitaban los gerentes de la empresa. La herramienta McAfee Endpoint Protection podía ser visualizada en el explorador Internet Explorer 8, que estaba en el servidor, por lo que se procedió a instalar el Internet Explorer 9. Las políticas de seguridad de información que fueron generadas en base a las leyes y normas las cuales permitieron clasificar toda la información fueron aplicadas de manera exitosa en la herramienta ya que la interfaz en la cual se desenvuelve McAfee es muy simple y amigable al usuario, por lo que al generarlas no se tuvo que hacer ningún tipo de codificación para que puedan ser ejecutadas correctamente. Además de que la información corporativa está segura; también está respaldada la información personal de cada usuario, por lo cual los niveles de seguridad llegan hasta el cliente interno.

Tras el análisis costo-beneficio realizado, al presentar esta solución al cliente y mostrar que el beneficio económico de prevenir la pérdida de información en el lapso de un año y tres meses es positiva ya que en la disminución de los pagos generados por la fuga de información gracias a la implementación del sistema de prevención de pérdida de datos, la empresa tiene la ventaja de hacer inversiones en lo que está actualmente requiriendo sin la necesidad de que haya un problema de costo al momento de aumentar o disminuir los usuarios en la empresa. Con esto la empresa puede reenfocar los recursos económicos en otros procesos que ayudaría a tener una mayor rentabilidad en la empresa, y así generar una mayor utilidad.

Una solución de prevención de perdida de datos cubre necesidades de seguridad importantes en las empresas ya que la información es clave para ellas; por lo que las soluciones actuales no son triviales de desplegar y se requiere de personas especializadas para la integración de las mismas, por lo que el dar la instrucción necesaria es fundamental para que la monitorización de la información sea lo más transparente posible. Es también importante indicar que para que el control sea exitoso se debe socializar la política de seguridad con cada usuario de la empresa; es decir cada uno de los empleados de la compañía tiene la obligación de saber que la seguridad de la información ya es un punto primordial de su lugar de trabajo.

6.2 Recomendaciones

Cada uno de los procesos realizados en este proyecto, tienen que ser tomados muy en cuenta debido a que en la actualidad, todas las empresas toman como uno de sus puntos más importantes el manejo de la información, así como la distribución y depuración de esta; por lo que han generado y establecido políticas, estándares normas y leyes que tienen que ser respetadas por cada uno de los empleados y clientes externos.

Cuando se tenga que realizar un plan de implementación del sistema de prevención de perdida de datos, se deben tener muy claros los riesgos, amenazas y posibles vulnerabilidades en todos los niveles de la empresa, así como elementos de y equipos de trabajo; además se tiene que tener en cuenta el beneficio que se da al tener implementado el sistema, tanto en niveles financieros como informáticos.

Para que se tenga una buena gestión de riesgos así como la clasificación de la información, se debe trabajar con los líderes de la empresa, ya que ellos determinarán las decisiones y situaciones de mejora que se den al momento de que haya una fuga de la información. Es decir que una amenaza o una

vulnerabilidad será una oportunidad de cambio que es positivo para la empresa.

Se recomienda dejar a un lado el punto de vista totalmente técnico en la protección de la información, sino que se debe trabajar en conjunto con cada una de las unidades del negocio con la finalidad de documentar los procesos críticos que conlleva a la fuga de información y así trabajar sobre cada uno de ellos.

Desarrollar técnicas para detallar los riesgos que hay en la seguridad de la información de cada empresa, es un punto de recomendación que se da cada una de ellas, debido a que si se integra cálculos que van directamente relacionados con el negocio, cada proceso de asesoramiento de riesgos, será mucho más fácil de analizar y gestionar.

Planificar técnicas de recopilación de datos es uno de los puntos que se puede recomendar ya que el desarrollar una mejora en la arquitectura de este proceso, en base a la generación de registros con los datos más relevantes, ayudará a tener una mejor capacidad de almacenamiento de datos y una mejor visión de los mismos para una posterior toma de decisiones.

