ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"SOLUCIÓN DE CONTROL DE FUGA DE INFORMACIÓN CONFIDENCIAL SALIENTE (DATA LOST PREVENTIÓN) A TRAVÉS DE NAVEGACIÓN WEB, CORREO ELECTRÓNICO Y ESTACIONES MÓVILES"

EXAMEN DE GRADO (COMPLEXIVO)

Previo a la obtención del Título de:

LICENCIADO EN SISTEMAS DE INFORMACIÓN

MANUEL AGUSTÍN VACA COJITAMBO

GUAYAQUIL – ECUADOR

AÑO: 2016

TRIBUNAL DE EVALUACIÓN

MSIG. Ronny Santana	**MSIG. Marjorie Chalén**
PROFESOR EVALUADOR	PROFESOR EVALUADOR

DECLARACIÓN EXPRESA

"La responsabilidad y la autoría del contenido de este Trabajo de Titulación, me corresponde exclusivamente; y doy mi consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"

.....

Manuel Agustín Vaca Cojitambo

RESUMEN

En la actualidad en el mundo de los negocios, muchas organizaciones utilizan sistemas de información para gestionar su información crítica, sensible y de negocio. La necesidad de proteger un componente tan esencial de la organización como son sus activos de información no puede ser subestimada. Se ha creado el concepto y herramientas de Data Loss/Leakage Prevention [1] para ser una de las maneras eficaces en prevención de pérdida de datos en las organizaciones.

Los directivos de LHENRIQUES S.A, una compañía que importa y distribuye suministros industriales, sospechaban que algunos de sus empleados venían incurriendo en prácticas desleales proporcionando información importante a la competencia. Para mitigar esta brecha de seguridad, la empresa se decidió adquirir un completo sistema de Detección de Perdida de Información (DLP Data Loss/Leakage Prevention [1]), para proteger la información de clientes, planes de ventas, proyecciones y demás información de propiedad exclusiva de la organización. Para lograrlo adquieren Websense Triton Enterprise [3], que consiste en una suite de varios productos para proteger la fuga de información por los canales Web, Email, Teléfonos Móviles y estaciones de trabajo; se aprovechan las bondades del producto para elevar el nivel de seguridad en la navegación web, ingreso y salida de correo de la organización.

La instalación del producto de DLP, la identificación de activos a proteger y la creación de políticas dentro de la herramienta permitieron tener una infraestructura protegida contra fuga de información. Mediante la generación de reportes y alertas en el sistema sobre intentos de fuga de información; los directivos de la empresa pueden evidenciar el monitoreo, seguimiento y control de los intercambios de información.

ÍNDICE GENERAL

CAPÍTULO 1

1. DESCRIPCIÓN DEL PROBLEMA

Las organizaciones actuales enfrentan el desafío de protegerse contra amenazas de seguridad web, seguridad de correo electrónico y prevención de perdida de datos (DLP [1]). Además, proporcionar un acceso racional a los servicios de Internet, procurando el uso de este recurso para actividades que contribuyan a la eficacia, la eficiencia laboral y sin exponer los recursos informáticos empresariales a sitios web con virus o con software malicioso.

La intención de los delincuentes de robar datos y convertir los resultados en dinero, los lleva a desarrollar enfoques ingeniosos para eludir las defensas; una técnica efectiva que utilizan los delincuentes informáticos sofisticados es robar datos lentamente, en incrementos aparentemente inocentes que no activan ningún umbral de detección. Otra técnica son las campañas de correo electrónico de phishing [2] dirigidas a un grupo o todos los usuarios de una organización, este es uno de los ataques más difíciles de detener; los delincuentes saben que un gateway de correo electrónico examinará la URL agresora; por tal, deciden enviar sus ataques durante un fin de semana porque saben que existe un retardo de tiempo entre el momento en que el usuario recibe el mensaje y el momento en que hace clic en un enlace dentro de un mensaje. También, confían en el hecho de que la mayoría de los Gateway de correo electrónico examinan la URL una vez y luego envían el mensaje al destinatario; por esta razón, usan un dominio seguro y confiable en su señuelo de phishing [2] y lo convierten en un enlace malicioso una vez que están seguros de que el escaneo de seguridad inicial ha terminado.

