ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"IMPLEMENTACIÓN DE UNA SOLUCIÓN DE PREVENCIÓN DE FUGA DE INFORMACIÓN EN UNA EMPRESA DE TELECOMUNICACIONES"

EXAMEN DE GRADO (COMPLEXIVO)

Previo a la obtención del grado de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

DAVID XAVIER SÁNCHEZ RODRÍGUEZ

GUAYAQUIL – ECUADOR

AÑO: 2015

AGRADECIMIENTO

A mis compañeros de aula y profesores del MSIA y a mis compañeros de trabajo que contribuyeron de manera directa o indirecta en el desarrollo de este trabajo.

A mis padres Carlos y Blanca y a mis hermanos Rocío y Juan Francisco, por sus consejos, dedicación, esfuerzo y generosidad, quienes han sido ejemplo de vida y guía para el logro de mis objetivos.

A mi esposa Elena Alexandra, por su comprensión paciencia y apoyo constante, lo que me ha permitido culminar esta etapa de superación profesional.

DEDICATORIA

A mis hijos: David, Gabriela y Carlos, pilares fundamentales y fuente de energía divina, quienes me han procurado la fortaleza para llevar adelante cada uno de los proyectos de desarrollo profesional y personal que he emprendido.

A mi entrañable hermano Carlos Alberto Sánchez Rodríguez, quien ha sido fuente de inspiración y que a pesar de ya no estar físicamente junto a mí su esencia ha estado y estará por siempre iluminando mi camino.

TRIBUNAL DE SUSTENTACIÓN

Mgs. Albert Espinal

Profesor Delegado
por la Maestría de Seguridad
Informática Aplicada

Mgs. Jorge Olaya

Profesor Delegado
por la Facultad en Ingeniería
en Electricidad y Computación

RESUMEN

El presente trabajo de titulación consolida las diferentes etapas que se ejecutaron durante la implementación de un proyecto de Prevención de Fuga de Información (o **DLP** por sus siglas en inglés). Este proyecto inició en el año 2013 en una empresa de telecomunicaciones del país, siendo su principal objetivo proveer a la organización de una solución de detección y prevención de posibles incidentes de fuga de información considerada sensible o confidencial.

Para cumplir con los objetivos planteados la solución DLP implementada cuenta con mecanismos que le permiten detectar información sensible que pudiera estar fugando de la compañía a través de: la red, en un dispositivo externo, del servicio de impresión corporativo u otros. Para el efecto se dispone de controles a nivel de los siguientes estados asociados a la información:

- Data en Tránsito: data transmitida hacia Internet vía la red LAN corporativa.
- Data en Uso: data manipulada en estaciones de trabajo y equipos portátiles de propiedad de la compañía

- Data en Reposo: data sensible almacenada en bases de datos y servidores de archivos.

Las reglas de detección implementadas obedecen a las necesidades que el negocio ha planteado para la protección de su información sensible, lo que le permite identificar tempranamente posibles eventos de fuga de información.

ÍNDICE GENERAL

ABREVIATURAS

CD	Disco Compacto
DLP	Prevención de Fuga de Información
DOC	Formato de archivos de Microsoft Word
FTP	Protocolo de Transferencia de Archivos
HTTP	Protocolo de Transferencia de Hipertexto
HTTPS	Protocolo de Transferencia de Archivos por SSL
ICAP	Protocolo de Adaptación de Contenidos de Internet
IMAP	Protocolo de acceso a mensajes de internet
ISO	Organización de Estándares Internacionales
ISO 27001	Estándar de Seguridad de la Información.
PC	Computadora Personal
PoC	Prueba de Concepto
RBAC	Control de Acceso Basado en Roles
SMTP	Protocolo de transferencia simple de correo electrónico
USB	Bus Serie Universal
XLS	Formato de archivos de Microsoft Excel

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En los últimos años, las empresas de telecomunicaciones no han sido ajenas a los riesgos inherentes a la protección de sus activos de información, se ha trabajado fuertemente en la reducción de las brechas de seguridad a nivel perimetral incorporando firewalls, sistemas de prevenciones de intrusiones, sistemas antispam, entre otros; sin embargo, a nivel interno es mucho lo que falta por hacer para asegurar los denominados datos sensibles o altamente confidenciales.

Recientemente se está reportando un aumento del número de incidentes de violación de datos vinculados con información privilegiada de las entidades atacadas en las cuales se ha denotado la participación de atacantes externos a la organización en cooperación con personal interno con acceso autorizado a dicha información sensible.

Con la finalidad de reducir la superficie de exposición de la información sensible, las organizaciones están incorporando restricciones a nivel del acceso a los datos que se encuentran en los sistemas comerciales, bloqueando o restringiendo el acceso a Internet e implementando sistemas de monitoreo en tiempo real que permitan alertar tempranamente la ocurrencia de algún incidente relacionado con una posible fuga de información sensible.

Sin embargo, estos esfuerzos no son suficientes en función de la poca granularidad de los controles que se pueden implementar, así como también en prestar las facilidades para que el intercambio de información con clientes, terceras partes y prestadores de servicios se realice de manera segura pero sin representar una camisa de fuerza que entorpezca los procesos del negocio.

En función de las necesidades que las operaciones del negocio demandan, las empresas se están encaminando en la implementación de **Soluciones de**

Prevención de Fuga de Información (o **DLP**, por sus siglas en inglés) que les permitan cubrir los siguientes macro objetivos:

- Alertar tempranamente posibles incidentes de fuga de información de manera más eficiente y eficaz.
- Gestionar activa, proactiva y predictivamente los incidentes de fuga de información, contribuyendo al enfoque integral de defensa en profundidad.
- Tener visibilidad de la información sensible que pudiera estar abandonando el perímetro corporativo por los diferentes canales de transmisión de información con que cuentan los colaboradores que disponen de acceso autorizado.
- Mejorar en el cumplimiento normativo y regulatorio al disponer de medidas de control que minimicen los incidentes de fuga de información.

El lector encontrará en el desarrollo de este documento las etapas que se siguieron en la implementación del Proyecto DLP, los alcances y limitaciones de la solución implementada, un conjunto de mejoras que

deberán considerarse para fortalecer los controles automáticos y las recomendaciones en torno a los procedimientos internos que la organización deberá aplicar en sus procesos operativos para mantener el círculo virtuoso de la mejora constante.

CAPÍTULO 1

GENERALIDADES

1.1 Antecedentes

En el contexto de la seguridad de TI, el objetivo es evitar la extracción accidental, intencional y no autorizada, inserción, modificación o destrucción de datos en una base de datos [1].

Como es de conocimiento público, grandes compañías como Target, Staples, eBay y Sony han sufrido graves violaciones en torno a la seguridad de sus datos, por lo que es hora de replantearse si las organizaciones están llevando a cabo las mejores prácticas de

seguridad de la industria en cuanto al manejo de la información sensible.

Actualmente, la mayoría de las empresas disponen de mecanismos que les permiten de cierta forma controlar el acceso a la información sensible. No obstante, estos controles no tienen la amplitud, especificidad y no se mantienen actualizados, por lo que el resultado es como ya hemos comentado que en empresas de diferente naturaleza y procedencia se produzcan fugas de información sensible o confidencial. Estas fugas generan riesgos que afectan a las empresas, a sus clientes y asociados de negocios, provocando incumplimientos de carácter legal o normativo, afectación a la imagen empresarial, con el consiguiente impacto en sus finanzas y en su credibilidad.

1.2 Objetivo General

Implementar una solución informática que permita identificar y prevenir posibles fugas de información sensible de la organización.

1.3 Descripción del Problema

En la actualidad las amenazas que afectan los sistemas informáticos y la información que es depositada en ellos o que se transmite a través de las redes corporativas son reales y van en aumento, en particular por el incremento de organizaciones cibercriminales que se apoyan en personal interno (“El 78% de las filtraciones de datos las cometen empleados autorizados de una empresa.”, según lo señala el Instituto Ponemon [2]), lo que compromete aún más los datos sensibles de las organizaciones. Esta situación afecta a empresas de diferente naturaleza y las empresas de telecomunicaciones no son ajenas a esta problemática, por lo que se vuelve necesario disponer de un mecanismo que posibilite prevenir, detectar y contener un posible comprometimiento de la información considerada sensible o confidencial. Ya no es suficiente contar con defensas perimetrales, ya que estas no ayudan contra las amenazas internas.

Como ya se ha indicado dado el número creciente de amenazas, tales como extracción no autorizada, espionaje o negligencia por parte de usuarios internos o externos a nuestra organización, así como la

sofisticación de las técnicas utilizadas por los potenciales atacantes el riesgo de exposición de la información se ha visto incrementado.

Por los motivos expuestos, se requiere tener visibilidad de la ubicación de la información sensible para establecer los mecanismos de protección y monitoreo apropiados, así como también se necesita contar con un conjunto de procedimientos internos en torno a la gestión que deben ejecutar los involucrados respecto del tratamiento de los incidentes relacionados con posibles eventos de fuga de información sensible.

1.4 Solución Propuesta

La problemática planteada vuelve necesario contar con herramientas que permitan detectar, prevenir y de ser necesario bloquear cualquier intento de fuga de información que pudiere estar afectando los intereses de la organización tales como: competitividad, imagen empresarial y cumplimiento normativo y regulatorio.

La organización consciente del riesgo actual en cuanto a las limitaciones de protección de su data sensible, tomó la decisión de implementar una solución que le permita adoptar el enfoque de equilibrio entre la identificación de comportamiento malicioso y la flexibilidad que la operativa de los procesos que ejecuta el personal interno requiere.