Es recomendable que las personas que vayan a administrar el sistema de gestión de seguridad de información sean introducidas dentro de la empresa para determinar un proceso estándar operativo, generando un flujo en base a los lineamientos corporativos, así como responsables y las actividades a realizarse. Si existe este proceso facilitará la inclusión de nuevos sistemas de gestión sin tener la necesidad de crear nuevas actividades.

Es importante definir que el éxito de la implementación va de la mano el compromiso que tiene la empresa, debido a que si hay una colaboración en definir los puntos de fuga, clasificar la información, tiempo para el desarrollo del mismo; la implementación será exitosa; como está la de este proyecto.

REFERENCIAS

Aceituno, V. (2009). *Seguridad de la Informacion: Expectativas, riesgos y técnicas de protección. .* Limusa Noriega Editores.

Calvo, J. (2009). *Fuga de Información en las organizaciones.* Recuperado el 23 de Mayo del 2014, de Slideshare: http://es.slideshare.net/bgarcias18/prevencin-de-perdida-de-datos-data-loss-prevention

Cisco Systems, Inc. (2014). *Medidas Prácticas para prevenirla perdida de datos: una gestión de lainformación vital para la empresa.* Recuperado el 15 de mayo del 2014, de www.cisco.com/web/ES/about/press/2008/cisco-noticias-08-03-28.html

Clark, K. (s.f.). *Automated Security Classification.* Consulting Technology Outsourcing.

Cohen, F. (1984). *Virus informáticos: teoría y experimiento.* Estados Unidos: Copyright.

Cormick, M. (2008). *Data Theft: A Prototypical Insider Threat.* Minneapolis.

Gartner. (s.f.). DLP Summary. Recuperado el 15 de Junio del 2014, de http://www.gartner.com

Gestopolis. (2012). *Modulo Administración Dirección Empresas.* Recuperado el 22 de Febrero del 2014, de http://www.gestiopolis.com/administracion-estrategias/modulo-administración-direccion-empresas-libro.pdf

Información Transparente. (2010). *Información Transparente.* Recuperado el 20 de Abril del 2014, de https://informaciontransparente.wordpress.com/lotaip

Inter American Community Affairs. (2012). *International DLP Model.* Recuperado el 15 de Julio del 2014, de http://www.interamericanusa.com/index.htm

International Organization for Standardization - ISO. (s.f.). *Sistema de Gestión de la Seguridad de la Información*. Recuperado el 30 de Junio del 2014, de http://www.iso27000.es/ download/doc_sgsi_all.pdf

Kanagasingham, P. (2012). *SANS Institute Reading Room.* Recuperado el 20 de Agosto del 2014, de Data Loss Prevention: www.sans.org/ reading_room/whitepapers/dlp/data_loss_prevention_32883

Kim, J., & Kim, H. (2010). *Design of Internal Information Leakage Detection System Considering the Privacy Violation.* IEEE.

Kim, Y., Park, N., & Hong, D. (2011). *Enterprise Data Loss Prevention System Having a Function of Coping with Civil Suits.* Computers, Networks, Systems, & Industrial Eng. SCI 365.

McAfee Firewall Enterprise. (2014). *DLP Firewall.* Recuperado el 14 de Mayo del 2014, de www.mcafee.com/es/enterprise/products/network_security/ firewall_enterprise.html

Panda Security. (2014). *Tecnología DLP.* Recuperado el 15 de Junio del 2014, de www.pandasecurity.com/spain/homeusers/media/pressreleases/ viewnews?noticia=5714&ver=20&pagina=9&numprod=&entorno=

Pretschner, A., & W¨uchner, T. (2012). *Data Loss Prevention based on data-driven Usage Control.* IEEE 23rd International Symposium on Software Reliability Engineering.

Prisak, D. (1999). *Dato, Información y Conocimiento* (4 ed.). Estados Unidos: Anonima.

Proctor, P., Mogull, R., & Oullet, E. (2007). *Magic Quadrant for Content Monitoring and Filtering and Data Loss Prevention.* Gartner Inc.