LHENRIQUES S.A, se encontraba expuesta a la pérdida o robo de información sensible de la empresa y sospechaban de fuga de información comercial hacia la competencia. Por lo tanto, se fijaron la búsqueda de una solución integral para control de perdida de información y control de amenazas. Previo a la obtención de la solución, la empresa no tenía una visión clara de cuantos activos de información estaban fugando fuera de la institución por los diferentes canales: Web, Email, medios

extraíbles, impresiones, etc. La herramienta adquirida. debía tener la capacidad de realizar descubrimientos y generar reportes de toda la información que haya generado incidentes DLP.

La solución requerida debía proteger contra amenazas de Internet y fuga de información tanto a los usuarios locales como remotos o móviles (vendedores). Además, la administración debía agrupar de todos los vectores de fuga de información [1] en una sola consola unificada. Para este efecto decidieron adquirir la solución Websense Triton Enterprise [3]; con esta adquisición obtuvieron una solución que permite aplicar las mismas políticas a todos los vectores de fuga, permite también tener de manera unificada visibilidad de violaciones a estas políticas.

CAPÍTULO 2

2. SOLUCIÓN TECNOLÓGICA PROPUESTA

Luego de un análisis de la infraestructura de la organización e identificar las necesidades de protección Web, Email y como pilar fundamental el control de fuga de información, se propone un diseño de ingeniería que contenía los siguientes elementos:

- Un appliance Websense v5000 [4] g2 para control de contenido Web.
- Un appliance Websense v5000 [4] g2 para control de correo electrónico.
- Una consola de administración.
- Un servidor de bases de datos y administración de Logs.
- Un appliance virtual para análisis de ActiveSync [5].
- Agentes de software para control de fuga de información en las estaciones de trabajo.