Esta preocupación ha dado lugar a la búsqueda de una solución que permita a la organización disponer de la capacidad de descubrimiento, monitoreo, prevención y protección de su información sensible, estas soluciones se conocen como **Prevención de Fuga de Información** (o **DLP** por sus siglas en inglés).

La solución referida incluye:

- Definición e implementación de reglas de detección de una posible fuga de información.
- Definición de políticas de uso autorizado y de protección de la información.

- Implementación de acciones de bloqueo del movimiento no autorizado de información.
- Notificación de Posibles Incidentes al personal asignado para su confirmación, descarte (falso positivo) o reacondicionamiento de las reglas de detección.

Con la implementación de un sistema DLP se obtienen los siguientes beneficios:

- El DLP ayuda a la organización con la identificación y tratamiento de los incidentes de fuga de información de manera más eficiente y eficaz.
- El DLP posibilita una gestión Activa, Proactiva y Predictiva en la detección de eventos de fuga de información, y forma parte del enfoque integral de defensa en profundidad.
- La organización obtiene visibilidad de la información sensible que pudiera abandonar su perímetro corporativo por los diferentes canales de transmisión de información con que cuentan sus colaboradores internos y externos.

- La organización mejora en su cumplimiento normativo y regulatorio al disponer de medidas que minimizan los incidentes de fuga de información.

Figura 1.1. Funciones del DLP

CAPÍTULO 2

SOLUCIÓN TECNOLÓGICA IMPLEMENTADA

2.1 Metodología

Para el proceso de gestión de incidentes de fuga de Información se consideran 4 Fases:

1. Visibilidad: descubrimiento de información sensible y monitoreo de incidentes a nivel de la consola de gestión
2. Remediación: Creación y afinamiento de reglas
3. Notificación: comunicación al empleado de una posible violación de seguridad y escalamiento a los responsables de los procesos del negocio involucrados con el incidente que se está evaluando

4. Prevención: aplicación de acciones de protección que pueden incluir las siguientes:
    a. Bloqueo
    b. Cifrado
    c. Cuarentena

El modelo de gestión de los incidentes de fuga de información incorpora los siguientes aspectos:

- Centralizado de tiempo parcial (5x8)
- Orientado a los requerimientos del negocio (definiciones de las reglas de detección provienen de las áreas internas dueñas de la información sensible)
- Procedimientos maduros de clasificación de información (tomando como base las políticas internas de clasificación de la información)

Para la generación de políticas o reglas de detección de incidentes se aplica el siguiente esquema:

Figura 2.1. Proceso para elaboración de políticas de DLP.

Las técnicas de detección usadas por la solución DLP a implementar son las siguientes [3]:

- Reglas basadas en análisis de expresiones (uso de expresiones regulares): examina el contenido de un documento digital buscando patrones específicos (ej.: un patrón de 10 dígitos asociados a una cédula de identidad o un formato de n dígitos asociados a una tarjeta de crédito). Este método es rápido y efectivo ya que busca dentro de un documento data que mantiene una estructura definida dentro de la regla de detección.

- Filtrado de Palabras Clave: es similar a la técnica anterior, excepto por el hecho de que la búsqueda se orienta a determinadas palabras o frases que denotan la sensibilidad de un documento o texto (ej.: “Confidencial”, Secreto”) que está siendo manipulado en sus diferentes vectores. También es de utilidad para identificar fuga de contenido digital que contiene una palabra específica.

- Coincidencia Exacta de Datos (Huella Digital): compara un conjunto de datos contra dato estructurada sensible de una fuente restringida para determinar si existe una coincidencia exacta. El conjunto de datos a comparar debe ser un subconjunto exacto de la data original, sin embargo, la sensibilidad de la comparación puede arrojar una ingente cantidad de falsos positivos. Esta técnica de detección es precisa pero dependiendo de la cantidad de data a comparar puede tornarse en un proceso lento que demande altos recursos del sistema, por lo que este método es usado preferentemente para data en reposo y data en uso.

- Coincidencia Parcial de Datos: la data sensible a proteger es dividida en pequeñas secciones y de éstas se obtiene su hash, luego será posible comparar el hash de un determinado conjunto de datos con las hashes “sensibles” para verificar su coincidencia. Esta técnica sería mucho más efectiva si se mantuviere un conjunto limitado de documentos catalogados como sensibles por la organización (lista blanca).

La siguiente tabla muestra la efectividad de cada una de las técnicas de detección mencionadas:

TECNICA	DATA EN MOVIMIENTO	DATA EN REPOSO	DATA EN USO	COMENTARIOS
Reglas basadas en de expresiones	Alta	Alta	Media	Efectiva para datos con estructuras bien definidas
Filtrado de Palabras Clave	Alta	Alta	Alta	Efectiva para data que está cambiando constantemente
Huella Digital	Media	Alta	Alta	Efectiva para data estructurada o archivos sensibles
Coincidencia Parcial de Datos	Media	Alta	Media	Efectiva para comparar un número limitado de datos sensibles

Tabla 1. Proceso para elaboración de políticas de DLP**.**

Nota: es importante acotar que independientemente de la técnica de detección usada para identificar data sensible no siempre será posible ejecutar una acción de bloqueo sobre la data identificada ya que esto podría perjudicar la operación del negocio, de la misma manera la organización debe estar consciente que no siempre será posible identificar una posible fuga de información sensible.

2.2 Desafíos del Proyecto

- Poca atención de las unidades de negocio hacia estas tecnologías y la dificultad de obtener apoyo y colaboración de parte de las mismas.

- La necesidad de establecer una estrecha colaboración con las unidades de negocio, propietarias de la información; y, por el otro, la definición de una política de seguridad de la información que contemple la clasificación de la información como uno de los pilares para garantizar su protección.

- Saber comunicar la importancia y los beneficios de la prevención de fuga de información

- Un elemento crítico en la implantación de una solución basada en DLP es la complejidad de la organización, en todas sus

dimensiones, siendo éste el factor de riesgo más determinante para el éxito del proyecto.

- Definir claramente lo que está permitido como uso personal de los recursos informáticos y lo que no, para no sembrar dudas acerca de la legitimidad del uso de estas herramientas. Ser lo más respetuoso e íntegro en el manejo de los resultados, para transmitir confianza a los usuarios. Comunicar todo esto de una forma eficaz y accesible para toda la organización.

- Para lograr una implementación exitosa de la solución DLP es necesario considerar las necesidades específicas de la organización para realizar las personalizaciones y ajustes que fueren requeridos.

2.3 Selección de Herramientas DLP a evaluar

El proyecto DLP inicio con la selección de las soluciones a evaluarse, para el efecto se tomó como referencia cuatro de las soluciones consideradas Líderes por la empresa consultora y de investigación de tecnologías de la información Gartner (Figura 2.2) y que contaban con representación local.

Figura 2.2. Cuadrante Mágico de Gartner - Soluciones DLP (Año 2013).

Fabricante	Producto	Breve Reseña de la Solución
websense ESSENTIAL INFORMATION PROTECTION	**Websense Data Security Suite**	Es la única solución de prevención de fugas de información (DLP) que permite conocer el contenido, el contexto y el destino de la información, con lo que los administradores pueden controlar quién puede enviar qué información dónde, y cómo lo hace. Websense Data Security Suite incorpora un avanzado sistema de definición de políticas que

		permite planificar las políticas de datos alrededor de los procesos empresariales y así proteger la información en la red y en los puestos de usuario. Incorpora una potente plataforma de creación y gestión de políticas para garantizar la continuidad de las operaciones y la seguridad de la información. Esta funcionalidad exclusiva ofrece los niveles de visibilidad y control necesarios para gestionar quién y qué va dónde, y cómo lo hace.
	**Symantec Data Loss Prevention**	Symantec Data Loss Prevention ofrece una solución unificada para detectar, supervisar y proteger la información confidencial sin importar dónde se almacene o cómo se utilice. Symantec ofrece una cobertura integral de la información confidencial en el endpoint, la red y los sistemas de almacenamiento, tanto si los usuarios están conectados a la red corporativa o como si no. Al reducir el riesgo sensiblemente, Symantec brinda a las organizaciones una confianza renovada para demostrar el cumplimiento, mientras protegen la marca, la propiedad intelectual y los clientes.
	Symantec™ Data Loss Prevention for Endpoint Agent Management	Symantec Data Loss Prevention se encarga de la protección de datos en medios portátiles con el fin de descubrir datos confidenciales de laptops, equipos de escritorio y de estaciones de trabajo. También proporciona a los clientes de punto final completa cobertura de los datos en cuanto a pérdida ya que protege la información confidencial, evitando: • Copiado al USB, tarjetas SD u otros medios extraíbles • Grabado a medios ópticos (CD / DVD) • Transferencias a través de correo electrónico, páginas web, mensajería instantánea o FTP.
	**McAfee Network DLP Discover**	Para identificar la información y la proliferación de riesgos McAfee Network DLP Discover puede ser configurado para buscar datos específicos que requieran protección dentro de repositorios. Adicionalmente todos los datos obtenidos por McAfee Network DLP Discover, se ordenan los datos sensibles de manera que sea rápida la búsqueda de estos datos, permitiendo encontrar la información que pueda ser sensible y entender como resguardarla.
	McAfee Network DLP Manager	Administración centralizada de dispositivos McAfee Network Data Loss Prevention. McAfee Network Data Loss Prevention (DLP) Manager está diseñado para ambientes grandes y medianos con varios dispositivos McAfee Network DLP instalados a lo largo de la red. Brinda un control total sobre múltiples dispositivos McAfee Network DLP.