Proctor, P., Mogull, R., & Oullet, E. (2013). *Magic Quadrant for Content Monitoring and Filtering and Data Loss Prevention.* Gartner Inc.

Relaciones Públicas Jurídicas. (2012). *RUA.* Recuperado el 20 de Febrero del 2014, de http://rua.ua.es/dspace/bitstream/10045/13057/8/TEMA 7 RJB

Revista Dintel. (s.f.). *Industria de la Seguridad*. Recuperado el 15 de Abril del 2014, de Prevención de Fuga de Información (DLP): http://www.revistadintel.es/Revista1/Docs Num29/Industria/Ortega.pdf

SANS Institute. (2009). *The Business Justification for Data Security.* Recuperado el 17 de 06 del 2014, de http://www.sans.org/reading-room/whitepapers/dlp/the-business-justification-for-data-security-33033?show=the-business-justification-for-data-security-33033&cat=dlp

Steffens, H. (2010). *Prevencion de Fuga de Datos DLP en 5 Sencillos Pasos*. Recuperado el 15 de Mayo del 2014, de http://liacolombia.com/2010/09/prevencion-de-fuga-de-datos-dlp-en-5-sencillos-pasos/

Thomas R., P. (2005). *Information Security Risk Analysis.* (C. Press, Editor) Recuperado el 18 de Agosto del 2014, de www.acis.org.co/fileadmin/Revista_105/JMGarcia.pdf

Tüv Süv Iberia. (2012). *ISO/IEC 27001*. Recuperado el 30 de Marzo del 2014, de Sistema de Gestión de Seguridad de la Información: http://www.tuv-sud.es/uploads/images/1350635458019372390409/pdf2-0039-iso-iec-27001-es-260412.pdf

Universidad Politécnica Salesiana. (2014). *Las Pymes en el Ecuador.* Recuperado el 20 de Mayo del 2014, de http://dspace.ups.edu.ec/bitstream/123456789/1442/5/|%202.pdf

Wikimedia. (s.f.). *File: Four Level Pyramid Model*. Recuperado el 16 de Abril del 2014, de http://commons.wikimedia.org/wiki/File:Four-Level-Pyramid-model

Wikimedia. (s.f.). *File: Sistemas de Informacion Evolución*. Recuperado el 17 de Abril del 2014, de http://commons.wikimedia.org/wiki/File:Sistemas_de_informacion_evolucion.png

ANEXOS

Anexo 1. Tablas para el desarrollo de la metodología DLP

Áreas Funcionales, de interacción de la empresa

Área Funcional	Áreas de Interacción	Tipo de Información	Descripción del tipo de información
Recursos Humanos	Finanzas, Logística, Sistemas	Base de datos de usuarios, compensaciones, tramites del seguro privado y público,	Información de cada usuario, así como sueldos y áreas de trabajo
Finanzas	Recursos Humanos, Logística, Sistemas	Administración de Crédito, Tiempos de Facturación, Cuadros de Ventas y Compra	Administración de los recursos monetarios. Define los presupuestos manejados por cada área de trabajo. Maneja el crédito y cobranzas por medio de la tesorería
Logística	Recursos Humanos, Finanzas, Sistemas	Calificación de Transporte, Inventarios de transportes, Seguimiento de mantenimiento, Importaciones	Maneja cada uno de los procesos de servicios para la empresa y clientes externos. Maneja todo tipo de importación de elementos de transporte; así como el inventario de cada uno de ellos
Sistemas	Recursos Humanos., Finanzas, Marketing	Inventario de Equipos, Políticas de Seguridad de la Información, Help Desk, Inducciones a usuarios	Maneja cada uno de los sistemas informáticos de la empresa, así como la información que utiliza el usuario en su trabajo diario.