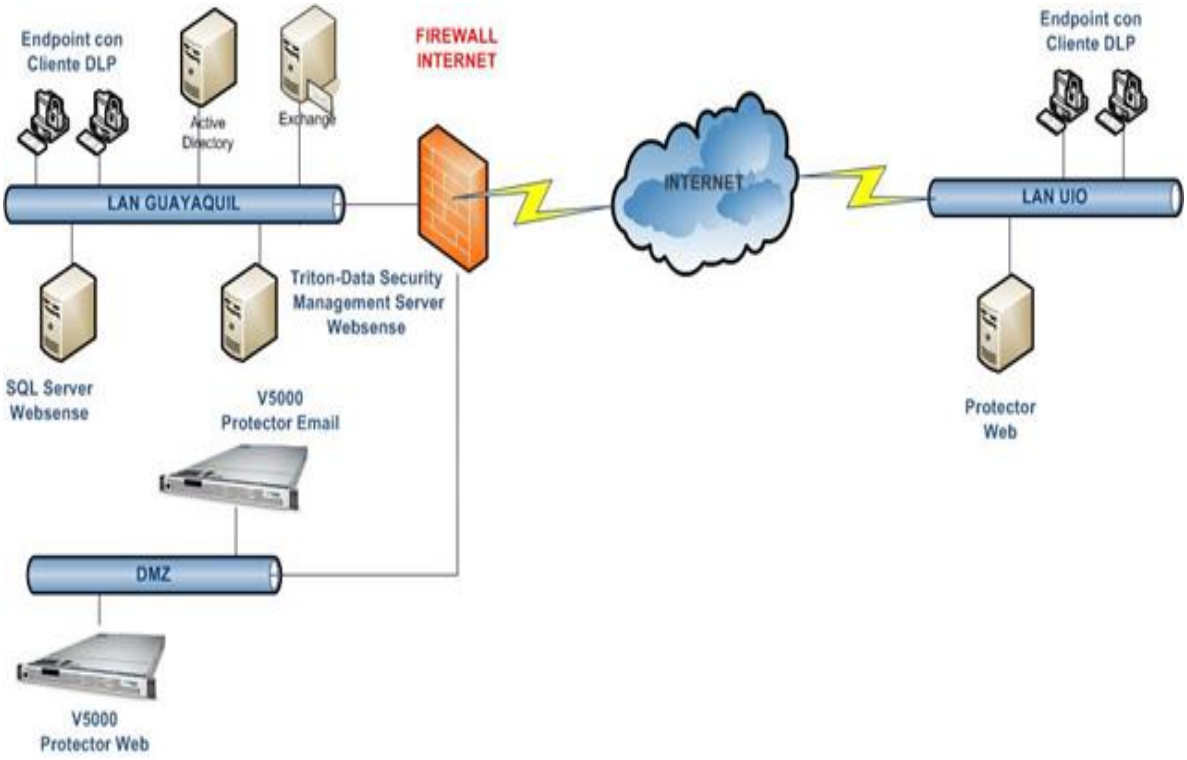

Figura 2.1: Diagrama de diseño propuesto

El diseño propuesto expuesto en la figura 2.1 consideró la infraestructura existente de la empresa, es decir su firewall y demás elementos de red que poseían.

Basado en experiencias previas y la utilización de Websense en implementaciones de control de fuga de información, se logró documentar una metodología para implementación proyectos de control de fuga de información; este procedimiento se lo describe en el punto 2.1.4.

2.1. Descripción detallada de la solución propuesta:

2.2. Seguridad Web

El desafío de LHENRIQUES S.A fue proveer a los usuarios del servicio de Internet un acceso que garantice el uso seguro y racional del Internet filtrando por categoría de sitios improductivos como de muestra en la figura 2.2 y 2.3, controlando el uso de las redes sociales, sitios de videos a los cuales acceden los usuarios y previniendo que estos sean afectados por sitios comprometidos con tráfico malicioso.

El filtrado Web fue implementado con Websense Web Security Gateway en función de la estructura organizacional reflejada en el Directorio Activo, permitiendo tener la flexibilidad de restringir por grupos de usuarios el acceso a los sitios, las categorías y las aplicaciones web. Así también, para garantizar el seguimiento al comportamiento del uso de Internet que le den los usuarios, el producto permite contar con reportes detallados y flexibles para realizar un análisis histórico de este comportamiento.

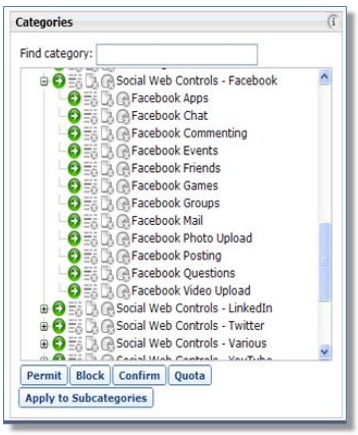

Figura 2.2: Categorías de control en redes sociales

Websense Web Security Gateway inspecciona el contenido Web, protege contra las amenazas dinámicas Web 2.0, previene la pérdida de datos confidenciales y mejora la productividad de los empleados.