RSA SECURITY	**RSA Data Loss Prevention Suite**	La solución de RSA está diseñada para permitir a las organizaciones descubrir, supervisar y gestionar de manera más adecuada los riesgos relacionados con la pérdida de datos confidenciales en sus infraestructuras, incluyendo smartphones y tablets.

Tabla 2. Soluciones DLP evaluadas.

2.4 Hitos del Proyecto

Para un mejor control y seguimiento de los avances del proyecto se lo dividió en 6 hitos:

1. Definición y Alcance del Proyecto
2. Requerimientos Técnicos
3. Evaluación Técnica de las soluciones ofertadas
4. Implementación
5. Capacitación
6. Puesta en Producción

2.4.1 Hito 1: Definición y Alcance del Proyecto

Identificar los datos estructurados y no estructurados que necesitan protección.

Clasificación de los datos: necesaria para lograr aplicar las políticas de prevención de fuga de información en función de las definiciones (reglas del negocio) de las áreas dueñas de la información. En esta etapa lo primero será definir cuál es la información que la compañía quiere proteger, dónde está alojada, cómo se utiliza y por parte de quién.

Dimensionamiento de la Solución: se deben considerar los siguientes aspectos para el dimensionamiento del hardware:

- El throughput de la interfaz que tiene conectada el Proxy de navegación Web.
- La cantidad de nodos que tiene el proxy web, si se encuentran en alta disponibilidad, y de qué forma operan: activo/activo o activo/pasivo.
- La cantidad de nodos que tiene el servicio de correo corporativo, si se encuentran en alta disponibilidad, y de qué forma operan: activo/activo o activo/pasivo.
- Disponen de un Gateway de correo de salida con capacidades de modificación de la cabecera de correo para la funcionalidad de cifrado del correo.

- Las conexiones de red de todos los puntos de integración al DLP son de cobre o de fibra óptica.
- Compatibilidad con marcas/versiones de base de datos y sistemas operativos para la función de detección de data sensible en reposo.
- Tráfico que maneja la interface de salida a Internet y protocolos que se desean monitorear.

Alcance de la solución DLP: contempló los siguientes 3 vectores de fuga de información:

- Data en **Movimiento (Red):** información que transita por la red corporativa
    - Monitoreo y Prevención de fuga de información que vaya hacia Internet
    - Protocolos: SMTP, HTTP, HTTPS, IM, FTP, entre otros.

- Data en **Reposo (Almacenamiento):** información que es almacenada en servidores de archivos y bases de datos críticas

- Monitoreo de un servidor de archivos y una base de datos crítica
- Directorios compartidos con información privilegiada
- Información Comercial de clientes y Documentos de Nuevos Proyectos y Estrategias de Comercialización

- Data en **Uso (Endpoint):** información que es manipulada en las estaciones de trabajo y dispositivos móviles.
  - PCs/Laptops con acceso a Internet con accesos privilegiados
  - Acceso a correo web, navegación web, almacenamiento en medios removibles, almacenamiento virtual, impresión de documentos, capturas de pantalla, entre otros.

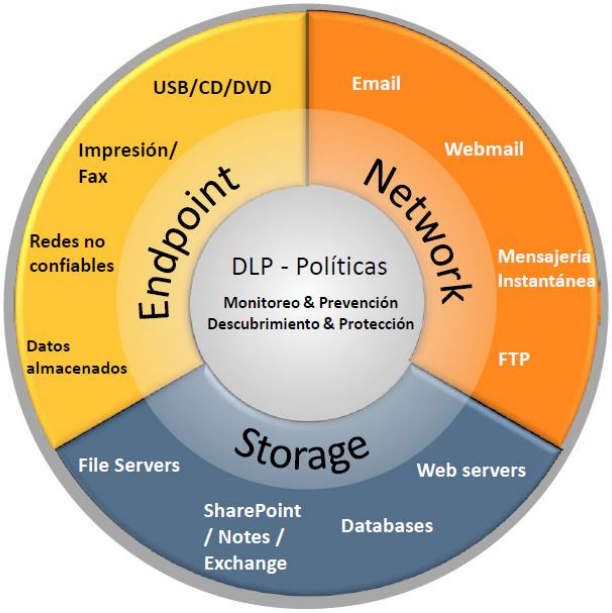

Figura 2.3. Vectores de Fuga de Información.

2.4.2 Hito 2: Requerimientos Técnicos

Los requerimientos técnicos requeridos a cada uno de los proveedores participantes se segmentaron en función de cada uno de los módulos que componen la solución de la siguiente manera:

A nivel de **Endpoint**:

- DLP de Endpoint para Descubrimiento y Prevención
- Puntos de fuga (PC, USB, CD, impresión, Web, correo, FTP, IM)

- El agente DLP se instalará en las PCs con acceso a Internet y equipos portátiles.
- Implementación de reglas de detección para los siguientes eventos:
  - Copia de documentos de ofimática a medios extraíbles.
  - Envío de documentos de ofimática usando el cliente de correo corporativo.
  - Cifrado de información sensible que se copia a medios extraíbles (USB, CD).
- Bloquear capturas de pantalla.
- Aplicación de políticas de DLP cuando el usuario se encuentra desconectado de la red corporativa (offline).
- Bloqueo de información sensible que se envía a imprimir sin autorización previa.
- Todas las acciones de prevención (Bloqueo, Notificación, Permite salida/Rechaza, Cuarentena, Permite salida basado en un código temporal) deben ser configurables en el sistema.
- Todos los incidentes deben generar registros en la consola de gestión y notificaciones vía correo al administrador o al equipo revisor.

A nivel de **Red**:

- DLP para Monitoreo/Prevención de Red (incluyendo Web y e-mail) (asociado al número de equipos/correos de la organización)
- Licencia de BD (en caso la solución requiera de BD para almacenamiento de incidentes u otros)
- Monitoreo de email corporativo, protocolos HTTP, HTTPS, FTP, SMTP, IM, P2P, y Correo Web (Yahoo Mail, Gmail, Hotmail, etc.).
- Identificación de fuga de información sensible vía:
    - Envío de correos con archivos adjuntos (.doc, .xls, otros) vía protocolo SMTP, HTTP, HTTPS.
    - Identificación de correos que contengan archivos cifrados (bloquear o permitir para usuarios de dominio autorizados).
    - Envío de información sensible vía protocolos de IM, o de protocolos inseguros como Telnet, FTP u otros.
    - Portales de almacenamiento virtual (Dropbox).
    - La sincronización del calendario corporativo y calendario de Gmail debe ser bloqueada.
- Acciones a tomar (parametrizables en la consola de gestión)
    - Bloqueo, Notificación, Permite/Rechaza salida, Cuarentena
    - Cifrado de correo

A nivel de **Almacenamiento**:

- DLP para Descubrimiento/ Prevención de Data en Reposo (asociado al número de usuarios del dominio corporativo)
- Integración con 1 base de datos Oracle 10g y 1 servidor de archivos.
- Implementación de reglas de monitoreo para la siguiente información:
    - Datos de clientes
    - Tarjetas de Crédito
    - Informes de Auditoría
    - Estados Financieros
    - Propiedad Intelectual

A nivel de la **Consola de Gestión**:

- Configuración de todos los módulos del DLP desde una única consola de administración
- Creación y Mantenimiento de Políticas desde una misma interface
- Los incidentes deben ser gestionados y reportados desde un servidor de administración centralizado

- El despliegue de los agentes debería ser ejecutado mediante la integración con herramientas de distribución de Software.
- Gestionar los agentes DLP desplegados desde el servidor de gestión central.
- Disponibilidad de tableros de mando que presenten información útil al administrador, tal como: últimos incidentes reportados, resumen de incidentes por severidad, tiempo, ubicación, por tipo de violación de seguridad, por protocolo, salud del sistema (sistema operativo, aplicación y base de datos).
- Administración de usuarios y accesos siguiendo el esquema RBAC.
- Conjunto de reportes predefinidos y herramientas para creación de reportes personalizados.

Integración con plataformas de terceros

- Integración con el Directorio Activo de Microsoft
- Integración con herramientas de filtrado de contenido vía el protocolo ICAP
- Integración con clientes de correo POP3

Adicionalmente, se requirieren los siguientes componentes y servicios:

- Cifrado de Correo: asociado al número de buzones de correo.
- Gateway de Correo: asociado al número de buzones de correo.
- Plan de Contingencia (Respaldo y Restauración de servicios DLP).
- Todas las notificaciones del sistema hacia el usuario final deben estar en idioma Español.

Arquitectura

El diagrama lógico de la solución implementada es el siguiente:

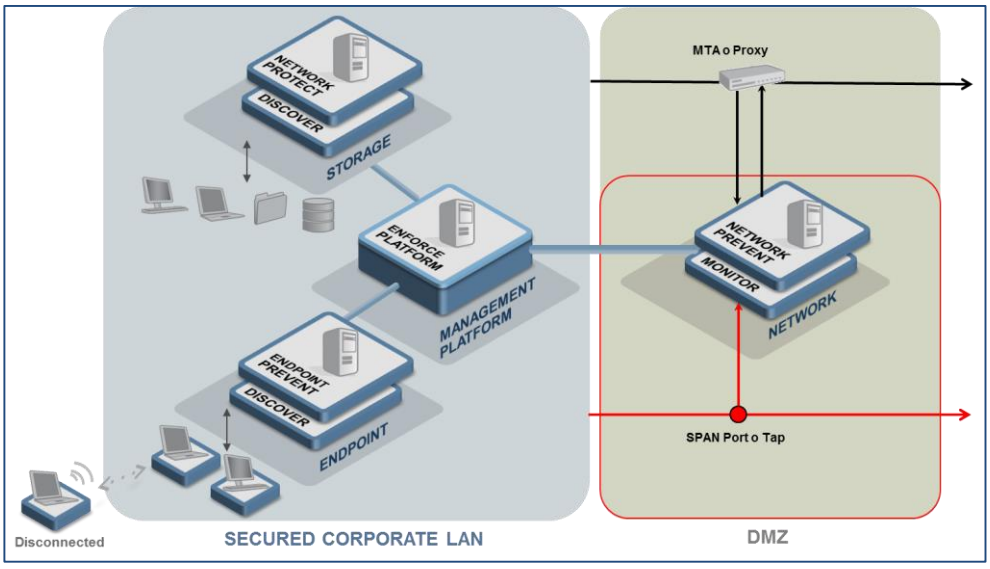

Figura 2.4. Diagrama Lógico de la Solución DLP.