Áreas funcionales de interacción en base a la frecuencia de uso de la información de la empresa

Área Funcional	Áreas de Interacción	Tipo de Información	Descripción del tipo de información	Frecuencia de Uso	Valor para la Empresa	Recepción	Ranking
Recursos Humanos	Finanzas, Logística, Sistemas	Base de datos de usuarios, compensaciones, tramites del seguro privado y público,	Información de cada usuario, así como sueldos y áreas de trabajo	5	5	TEC,SA	5
Finanzas	Recursos Humanos, Logística, Sistemas	Administración de Crédito, Tiempos de Facturación, Cuadros de Ventas y Compra	Administración de los recursos monetarios. Define los presupuestos manejados por cada área de trabajo. Maneja el crédito y cobranzas por medio de la tesorería	5	5	TEC, SA, C	5
Logística	Recursos Humanos, Finanzas, Sistemas	Calificación de Transporte, Inventarios de transportes, Seguimiento de mantenimiento, Importaciones	Maneja cada uno de los procesos de servicios para la empresa y clientes externos. Maneja todo tipo de importación de elementos de transporte; así como el inventario de cada uno de ellos	4	5	TEC, SA, C	5
Sistemas	Recursos Humanos., Finanzas, Marketing	Inventario de Equipos, Políticas de Seguridad de la Información, Help Desk, Inducciones a usuarios	Maneja cada uno de los sistemas informáticos de la empresa, así como la información que utiliza el usuario en su trabajo diario.	4	5	TEC, SA	5

Control de análisis de riesgo de la empresa

Área	Tipo de Información	Riesgo	% TAO		Impacto (1 al 5)			Total		%+-
			% Anterior	% actual	ECT	C	SA	Anterior	Actual	
Recursos Humanos	Base de datos de usuarios, compensaciones, tramites del seguro privado y público,	Alto	6,00%	6,25%	5	2	5	12,060	12,06	%+
Finanzas	Administración de Crédito, Tiempos de Facturación, Cuadros de Ventas y Compra	Alto	3,50%	5,00%	5	4	5	14,035	14,05	%+
Logística	Calificación de Transporte, Inventarios de transportes, Seguimiento de mantenimiento, Importaciones	Alto	2,08%	6,67%	5	5	5	15,021	15,06	%+
Sistemas	Inventario de Equipos, Políticas de Seguridad de la Información, Help Desk, Inducciones a usuarios	Alto	1,67%	8,00%	5	2	5	12,017	12,08	%+

Registro de incidentes e impacto generado en la empresa

Identificador de Seguimiento	Incidente	Área	Tipo de Información afectada	Impacto (1-5)			Solución	Observación
				ECT	C	SA		
1	Almacenamiento de información financiera en distintas carpetas	Finanzas	Administración de Crédito, Tiempos de Facturación, Cuadros de Ventas y Compra	5	4	5	Colocar en una carpeta en una ubicación de red	
2	Información confidencial de los usuarios en manos de los trabajadores	Recursos Humanos	Base de datos de usuarios	5	2	5	Se definió las políticas de acceso para los usuarios	
3	Información de cada manejo de transporte e ingreso de los repuesto con valores a los usuarios en general	Logística	Seguimiento de mantenimiento e importaciones	5	5	5	Se definió las políticas de acceso para los usuarios	

Permisos otorgados a usuarios para manejo de información

Código Empleado	Nombre	Cargo	Área Funcional	Tipo de Información	Permisos	Nivel de Seguridad
60078945	CAROLINA ORBE	GERENTE DE LOGÍSTICA	LOGÍSTICA	Calificación de Transporte, Inventarios de transportes, Seguimiento de mantenimiento, Importaciones	ACCESO TOTAL	ALTO
60074125	DANIELA HERRERA	ASISTENTE DE FINANZAS	FINANZAS	Administración de Crédito, Tiempos de Facturación, Cuadros de Ventas y Compra	ACCESO PARCIAL	MEDIO
60052369	DAVID RAMÍREZ	ESPECIALISTA SISTEMAS	SISTEMAS	Inventario de Equipos, Políticas de Seguridad de la Información, Help Desk, Inducciones a usuarios	ACCESO TOTAL	ALTO
60074586	DAYANA SÁNCHEZ	COMPENSACIONES Y BENEFICIOS	RECURSOS HUMANOS	Base de datos de usuarios, compensaciones, tramites del seguro privado y público,	ACCESO PARCIAL	MEDIO-ALTO