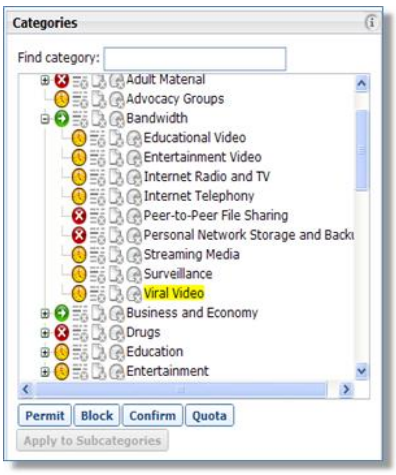

Figura 2.3: Categorías de control de video

2.3. Seguridad Email

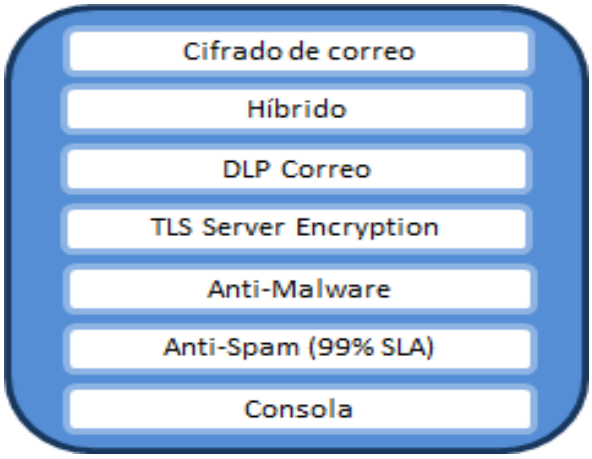

Figura 2.4: Funcionalidades Gateway de Correo

Desafortunadamente, las defensas en las se ha confiado durante años (anti spam, antivirus) son ineficaces en el mundo moderno; sólo en 2010, más de 900 amenazas únicas de día cero no fueron detectadas por los productos de seguridad tradicionales. Sólo uno de cada cuatro productos antivirus [7] son lo suficientemente avanzados como para detectar ataques combinados de email y web (correos con phishing). Las amenazas de correo electrónico han

evolucionado, correos electrónicos con phishing [2] que enlazan a sitios web infectados son la causa de muchas de las violaciones de seguridad de información de hoy en día. Sin embargo, los productos típicos de seguridad de correo electrónico utilizan métodos obsoletos para detectar a tiempo el phishing [2]. No pueden detectar las amenazas combinada web/email que pueden conducir a la infección por malware, y no pueden detectar actividades de empleados que pueden conducir a la pérdida de datos.

Websense® Email Security Gateway a diferencia de otras soluciones de seguridad de email que se basan exclusivamente en anti spam [7], antivirus [7], análisis de reputación y filtrado URL, va más allá de esto; combina la protección email con análisis Web para brindar protección contra ataques combinados (web/email). Email Security Gateway se combina con la tecnología DLP [1] para detectar la pérdida de datos confidenciales que se puedan producir a través del email. La figura 2.4 muestra un resumen grafico de las funcionalidades de Websense Email Security.

LHENRIQUES S.A necesitaba una solución de seguridad email que provea todas las características antes mencionadas. Además, requería realizar encriptación de correos electrónicos para mantener comunicación confidencial con sus socios de negocios y clientes. La solución propuesta utiliza las mismas políticas y reglas de control de fuga de información en todos los vectores de fuga (web, email, endpoint, móviles).

2.4. Seguridad Contra Perdida de Información

Figura 2.5: Diseño y funcionalidades Websense AP-Data

Un solo incidente de pérdida de datos puede mermar la ventaja competitiva de un negocio, debilitar la confianza del cliente, y dar lugar a multas o sanciones de las entidades reguladoras. El problema se agrava aún más con la rápida proliferación de dispositivos móviles, el uso generalizado de los periféricos, y fácil acceso a programas para compartir archivos. Todo esto aumenta la posibilidad de pérdida y robo de datos.

Websense ofrece a LHENRIQUES S.A la tecnología en prevención de pérdida de datos diseñada para identificar, monitorear y proteger la información confidencial. La figura 2.5 describe gráficamente el diseño y funcionalidad de Websense Data Security. Al aprovechar el análisis de contenido unificado que proporcionan las tecnologías de seguridad Web, seguridad Email y prevención de la pérdida de datos (DLP), la solución DLP [1] de Websense usando su motor DICE (Data Identification and Classification Engine) previene con máxima precisión la pérdida de datos, asegura los procesos corporativos y administra el riesgo y el cumplimiento. La solución proporciona una visibilidad para conocer quién envía los datos confidenciales, qué tipos de datos se envían y dónde van esos datos.