El diagrama físico de la solución implementada es el siguiente:

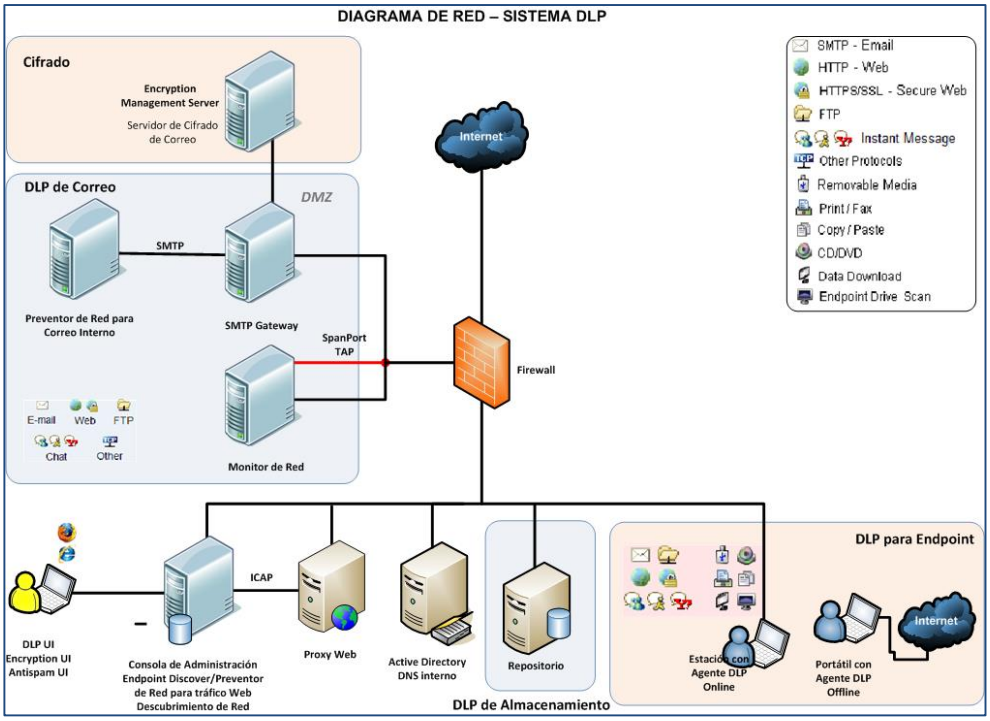

Figura 2.5. Diagrama Físico de la Solución DLP.

Hardware Requerido

- La solución a implementar debe soportar chasis del tipo Blade.
- Dada la no disponibilidad de configurar puertos SPAN en el switch core debe incluirse un dispositivo que replique el tráfico hacia los sensores del DLP.

- Debe considerar un equipo físico independiente (no virtual) a ser publicado en la DMZ de Internet para que los usuarios externos puedan leer los correos cifrados.
- Debe garantizarse la alta disponibilidad de los servicios.
- Los equipos deben contar con capacidades de tolerancia a fallas, de tal forma que la operación del servicio de correo corporativo y filtrado de contenido web no se vea interrumpida.

2.4.3 Hito 3: Proceso de Evaluación de las Soluciones DLP

A partir de la definición de las necesidades del negocio se realizó un plan de pruebas que sería evaluado por un comité interdisciplinario en el que se consideraron los siguientes aspectos clave:

- Creación de políticas
- Integración con el servicio de correo
- Gestión de incidentes
- Integración con el Directorio Activo, Filtrado de Navegación Web y Gateway de Correo
- Integración con repositorios de archivos y base de datos

- Funcionalidades a nivel del agente de endpoint (incluyendo aplicación de políticas mientras se encuentra offline).
- Visualización de incidentes por protocolo específico de red
- Acciones de Prevención/Bloqueo.

Se ejecutaron pruebas de concepto (PoC) para cada una de las soluciones evaluadas, realizándose con tres de ellas las pruebas con datos de producción en tiempo real.

El resultado de las PoC permitió al equipo evaluador conformado por las áreas de TI, financiera y de Seguridad Informática tener visibilidad de las fortalezas y debilidades de cada herramienta, así como sus ventajas y desventajas desde el punto de vista técnico y funcional.

El resultado de la evaluación se muestra en la tabla consolidada a continuación:

Sección	Calificación			
	DLP 1	DLP 2	DLP 3	DLP 4
DLP DE RED	19,38	18,00	17,50	20,00
DLP DE ALMACENAMIENTO	20,00	18,33	16,00	17,25
DLP DE ENDPOINT	28,00	31,25	30,00	29,50
ADMINISTRACION DE LA SOLUCION	1,50	4,50	9,50	8,50
INTEGRACION CON PLATAFORMAS DE TERCEROS	7,50	10,00	10,00	9,00
SUBTOTAL 1 - Requerimientos Técnicos	**19,38**	**18,00**	**17,50**	**20,00**
SUBTOTAL 2 - Servicios Profes, Calificaciones del Staff y de la Empresa, Propuesta detallada	**57,00**	**64,08**	**65,50**	**64,25**
TOTAL	**76,38**	**82,08**	**83,00**	**84,25**

Tabla 3. Proceso para elaboración de políticas de DLP.

2.4.4 Hito 4: Implementación

Para la implementación del proyecto se consideraron las siguientes macro-actividades:

a. Elaboración del Cronograma del Proyecto

- La duración del proyecto fue de 12 meses, sin incluir el proceso de evaluación las soluciones.

b. Kick-off del Proyecto

c. Preparación del entorno de TI (Hardware y comunicaciones)

- Instalación del Hardware
- Diagramas, capacidades, parametrizaciones

d. Instalación y configuración de la solución base (Software y requerimientos de integración)
    - El proveedor instalará y configurará la solución básica del sistema DLP considerando el alcance del proyecto (prevención y monitoreo de red).
    - Incluye creación de usuarios, integración con plataformas de correo/antispam, instalación de agentes en los endpoints definidos dentro del alcance del proyecto, integración con el AD para autenticación, endurecimiento de la plataforma.
    - Despliegue de los agentes DLP en las estaciones de trabajo y equipos portátiles de la empresa.

e. Implementación de Casos de Uso (Políticas DLP)
    - La información a proteger es definida por las áreas dueñas de la información.

- Creación de Diccionarios de palabras reservadas.
- Configuración de flujos de trabajo basados en roles y responsabilidades previamente definidos y de las acciones que se tomarán frente a un incidente: solo monitoreo, bloqueo, notificación y/o registro.

f. Creación de Cuentas de Acceso

- Se deberán crear cuentas para los responsables de la administración del sistema y de la gestión de resolución de incidentes reportados desde la herramienta DLP.
- Roles y Responsabilidades: delimitar y documentar los roles y responsabilidades del personal que se encargará de la revisión de las alertas de posible fuga de información. Los roles y perfiles de responsabilidad deberán contar con la aprobación de la gerencia o dirección correspondiente.

g. Pruebas

- Las pruebas incluirán los módulos implementados y considerados dentro del alcance del proyecto.
- Participarán las áreas de negocio y TI.

h. Transferencia de conocimientos

- Garantiza la transferencia completa de información a los administradores de la solución.
- Procedimientos de soporte, mantenimiento y actualización.

2.4.5 Hito 5: Capacitación

- Entrenamiento y Capacitación
  - Capacitación formal del fabricante para 6 personas en la Instalación, Configuración y Administración de la Solución.
  - Presentación del proceso de gestión de incidentes a los responsables de su análisis y resolución (flujo de revisión de las alertas).

- Plan de comunicación, Difusión
    - Informar la metodología de protección de información sensible a las áreas.

2.4.6 Hito 6: Puesta en Producción

- Se declarará al sistema en producción (incluyendo todos los módulos implementados y considerados dentro del alcance del proyecto).
- Acta de Entrega/Recepción

2.5 Operación

- Acompañamiento y Afinamiento de la Solución
    - Garantiza que el diseño, el tamaño y la configuración de la solución estén optimizados

- Gestión de Incidentes
  - Para analizar la causa raíz de un incidente de fuga de información se utiliza el flujo de trabajo [4] esquematizado en la Figura 2.6, este flujo actualmente se lleva de forma manual y las comunicaciones se efectúan vía correo electrónico.