Utilización de equipos de trabajo y dispositivos extraíbles

Nivel de Información Analizada	Área	Tipo de Información	Usuario	Cargo	Equipo	Dispositivo
ALTA	LOGÍSTICA	Calificación de Transporte, Inventarios de transportes, Seguimiento de mantenimiento, Importaciones	CAROLINA ORBE	GERENTE DE LOGÍSTICA	LAPTOP	USB
MEDIA	RECURSOS HUMANOS	Base de datos de usuarios, compensaciones, tramites del seguro privado y público,	DAYANA SÁNCHEZ	COORDINADORA DE RECURSOS HUMANOS	LAPTOP	USB
ALTA	FINANZAS	Administración de Crédito, Tiempos de Facturación, Cuadros de Ventas y Compra	DANIELA HERRERA	ASISTENTE DE FINANZAS	LAPTOP	USB

Control de Respaldos

Responsable	Área	Cargo	Tipo de Información	Medio de Respaldo	Autorización	Cargo	Fecha
DAVID RAMÍREZ	LOGÍSTICA	ESPECIALISTA SISTEMAS	Calificación de Transporte, Inventarios de transportes, Seguimiento de mantenimiento, Importaciones	USB	CAROLINA ORBE	GERENTE DE LOGÍSTICA	10/10/2014
DAVID RAMÍREZ	FINANZAS	ESPECIALISTA SISTEMAS	Administración de Crédito, Tiempos de Facturación, Cuadros de Ventas y Compra	USB	BYRON ALMEIDA	COORDINADOR DE FINANZAS	14/10/2014
DAVID RAMÍREZ	RECURSOS HUMANOS		Base de datos de usuarios, compensaciones, tramites del seguro privado y público,	CD	GALO VÁSQUEZ	COORDINADOR DE RECURSOS HUMANOS	15/10/2014
DAVID RAMÍREZ	SISTEMAS		Inventario de Equipos, Políticas de Seguridad de la Información, Help Desk, Inducciones a usuarios	USB	JUAN CARLOS PAREDES	COORDINADOR DE SISTEMAS	18/10/2014

Anexo 2. Políticas y directivas de seguridad de la información Winchas Tarqui

Directriz Winchas Tarqui
Acerca de la protección de datos Personales

Preámbulo

Como grupo que funciona en Ecuador, Winchas Tarqui utiliza sistemas en todas las áreas para procesar e intercambiar datos entre las unidades del grupo, así como con terceros. Aumentando la cooperación económica y científica y la provisión mutua de servicios de procesamiento de datos que también exigen el intercambio de datos personales, una tendencia reforzada por el incremento en la utilización de los recursos modernos de telecomunicación. Por lo tanto, es necesario que los datos personales sean procesados cuidadosamente.

1. COMPROMISO

Winchas Tarqui declara que cumplir con los principios de protección en el procesamiento de datos personales (ej. datos de clientes, proveedores y empleados) es un objetivo corporativo. Como tal, Winchas Tarqui está comprometido en respetar los derechos personales y privacidad de estos individuos.

Como grupo encargado del cuidado de la salud, Winchas Tarqui trata los datos personales de clientes y usuarios internos con cuidado especiales.

2. OBJETIVOS

Adoptar la actual directriz del grupo Winchas Tarqui acerca de la protección de datos personales ("directriz"), Winchas Tarqui está persiguiendo tres objetivos. Primero, la directriz establece un estándar mínimo uniforme a ser

aplicado por todas las compañías de Winchas Tarqui en el procesamiento de datos personales y fijar las bases para acuerdos contractuales con terceros. Segundo, la directriz proporciona salvaguardias preventivas contra la infracción de los derechos de personalidad y privacidad a través de procesamiento inadecuado de datos personales. En tercer lugar, la directriz proporciona un nivel adecuado de protección de datos personales según los requisitos de establecidos.

3. DEFINICIONES

Para el propósito de esta directriz, las siguientes definiciones aplican:

Asunto de los datos significará cualquier persona natural cuyos datos personales sean procesados por o en nombre de Winchas Tarqui.