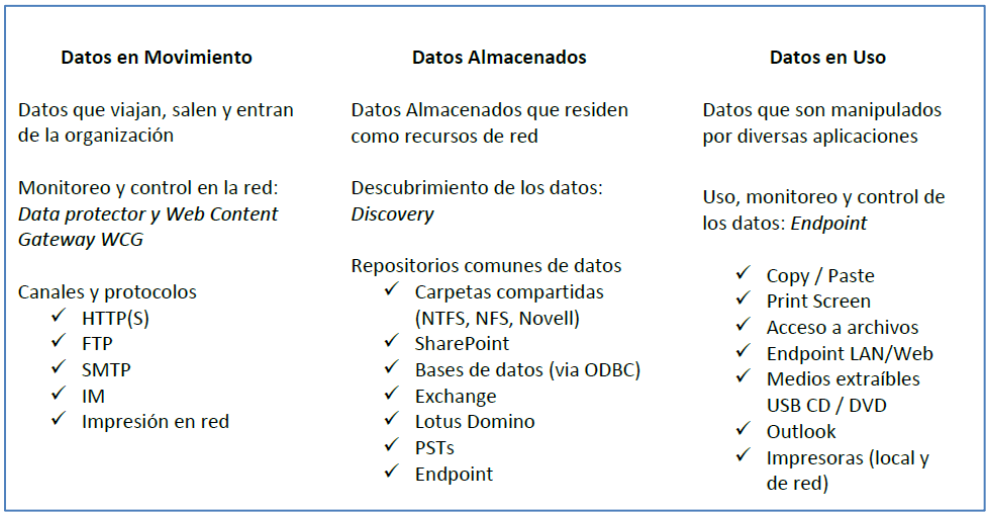

Figura 2.6: Orígenes de datos a proteger

El primer paso para proteger los datos confidenciales es conocer dónde están, cómo están protegidos, quiénes pueden tener acceso a ellos y hacia dónde se pueden enviar. La solución Websense Data Security proporciona un perfil

detallado de sus datos confidenciales, protegiendo datos almacenados, datos en movimiento y datos en uso como se muestra en la figura 2.6. En el caso particular de esta implementación los datos en movimiento serán protegidos por los Gateway de web, correo y ActiveSync [5]; cuando el usuario no se encuentre dentro de la red de la empresa serán protegidos por Websense Endpoint [8].

Los datos almacenados serán analizados con tareas de descubrimiento que se ejecutarán desde servidores de Websense Data Security Server y en las estaciones de trabajo a través del motor Data Security del Endpoint [8] de Websense. Dentro de los datos almacenados se consideran carpetas compartidas, bases de datos, bases de correo electrónico, Microsoft SharePoint y datos almacenados en las estaciones. Los datos en uso serán analizados con los clientes Websense Endpoint [8] y se refiere a la capacidad de detectar uso de información protegida dentro de documentos de ofimática, PDF y navegadores.

La herramienta cuenta con clasificadores incorporados para identificar datos. Clasificadores que se pueden apreciar en la figura 2.7, tales como: patrones, diccionarios, propiedades de archivos, identificación precisa basados en lenguaje natural. En el caso de LHENRIQUES S.A, se definen clasificadores propios basados en la información que desea proteger.

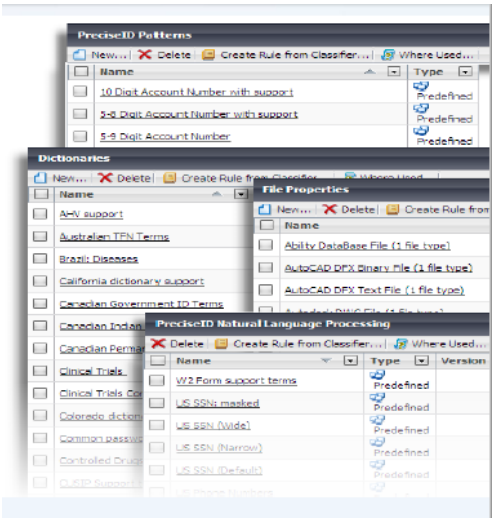

Figura 2.7: Clasificadores incorporados en Websense Data Security

Websense Data Security Suite (DSS) consiste de tres módulos: Data Security Gateway, Data Discover [9] y Data Endpoint [8]. Éstos elementos ayudan a gestionar el riesgo de pérdida de datos por usuarios malintencionados o un mal uso accidental; integrados en una consola centralizada desde donde se pueden administrar todas las políticas, realizar reportes y manejar incidencias.