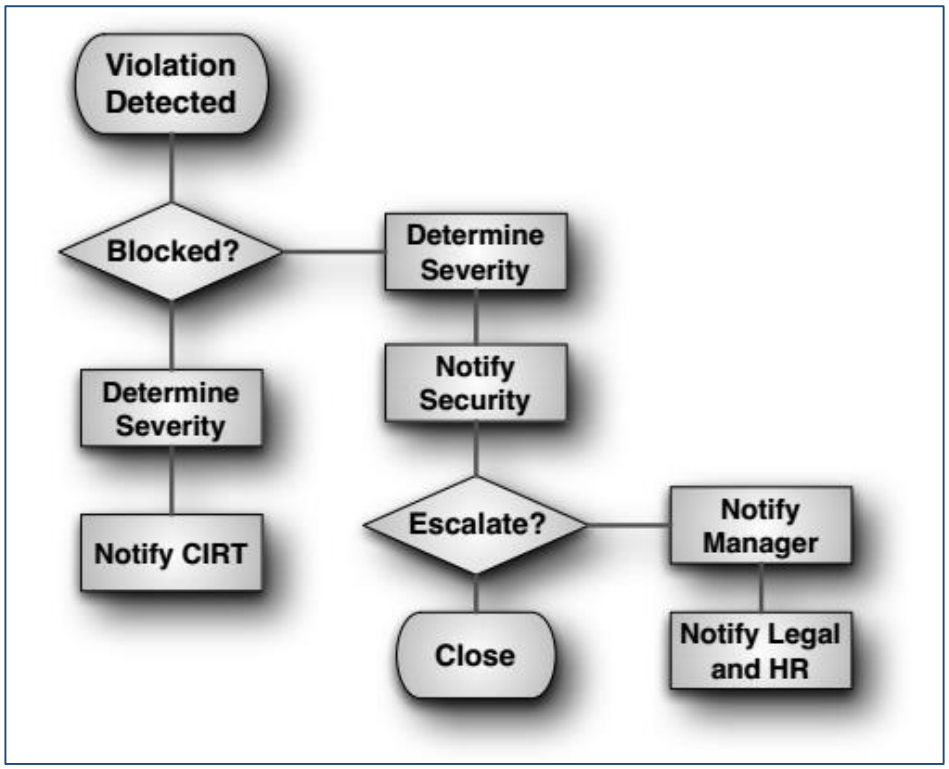

Figura 2.6. Flujo de atención de Incidentes de Fuga de Información.

2.6 Soporte y Mantenimiento

La empresa requirió que se incorpore soporte y mantenimiento con el fabricante y con el proveedor local por 1 año contado a partir de la fecha de puesta en producción oficial de la solución.

Las características de este servicio son las siguientes:

- Servicios de actualización para todas las versiones nuevas.
- Migración a nuevas versiones y prueba de políticas.
- Revisiones técnicas y empresariales trimestrales.
- Comprobaciones del uso óptimo del sistema DLP.

CAPÍTULO 3

RESULTADOS OBTENIDOS

Este capítulo se orienta al análisis de datos poniendo de manifiesto cómo el sistema DLP ayuda en la identificación de incidentes de posible fuga de información.

3.1 Identificación de brechas de seguridad

El DLP luego de su implementación ha proporcionado una plataforma de gestión de datos empresariales sensibles dándole visibilidad a la organización en torno a aspectos que pudieran provocar incidentes de fuga de información, tales como:

- Identificación de debilidades a nivel de infraestructura de la red
- Identificación de la ubicación de datos sensibles (repositorios locales o de red) y cómo son manipulados y quiénes tienen acceso a estos.
- Mejoras en la asignación de roles de acceso a la data sensible.
- Categorización de la data sensible de tal forma que pueda ser incorporada en nuevas políticas de DLP.
- Identificación de procesos operativos que pudieren ocasionar pérdida accidental de información confidencial a través del correo corporativo o pérdida incidental a través del correo web personal.
- Identificación del uso no autorizado de servicios o aplicaciones (tales como: IM, P2P, FTP, redes sociales), o de uso autorizado de estos servicios, para enviar información sensible.
- Registro de las actividades de los usuarios de equipos portátiles una vez que el equipo es desconectado de la red corporativa.
- Elaboración y/o mejora de políticas y procedimientos de protección de datos empresariales sensibles.

3.2 Análisis de la problemática de fuga de información resuelta por el DLP

Producto del monitoreo de incidentes de fuga de información sensible y en base a los casos de uso implementados encontramos a nivel de:

- Data en Reposo: se ejecutó el escaneo de información sensible en el servidor de archivos corporativo y se estableció que existían debilidades en cuanto a los permisos de seguridad asignados a cada usuario/grupo. Se regularizaron los permisos de acceso a los recursos compartidos solo a aquellos usuarios quienes lo necesitaban.

- Data en Uso: a partir de los registros entregados por los agentes DLP desplegados en los equipos sensibles de la organización, se ha creado conciencia entre los colaboradores del uso responsable que debe darse a la información sensible a la cual tiene acceso en función de su cargo de responsabilidad.

- Data en Movimiento: ha sido posible identificar data sensible que es transmitida a nivel de protocolos de red tales como SMTP, FTP, IM, HTTP/S, etc., incluyendo datos del remitente, destinatario, contenido y otros detalles.

3.3 Estadísticas de Incidentes

A nivel de **Red**: con el DLP se dispone de una herramienta efectiva para el control de riesgos de los datos que viajan por la red corporativa.

- Período de análisis: 80 días de monitoreo de la red
- Tráfico analizado: más de 2370.14 GB, 0 paquetes perdidos
- Incidentes generados: más de 487 millones de mensajes analizados generaron más de 751 mil incidentes, la mayor parte de baja severidad considerando que es necesario trabajar en el afinamiento de las políticas DLP para reducir el número de incidentes a analizar.
- Archivos cifrados transmitidos: 3.517 adjuntos cifrados

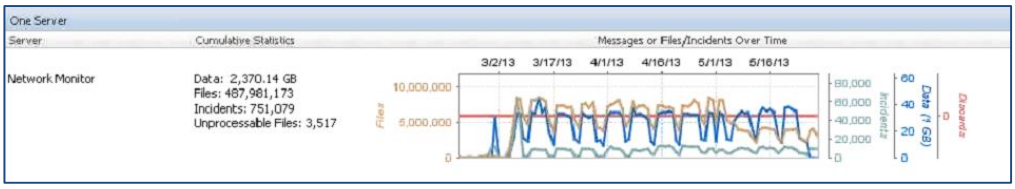

Figura 2.7. Datos del monitoreo de red.

A nivel de **Data en reposo**:

- Carpetas con permisos asignados incorrectamente: 15 carpetas en el servidor de archivos corporativos
- Información de cuentas VIP: se identificó 194.003 incidentes relacionados con información de cuentas corporativas transmitidas por correo sin las protecciones respectivas. Este tipo de detecciones permite a la organización fortalecer sus procesos operativos.

A nivel de **Endpoint**:

- Información no cifrada enviada por correo o copiada a un USB: se detectaron 4.358 eventos en los cuales se encontró referencias a diagramas de infraestructura de red, guías comerciales, manuales de procedimientos, entre otros.

En la Figura 2.8 se muestran varios de los incidentes categorizados:

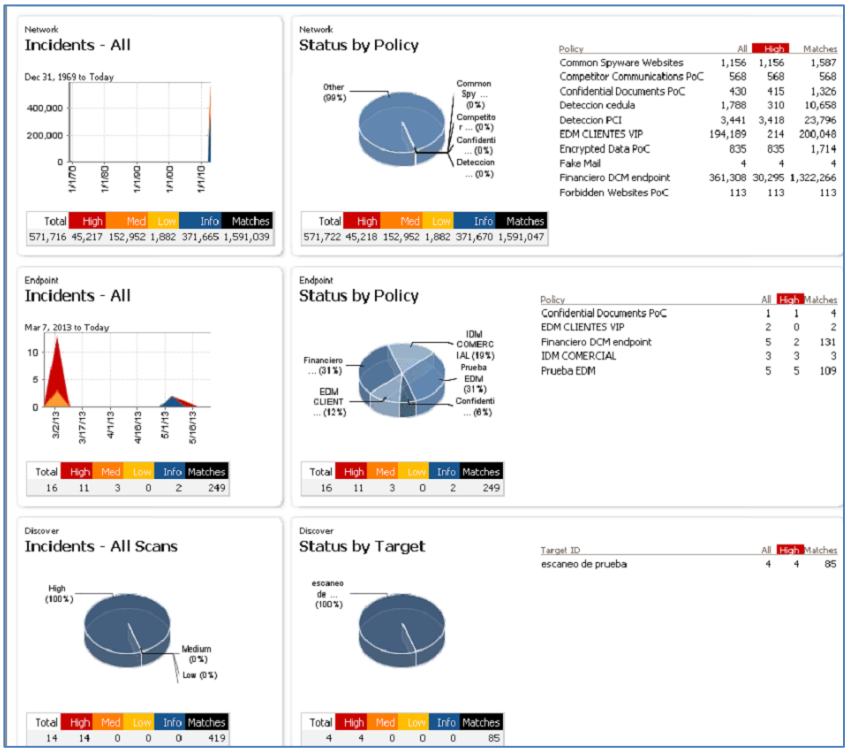

Figura 2.8. Tablero de Control que muestra los incidentes categorizados.

Nota: Es importante mencionar que dado lo sensible de la información anteriormente mencionada los datos estadísticos presentados son meramente demostrativos.

3.4 Mejoras en los procedimientos de gestión de incidentes

Como se aprecia en la Figura 2.9, el modelo de gestión de incidentes usado por la organización para la reducción del riesgo asociado con fuga de información sensible inicia con una primera fase de monitoreo, para luego elaborar las reglas de detección y tomar acciones de

bloqueo o de mejoras en los procesos internos, y este último sobre el cual se debe emprender en una campaña de concientización de todos los colaboradores dado que varios de los vectores de fuga de información pueden ser resueltos teniendo en cuenta simples medidas de seguridad, tales como:

- Evitar dejar documentos impresos en impresoras compartidas
- Sensibilizarse de que la seguridad de la organización es una problemática común que debe ser atendida en sus procesos operativos
- Cumplir con las políticas internas, que incluyen mantener prácticas de escritorio despejado y guardar la documentación sensible bajo su custodio bajo llave.