Datos personales significará cualquier información que se relacione con una persona natural identificada o identificable, de la cual se exprese algo acerca del reconocimiento médico, fisiológico, psicológico, mental, económico, de identidad cultural o social.

Proceso significará cualquier operación o sistema de operaciones realizadas en los datos personales, que incluyen, pero no se limitan a la colección, grabación, almacenaje, alteración, análisis, uso, transmisión, combinación, bloqueo, borrado y destrucción.

4. APLICACIÓN

Esta directriz aplica a todas las compañías de Winchas Tarqui y a sus empleados.

Donde los datos personales son procesados por terceras partes a nombre de Winchas Tarqui, las medidas apropiadas serán tomadas para asegurar el

cumplimiento de dichos terceros con los principios dispuestos en esta directriz.

La legislación nacional que prevé salvaguardias más sensitivas acerca de los datos personales también será observada en todos los casos específicos donde tal legislación aplique.

5. PRINCIPIOS

En general, los datos que revelan información racial del sujeto o de origen étnico, puntos de vista políticos, convicciones religiosas o filosóficas o una afiliación con una organización que represente los intereses de empleados deben ser clasificados como altamente sensibles, al igual que datos sobre la salud o el comportamiento sexual del sujeto. Todos los datos personales se deben procesar legalmente. En particular, los siguientes principios aplican:

5.1 Criterios de legalidad

Los datos personales pueden ser procesados si por lo menos uno de los siguientes aplica:

- El sujeto de los datos ha dado consentimiento;
- El proceso es necesario para el funcionamiento de un contrato del cual el sujeto de los datos es parte;
- El proceso es necesario para el cumplimiento de una obligación legal;
- Winchas Tarqui está persiguiendo un interés legítimo, excepto donde tal interés es eliminado por el interés del sujeto afectado por los datos.

5.2 Principios referentes al proceso

Los datos personales se deben procesar de una manera compatible con el propósito para el cual fueron recogidos.

- El principio de la proporcionalidad se aplicará al proceso de datos personales. Entre otras cosas, esto implica un deber de abstenerse de recoger datos personales innecesarios.

- Los datos personales que se utilizan serán exactos y actualizados.

- Los datos personales se utilizan qué y que son exactos o completos no más largo serán corregidos o suprimidos.

- Conforme a las estipulaciones legales que requieren un periodo de validez más largo, los datos personales deben ser almacenados no más que lo necesario para efectuar los propósitos para los cuales fueron recogidos o procesados.

- Los datos personales deben ser procesados de una manera siempre constante con el principio de la buena fe. Esto significa que los sujetos de los datos pueden confiar en los procesadores que ejercen el debido cuidado en todos los aspectos del procesamiento de datos.

6. DERECHOS DEL SUJETO CON RELACIÓN A SUS DATOS

Las personas de quienes se han procesado datos personales deben ser consecuentemente informadas bajo requerimiento. En particular, ellas tienen el derecho de ser informadas de los propósitos para los cuales se están procesando los datos, la categoría de los datos implicados y la identidad de los destinatarios de los datos. Cuando sea apropiado, los sujetos de los datos también tienen el derecho de requerir que los datos sean corregidos, bloqueados o suprimidos.

Los derechos ya mencionados pueden ser restringidos solamente donde tal restricción sea prohibida por la ley. Esto aplica, en particular, al manejo de las investigaciones científicas.

7. MEDIDAS

Las compañías del grupo de Winchas Tarqui son los que ponen en practicar las medidas técnicas y organizacionales necesarias para garantizar la seguridad de los datos personales.

En particular, los datos personales serán protegidos contra divulgación no autorizada y cualquier forma de proceso ilegal. Las medidas implementadas deben asegurar un nivel de seguridad apropiado a la naturaleza de los datos protegidos y de los riesgos que se presentan en el procesamiento de datos.

8. PUESTA EN PRÁCTICA

Todas las compañías de Winchas Tarqui a nivel individual son responsables de implementar y hacer cumplir esta directriz.