Websense Data Security Gateway [9]: supervisa los canales de comunicación más comunes tales como web, correo electrónico, FTP, ActiveSync [5] para correo electrónico móvil. Éstos gateways, cuando encuentran datos sensibles que emparejen con una política, tienen la capacidad de bloquear su transmisión, registrar el incidente o ejecutar automáticamente una acción de remediación.

La solución comprende implementar en LHENRIQUES S.A: un Gateway de Web, un Gateway de correo electrónico y un Gateway para análisis de trafico de sincronización de correo electrónico desde y hacia los dispositivos móviles (ActiveSync [5]).

Websense Data Endpoint [8]: Supervisa el tráfico en tiempo real, amplía la visibilidad y control de acceso a datos confidenciales; quien los usa; cómo se están utilizando; donde están siendo transferidos; y qué medidas en tiempo real se toman para evitar la pérdida de datos en las estaciones.

LHENRIQUES S.A adquiere 200 Websense Endpoint [8] para evitar la fuga de información en las estaciones de trabajo que se encuentran en las oficinas de la empresa; así como las estaciones de vendedores que tienen que moverse por todo el país. Websense Endpoint [8] tiene la capacidad de proteger las estaciones de trabajo de los vendedores, aunque estén desconectadas de la LAN; tiene la capacidad de mantener una copia en la estación de las ultimas políticas de protección y actuar de manera independiente, esperando retornar a la empresa para sincronizar los logs e incidencias con la consola central.

Websense Data Discovery [9]: identifica datos con alta precisión, utilizando el motor “DICE” [9] que es un conjunto de tres clasificadores de datos (basados en texto, huellas digitales y aprendizaje basado en ejemplos), que le permite ser más preciso en la búsqueda de información en reposo. DICE soporta tres

categorías de datos: descrito, registrado y aprendido. Los datos descritos incluyen expresiones regulares, diccionarios y clasificadores de lenguaje natural, incluyendo más de 1700 políticas y plantillas. Los datos registrados incluyen fingerprint (huellas digitales), que se pueden comprimir y almacenar en el punto final para protección fuera de la red. Los datos aprendidos son tecnología de aprendizaje avanzado, que emplea algoritmos para analizar pequeñas muestras de datos para llenar la brecha entre los datos descritos y registrados para brindar una mayor precisión y eficiencia. Las capacidades de protección contra robo de datos incluyen reconocimiento óptico de caracteres (OCR) de texto dentro de las imágenes, detección de archivos cifrados y robo de archivos de contraseñas.

Por último, provee la integración de todos los productos en una sola consola de administración llamada TRITON Security, que combina las capacidades de administración e informes de las tecnologías de seguridad Web, seguridad de Email y prevención de la pérdida de datos en una sola interfaz. La consola TRITON de Websense permite a los usuarios definir políticas, administrar incidentes, preparar informes y realizar tareas administrativas desde un punto central basado en Web. Esto proporciona mayores capacidades de administración, visibilidad y control.

2.5. Metodología para implementar Data Lost Prevention.

Figura 2.8: Etapas de un Proyecto Data Lost Prevention

El proyecto Prevención de fuga de información [1] contempló un flujo básico que se aprecia en la figura 2.8, como la metodología para la implementación en LHENRIQUES S.A, este flujo consta de los siguientes pasos:

- Fortalecimiento de la Infraestructura de Seguridad de la Información.
- Identificación de la información a proteger y los riesgos asociados.
- Acciones de Auditoria para la data en movimiento, data en reposo y data en uso.
- Diseño de Políticas para Prevención de fuga de información [1].
- Administración de la Solución DLP [1] y Presentación de Informes.