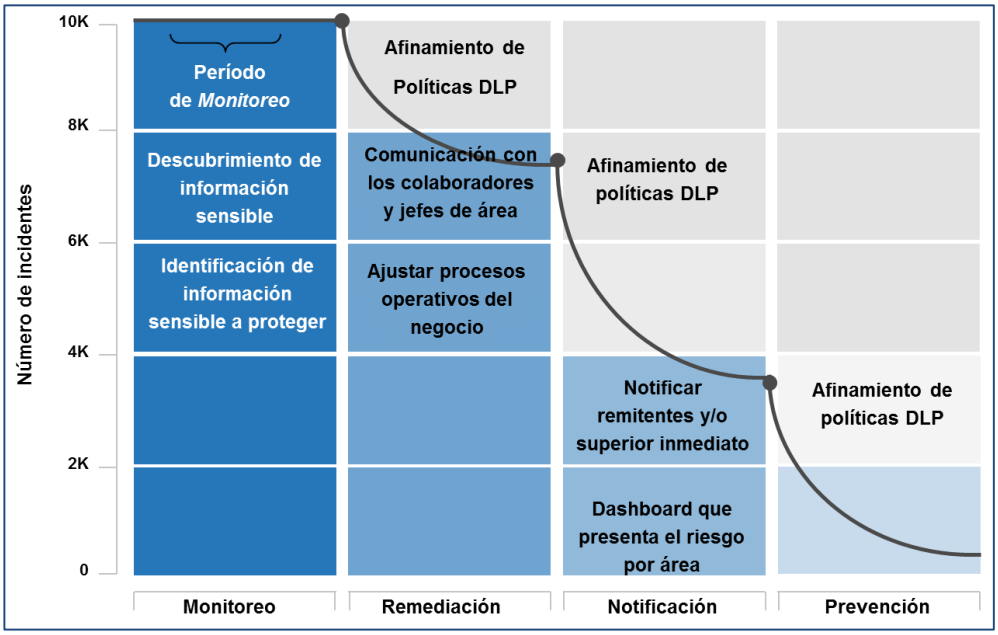

Figura 2.9. Fases para la reducción del riesgo.

3.5 Limitaciones del DLP

- Las herramientas DLP solo pueden monitorear el tráfico cifrado cuando tienen acceso a los certificados usados para el cifrado de esta información (ej.: este es el caso del tráfico web que es autorizado a nivel del proxy de navegación).

- Las soluciones DLP que solo disponen del módulo de monitoreo de red están limitadas a las posibilidades de detección que ofrece este componente (por ejemplo no podrían detectar data sensible que viaje vía un protocolo tunelizado), es por este motivo que se vuelve necesario contar con un agente a nivel del endpoint, el cual está en capacidad de detectar la manipulación de información sensible previo a que sea enviada por la red.

- Finalmente, es importante mencionar que las soluciones DLP están en proceso de maduración constante, por lo que lo que se busca al implementar este tipo de herramientas es reducir la superficie de exposición de la información sensible.

CONCLUSIONES

1. El entendimiento cabal de los procesos operativos de manipulación de la información sensible permite que el sistema DLP oriente su detección y acciones de prevención a incidentes de fuga de información reales.

2. La solución DLP ayudó a la organización en la implementación de un marco de trabajo práctico y eficiente en cuanto a:

a. Descubrimiento de información sensible
b. Protección de la información sensible
c. Implementación de nuevas políticas DLP y afinamiento de las políticas DLP existentes en base al conocimiento alcanzado de los flujos de información propios de la operativa del negocio producto del monitoreo constante de comportamientos anómalos o sospechosos de los usuarios permitiendo así minimizar los falsos positivos.

3. A pesar de que la solución DLP tiene el carácter preventivo esto no siempre es posible, por lo que es necesario avanzar el entendimiento de los procesos del negocio e ir madurando los procedimientos internos y la concientización de los usuarios del uso dado a la información sensible, para finalmente emprender en acciones restrictivas reduciendo la posibilidad de afectaciones a la operativa de los procesos del negocio.

4. Una vez implementada la solución fue visible para la organización la cobertura dada a las brechas de seguridad relativas a fugas de información a nivel de los tres componentes del DLP:
    a. Data en Movimiento: permitió tener visibilidad del tráfico que salía de la red corporativa vía los protocolos HTTP, HTTPS, FTP, Telnet, IMAP, SMTP, etc.
    b. Data en Reposo: se identificó data sensible de recursos de red compartidos no asegurados apropiadamente, así como también se identificó data cifrada con diversos esquemas de cifrado por lo que se deberá trabajar con el área de TI en un esquema de cifrado único para la organización.
    c. Data en Uso: se registró que información sensible era copiada a medios extraíbles o impresa sin previa autorización.

5. La selección de la tecnología de prevención de fuga de información debe ser realizada desde la perspectiva de las necesidades del negocio en lugar de ser escogida en base a los requerimientos del equipo de seguridades de TI.

6. Finalmente, los procedimientos de protección de la información y de detección de fuga de información deben formar parte de un proceso de continuo afinamiento y actualización sin perder de vista lo realmente importante… Proteger la Información Sensible de la Organización.

RECOMENDACIONES

1. Sea realista en el alcance de la solución propuesta para su organización, priorice los aspectos más críticos que el negocio requiere proteger; conforme los usuarios y los procesos operativos se vayan adecuando al nuevo esquema de protección de la información se podrá ampliar el alcance y aplicar acciones automáticas de prevención.

2. Defina los siguientes elementos que permitan alcanzar el éxito del proyecto y mantenerlo efectivo durante su operación:
    - Responsables de la revisión de los posibles incidentes de seguridad detectados por la solución DLP y actualice los controles de protección implementados en la herramienta.
    - Lista de documentos sensibles, identifíquelos con una marca única o etiqueta (ej.: SENS_NombreArchivo, incorporar un atributo en la metadata del archivo, incluir una marca en el encabezado o pie del documento), de tal forma que las reglas de detección puedan operar eficientemente. También ayudaría disponer de un repositorio único de información digital sensible, sobre el cual adoptar las medidas de protección que fueren necesarias.

3. Diseñe planes de capacitación y concientización dirigido a:
    - Todos los empleados relativo a la protección de la información que la empresa ha definido como sensible.
    - Los dueños de la información, quienes deberán impulsar la adopción de buenas prácticas de seguridad de protección de información.

4. Es importante que la organización disponga de políticas de gobernabilidad, cumplimiento y riesgo en relación a la protección de su información sensible de tal forma que estas reglas del negocio sean los lineamientos sobre los que se construyan las políticas de detección en la herramienta DLP.

5. Al implementar una solución DLP, siempre deberá considerar los siguientes factores: compatibilidad con sistemas operativos y endpoints (estaciones de trabajo, portátiles y dispositivos móviles) de la organización, la experiencia del equipo de trabajo que realizará la implementación, así como también los acuerdos de niveles de servicio y el personal que dará soporte al sistema en producción.

6. Para lograr examinar el contenido cifrado que es enviado fuera de la organización es imprescindible contar con un sistema de cifrado corporativo para satisfacer la necesidad interna en cuanto a la protección de la data que se comparte con terceras partes o asociados del negocio.

Cualquier otro esquema de cifrado de información debe ser prohibido y la transferencia de esta información debe ser bloqueada por el DLP.

BIBLIOGRAFÍA

[1] G. Torsten, «Security Week,» 4 Febrero 2015. [En línea]. Available: http://www.securityweek.com/data-integrity-core-security. [Último acceso: 15 Marzo 2015].

[2] Trend Micro, «Trend Micro,» Enero 2008. [En línea]. Available: http://es.trendmicro.com/imperia/md/content/es/whitepaper/wp01_leakproof_080123es.pdf. [Último acceso: 10 Marzo 2015].

[3] «IRS,» 15 Enero 2015. [En línea]. Available: http://www.irs.gov/uac/Preventing-Data-Leakage-Safeguards-Technical-Assistance. [Último acceso: 13 Abril 2015].

[4] R. Mogull, «Securosis, L.L.C,» [En línea]. Available: https://securosis.com/assets/library/reports/DLP-Whitepaper.pdf. [Último acceso: 27 Septiembre 2013].

[5] «Segu-Info,» 23 Junio 2011. [En línea]. Available: http://seguinfo.blogspot.com/2011/06/informe-de-dlp-prevencion-de-fuga-de.html?utm_source=feedblitz&utm_medium=FeedBlitzEmail&utm_campaign=Nightly_%272011-06-27+00%3A30%3A00%27&utm_content=32516. [Último acceso: 20 Febrero 2015].

GLOSARIO

Antispam: El antispam es lo que se conoce como método para prevenir el correo basura. Son sistemas informáticos que impiden la entrada/salida de correo no deseado y ataques de suplantación de identidad que llega a las bandejas de entrada de los correos corporativos o personales.

Endpoint: infraestructura de TI que incluye terminales, estaciones de trabajo, equipos portátiles, servidores de archivos, dispositivos móviles (teléfonos inteligentes y tabletas), entre otros.