Los empleados de Winchas Tarqui implicados en el procesamiento de datos personales deben ser informados apropiadamente.

Los procedimientos para el procesamiento de datos personales hechos por terceras partes estarán de conformidad con acuerdos contractuales por escrito. La compañía Winchas Tarqui respectiva se asegurará que los terceros contratados estén procesando los datos correctamente y que estén cumpliendo con los principios dispuestos en esta directriz. Si en cualquier momento se determina que la tercera parte esta incapacitad para garantizar una adecuada seguridad de los datos personales, Winchas Tarqui terminará el acuerdo.

9. FECHA EFICAZ

El actual Directriz fue adoptada por el comité ejecutivo corporativo el 11 de septiembre de 2014, y entró en efecto esa fecha.

Directriz Winchas Tarqui acerca del "Uso de las herramientas de comunicación electrónica de Winchas Tarqui"

1. Objetivo

Esta directriz se dirige al uso de herramientas de comunicación electrónica de Winchas Tarqui esquematizando las reglas principales de conducta a ser observadas por los empleados de Winchas Tarqui al utilizar las herramientas electrónicas de comunicación en la empresa.

2. Definiciones

- El término "herramientas de comunicación electrónica de Winchas Tarqui" cubre los teléfonos propios de la compañía, máquinas de fax, computadoras, sistemas de correo electrónico, sistemas Intranet y sistemas Internet.

- El término "uso personal" significa cada instancia de uso que no está directamente relacionada con los propósitos del negocio de Winchas Tarqui.

3. Uso

- Las herramientas de comunicación electrónica de Winchas Tarqui deben ser utilizadas en principio y sobre todo para los propósitos del negocio.

- En casos excepcionales, los empleados de Winchas Tarqui pueden utilizar las herramientas de comunicación electrónica de Winchas Tarqui

para su propio uso personal, siempre y cuando las siguientes precondiciones se cumplan:

- El rendimiento personal del empleado en el trabajo no se deteriora;
- El trabajo de otros empleados no es afectado negativamente;
- Winchas Tarqui no incurre en costos adicionales significativos;
- solamente un mínimo de los recursos de Informática son utilizados;
- La utilización mantiene el debido cuidado, confidencialidad y cumplimiento legal según lo publicado en el artículo 5 de este documento.

4. Procedimientos de seguridad y autorización

- Empleados quiénes tienen acceso a las herramientas de comunicación electrónica de Winchas Tarqui deben manejarlas con el debido cuidado y asegurar que no se dañen, se pierdan ni se cambien de lugar.
- El retiro de cualquier herramienta electrónica de comunicación de Winchas Tarqui fuera de las instalaciones de la compañía, debe ser aprobado por adelantado. El grupo de seguridad debe verificar tales autorizaciones en cualquier momento.

5. Debido cuidado, confidencialidad y cumplimiento legal

- Mensajes creados y remitidos usando las herramientas de comunicación electrónica de Winchas Tarqui, se deben redactar siempre con el debido y correspondiente cuidado según el caso en particular.

- Mensajes deben ser enviados solamente a aquellas personas, tanto en el interior como en el exterior de la compañía, que necesiten realmente la información comunicada.

- Información Confidencial debe ser tratada con la precaución necesaria. Al usar las herramientas de comunicación electrónica vía Internet, la confidencialidad de un mensaje no puede ser garantizada a menos que se cifre.

- Los siguiente tipos de mensaje no pueden ser creados o transmitidos:

  - Mensajes con contenido ilegal, indecente, discriminatorio, acosador, despectivo, deshonroso, amenazador o moralmente ofensivo;

  - Uso de documentos y/o software, en contra de los derechos de autor.

  - Cartas de cadena;

  - Comunicaciones en las cuáles se ha cambiado o encubierto la identidad del autor.

6. Protección de los datos del E-mail y del Internet

- El uso del sistema Internet por parte de los usuarios a nivel personal está sujeto a las leyes de protección de los datos. El personal de Informática está facultado para leer mensajes o enviar información al exterior o hasta donde sea necesario para remediar un malfuncionamiento, para propósitos de mantenimiento o para asegurar los datos en el sistema de E-mail o en el sistema de Internet. El personal de Informática está autorizado para hacer que la información obtenida sea accesible a los terceros solamente si se asegura la confidencialidad y si tal divulgación es absolutamente necesaria para la terminación del trabajo en cuestión.

- La confidencialidad de los datos sin reserva no está garantizada. La confidencialidad de los datos puede ser revocada para usuarios individuales de acuerdo con los requerimientos legales locales que apliquen. Por ejemplo tal paso puede ser considerado si hay argumentos legales tales como la prevención o la limitación del daño en donde Winchas Tarqui o los empleados de Winchas Tarqui de alguna manera puedan incurrir. Es cuestión del departamento legal y del departamento de seguridad Informática de Winchas Tarqui decidir, en consulta con el gerente de recursos humanos relevante, qué medidas pueden ser tomadas según sea el caso.

7. Medidas

- Todas las compañías en el grupo Winchas Tarqui deben tomar las medidas técnicas y organizacionales necesarias para garantizar el cumplimiento de esta directriz.

- Esta Directriz no afecta las provisiones de la Política de Seguridad de Informática ni otras regulaciones detalladas vigentes a nivel departamental ni a ningún otro nivel; tales regulaciones deben ser siempre observadas.

8. Ejecución

- Todas las personas de la compañía Winchas Tarqui son responsables de hacer cumplir esta Directriz.

- Todos Los empleados de Winchas Tarqui deben ser informados consecuentemente.

9. Entrada en vigor

Este Directriz con respecto al uso de las herramientas de comunicación electrónica de Winchas Tarqui fue adoptada por el comité ejecutivo corporativo el 11 de Septiembre de 2014 y entro en vigor el mismo día.

De: **Winchas Tarqui.** **Sistemas**

Para: **Usuario** **31 de agosto de 2015**

REF.: Confidencialidad de su contraseña personal para los Sistemas de Información Winchas Tarqui Ecuador

Para permitir su identificación cuando utilice nuestro Sistema, se le ha asignado un **USER-ID** (**……..**) será usado junto a una contraseña **PASSWORD** (……), que podrá ser cambiado presionando CTRL + ALT + SUPR, seleccionando Change Password. Tenga en cuenta que: Windows 7 valida **mayúsculas** y **minúsculas**.

Su contraseña es para su uso personal, actúa como su identificación en cualquier terminal que usted utilice. Su contraseña no debe, **bajo ninguna circunstancia** ser comunicada a otra persona y no debe haber ninguna otra persona trabajando en el computador usando su User-id. Usted es responsable por cualquier daño intencional o accidental que pueda ocurrir mientras se usa su USER-ID, para garantizar la seguridad de la información, usted debe cambiar su contraseña cada vez que lo considere necesario, o por lo menos cada 360 días, de lo contrario el computador lo obligará a hacerlo.

Cuando seleccione su nueva contraseña siga estas normas:

- La contraseña debe ser una combinación de mínimo 8 caracteres, teniendo en cuenta que contenga una mayúscula y un número, NO debe contener caracteres especiales.

- La contraseña no debe ser trivial, como su nombre y/o apellido, nombres de familiares o palabras muy conocidas.

- Nunca escriba su contraseña en sitios con fácil acceso, seleccione una que pueda recordar fácilmente.

Dirección del Correo Electrónico: ……@wtarqui.com.ec

Atentamente,

Sistemas-Winchas Tarqui, Ecuador

_ _

De: **……** Winchas Tarqui Ecuador.

Confirmo que leí y entendí las condiciones de confidencialidad y estoy de acuerdo con las reglas pertinentes a la seguridad del Sistema; tanto confidencialidad de la contraseña, de la información, de los archivos, así como de los programas y documentación. Entiendo que revelar información confidencial podría acarrearme sanciones por parte de la compañía.

Firma del Usuario: Red PC's: Windows 7

31 de agosto de 2015