APÉNDICES

Apéndice A: Motivos principales de Incidentes de Fuga de Información

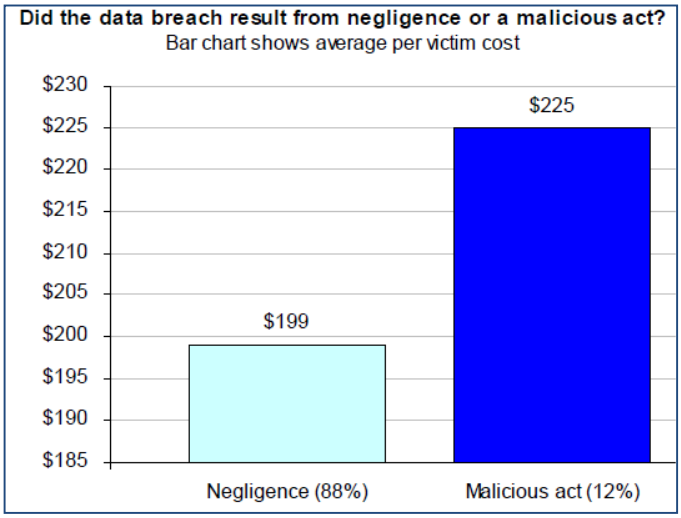

Figura A.1. Motivos principales de Incidentes de Fuga de Información.

Fuente: Segu-Info [5]

Apéndice B: Protecciones a nivel del Endpoint (Data en Uso)

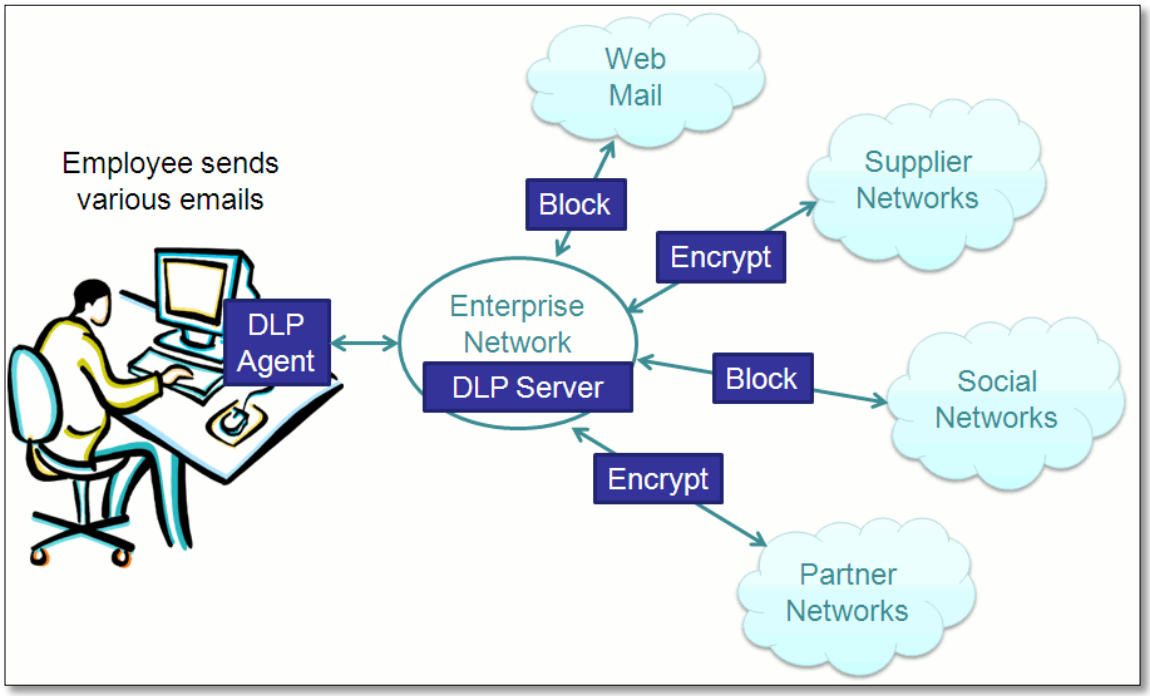

Figura B.1. Protecciones DLP a nivel del Endpoint.

Apéndice C: Ejemplos prácticos de uso del DLP

ACCION	ANALISIS DLP	RESULTADOS
Pedro empleado de una empresa de comercialización, está trabajando en un informe de ventas en su PC de la oficina, dado que no lo ha terminado lo intenta enviar a su cuenta de Yahoo para continuar desde su casa.	Aunque el acceso al correo web está permitido para Pedro, el DLP reconoce que se trata de información confidencial por lo que no debe ser enviado por correo electrónico fuera de la empresa a menos que se encuentre autorizado.	Se bloquea el envío del informe a la cuenta de Yahoo y Pedro es notificado automáticamente de que esta acción no está permitida según se establece en la polítca de seguridad corporativa. Estas acciones quedan registradas en el log del sistema.
Luis quiere usar como ejemplo para su presentación de la universidad un documento de la empresa para la que trabaja por lo que intenta imprimirla en la impresora de la oficina.	El sistema DLP reconoce que Luis está intentando imprimir un documento que es confidencial y evita que se imprima.	Luis recibe una notificación de que lo que está intentando realizar va en contra de la política de seguridad de la compañía, esto es que está prohibido imprimir documentos sensibles sin contar con una autorización previa.

Tabla 4. Casos de Uso de Políticas DLP.

Apéndice D: Estudio de Causas de Fuga de Datos

El estudio presentado a continuación fue realizado por las empresas Ponemon y Symantec señala que los errores humanos y de sistemas informáticos causan la mayoría de incidentes de fuga de información. Indica además que los ataques criminales y maliciosos son los más costosos en todo el mundo.

MOUNTAIN VIEW, California – 5 de junio de 2013 – Symantec Corp. (Nasdaq: SYMC) y Ponemon Institute dieron a conocer hoy el Estudio sobre el Costo de las Fugas de Datos 2013, el cual que indica que los errores humanos y los problemas en los sistemas causaron dos terceras partes de las fugas de datos en 2012 e incrementaron la media a nivel mundial hasta $136 dólares por registro. Esto incluye el manejo no apropiado de los datos confidenciales por parte de los empleados, la falta de controles en los sistemas y la infracción de las regulaciones industriales y gubernamentales. A nivel global, los sectores con fuertes regulaciones – como el financiero, farmacéutico y el de salud – sufrieron costos por fugas de datos 70 por ciento más altos que los de otros sectores.

El costo mundial por cada registro de cliente comprometido fue superior a lo observado el año pasado y el costo total por fuga de datos en Estados Unidos se redujo ligeramente a US$5.4 millones de dólares. Esta reducción se atribuyó al nombramiento de Directores de Seguridad de la Información (CISOs por sus siglas en inglés), quienes tienen responsabilidad en toda la empresa de diversas tareas como la puesta en marcha de planes completos de respuesta ante incidentes y programas generales de seguridad más sólidos.

“Los atacantes externos y la constante evolución de sus métodos y acciones representan una gran amenaza para las compañías, pero los peligros asociados con las amenazas internas pueden ser igualmente destructivos y traicioneros. Ocho años de estudio sobre las fugas de datos nos han mostrado que el comportamiento de los empleados es uno de los problemas que más afectan a las organizaciones actualmente, esto se ha incrementado en 22% desde el primer estudio que hicimos”, señaló Larry Ponemon, Presidente de Ponemon Institute.

“Debido a que las organizaciones con fuertes posturas sobre seguridad y planes de respuesta ante incidencias han sufrido costos por fugas de datos 20 por ciento menores a los de otras compañías, resulta evidente la importancia que tiene contar con un enfoque holístico bien coordinado y completo. Las compañías deben proteger la información confidencial de sus clientes, independientemente de donde esté guardada, ya sea en una PC, un dispositivo móvil, una red corporativa o centro de datos”, comenta Anil Chakravarthy, Vicepresidente Ejecutivo del Grupo de Seguridad de la Información en Symantec.

El octavo informe global anual del Instituto Ponemon y Symantec está basado en experiencias sobre fugas de datos de 277 compañías en nueve países: Estados Unidos, Reino Unido, Francia, Alemania, Italia, India, Japón, Australia y Brasil. Los informes de los nueve países y el informe mundial se pueden encontrar aquí. Todas las incidencias de fugas de datos estudiadas en el informe ocurrieron en el año 2012. Para realizar un seguimiento adecuado de los datos sobre la tendencia, el Instituto Ponemon no incluye los incidentes conocidos como “mega fugas de datos” con más de 100,000 registros en peligro.

Las compañías pueden analizar sus propios riesgos visitando la calculadora de Symantec sobre riesgo de fugas de datos en databreachcalculator.com la cual toma en cuenta el tamaño, sector, ubicación y las prácticas en seguridad de una organización para estimar el riesgo, tanto a nivel por registro y de toda la organización.

Entre los hallazgos principales del estudio están las siguientes:

- **El costo promedio por fuga de datos varía ampliamente en todo el mundo.**

  Muchas de estas diferencias son debidas a los tipos de amenazas que afectan a las organizaciones, además de las leyes de protección de datos en los respectivos países. Algunos países como Alemania, Australia, Reino Unido y Estados Unidos tienen leyes y normativas más establecidas para la protección del consumidor con el objetivo de fortalecer la seguridad informática y la privacidad de los datos. Estados Unidos y Alemania continúan experimentando las fugas de datos más costosas (con un costo promedio por registro comprometido entre US$188 y US$199 dólares, respectivamente). Estos dos países también tuvieron los mayores costos totales por fuga de datos (US$5.4 millones de dólares en Estados Unidos y $4.8 millones de dólares en Alemania).

- **Los errores de las personas y aquellos en los sistemas son las causas principales de las fugas de datos.**

  Juntos, los errores humanos y los problemas de los sistemas representaron el 64% de las fugas de datos en el estudio mundial, cabe mencionar que el estudio anterior indicó que 62% de los empleados pensaba que era aceptable transferir datos corporativos fuera de la compañía y que la mayoría nunca borraba los datos, siendo vulnerables a posibles fugas. Esto muestra el gran impacto que pueden tener los empleados en las fugas de datos y el alto precio que pueden tener estos incidentes para las organizaciones. De acuerdo con el estudio, las compañías brasileñas son las que tienen mayor probabilidad de sufrir fugas de datos debido a errores humanos. Las compañías de la India son las que tienen mayor probabilidad de sufrir fugas de datos por problemas en sistemas o por fallas en procesos del negocio. Entre los problemas de los sistemas se incluyen las fallas de aplicaciones, vaciados de datos de forma involuntaria, errores lógicos en transferencia de datos, fallas de identidad o de autenticación (acceso incorrecto), errores de recuperación de datos, entre otros.

- **Los ataques criminales y maliciosos son los más caros a nivel global.**

  Las conclusiones del informe indican que los ataques maliciosos o con fines criminales causan el 37% de las fugas de datos y son los incidentes más costosos de este tipo en los nueve países participantes en el estudio. Las compañías de Estados Unidos y las alemanas sufren los incidentes de fugas de datos más caros debido a las acciones de atacantes maliciosos, y cada registro comprometido tiene un valor de entre US$277 y US$214 dólares respectivamente. Brasil e India registraron las fugas de datos menos costosas, con US$71 y US$46 dólares por registro, respectivamente. Las compañías alemanas fueron también las que, con mayor frecuencia, sufrieron un ataque malicioso o delictivo, seguidas de las de Australia y Japón.

- **Algunos factores organizacionales disminuyen los costos.**

  Las compañías de Estados Unidos y Reino Unido recibieron las mayores reducciones en costos asociados con fugas de datos gracias a su fuerte posición en seguridad, a los planes para respuesta ante incidentes y al nombramiento de un CISO o encargado de seguridad. Por su parte,

Francia y Estados Unidos redujeron también sus costos gracias al empleo de asesores para encontrar soluciones a las fugas de datos.

Apéndice E: Calculadora de Riesgos

https://databreachcalculator.com/

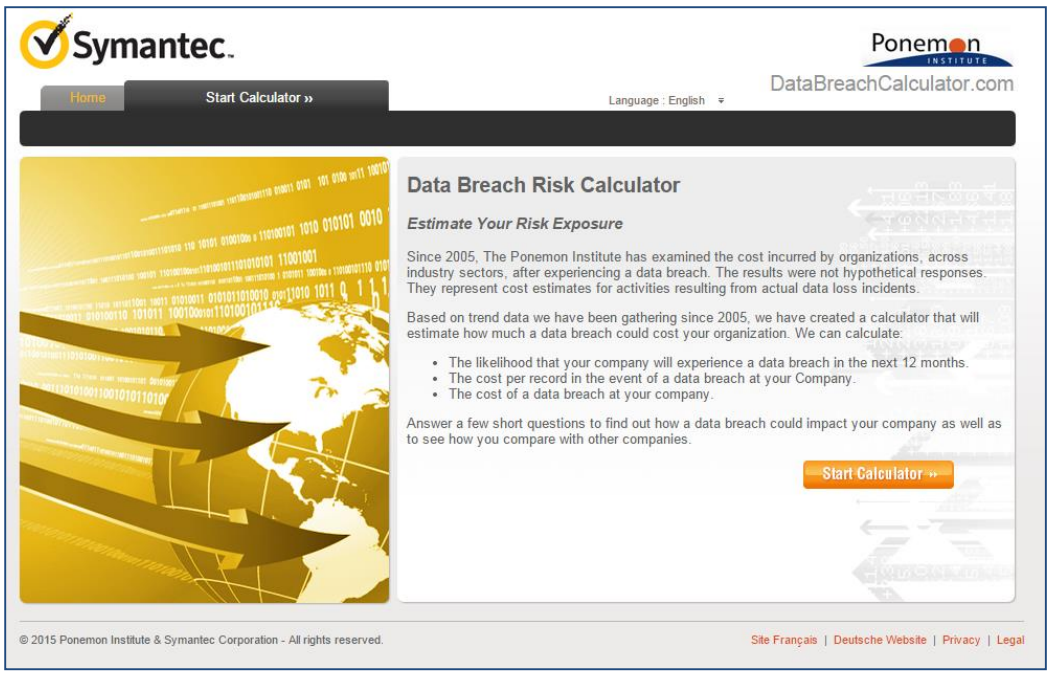

Figura E.1. Calculadora de Riesgos (Inicio)

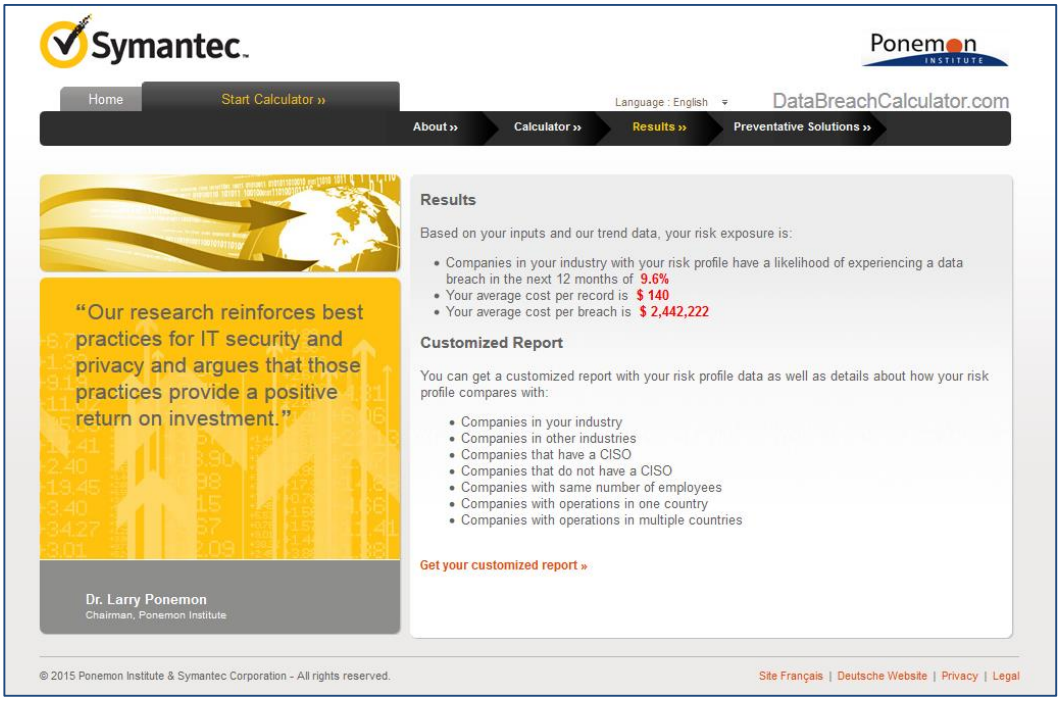

Figura E.2. Calculadora de Riesgos (Resultado)

Apéndice F: Niveles de Riesgo

En el gráfico a continuación puede visualizarse el riesgo identificado para cada uno de los activos de TI en los cuales se encuentra la información, de esta manera se pueden enfocar los esfuerzos para llevar adelante reglas de detección y prevención en función del impacto que tendría en la organización.

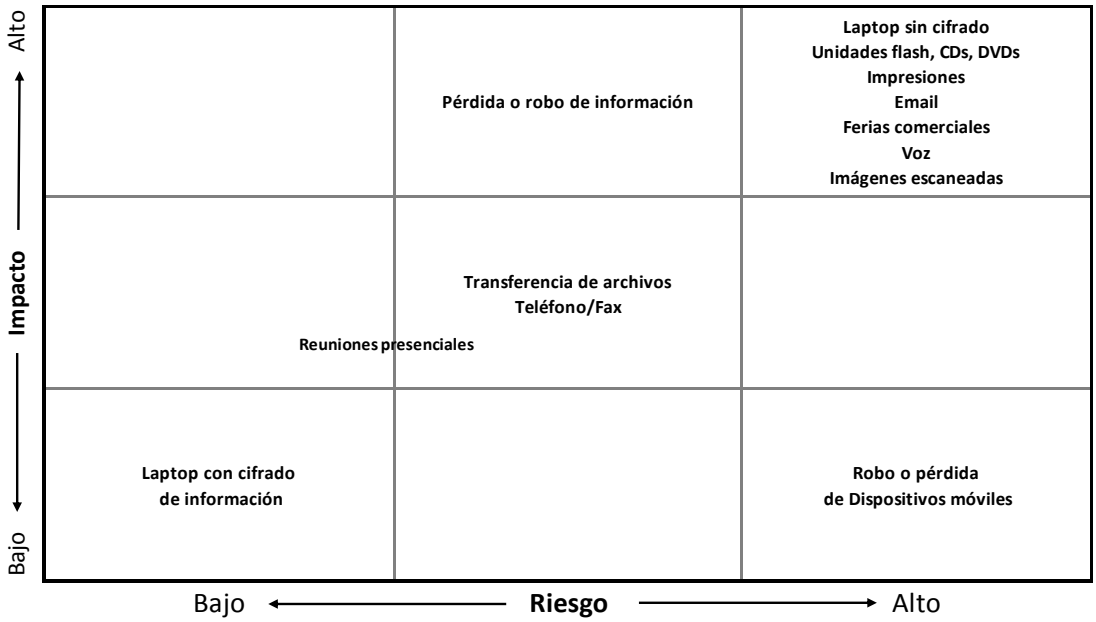

Figura F.1. Nivel de Riesgo en eventos de fuga de información.