Fortalecimiento de la Infraestructura de Seguridad de la Información. La primera parte del flujo, la cubre con el fortalecimiento de la infraestructura de seguridad que se adquiere al utilizar herramientas que aseguran los vectores de fuga y a la vez sirvan para protección en esos canales. Se cumplen con la creación de políticas de control de navegación Web, para correo electrónico y análisis de tráfico para correos en móviles ActiveSync [5].

Identificación de datos a proteger y riesgos. Basado en la experiencia de perdida de datos, LHENRIQUES S.A identifica los activos a proteger; enfocando este análisis en la protección de información de plan estratégico de ventas, listado de precios y documentos financieros. Dentro de esta tarea se realizaron fingerprint (una huella digital) de la información confidencial a proteger que se encontraba dentro de bases de datos Oracle y servidores de archivos,

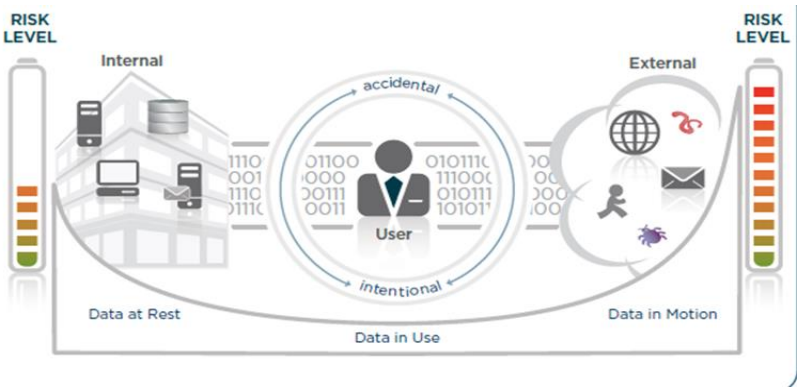

Figura 2.9: Acciones de Auditoria.

Acciones de Auditoria. Luego de haber identificado los datos a proteger se implementa el producto y se realiza un análisis en modo monitorización. En ese momento, no se ejecuta acciones de bloqueo para los incidentes que registren fuga de información; es una etapa de reconocimiento donde se determinan posibles falsos positivos que sirven para afinar y crear reglas claras de monitorización. En la figura 2.9 se muestran gráficamente los eventos que pueden ocurrir en esta etapa y el análisis que deben hacer personal de tecnología junto con los dueños de la información.

Diseño de Políticas. Sin duda que el llegar a esta parte del proyecto fue el momento que todo el personal había esperado pero el más crítico de enfrentar, debido que se le iba a dar tratamiento a fugas de información y posiblemente generaría reacciones en el recurso humano.

Figura 2.10: Diseño de Políticas

Mediante la figura 2.10 se puede observar cuáles son los puntos preponderantes en el diseño de políticas para el control de fuga de información:

- Quién tiene la Información Confidencial, es decir que Áreas del Negocio poseen la información.
- Qué tipo de Información Confidencial debe protegerse. En el caso de la organización se enfocaron en información de ventas y financiera.

- Dónde se encuentra la información a proteger. Dentro de esta etapa se realizó el descubrimiento de información dentro de toda la organización.
- Cómo se va a enviar esta información, cuál es el destino final de la información y por qué medio intentará salir de la organización.
- Acciones a tomar para el envío de información. Cuál es la acción que tomaremos cuando información que intente salir de la organización cumpla las condiciones que están configuradas en una política. Se bloqueará la información, se la enviará a cuarentena, se transformará la información o se la cifrará.

Aplicación de Políticas.

Después del diseño de Políticas de Prevención de fuga de información [1], se realizó la implementación de las mismas en Triton Data Security.

La creación de Políticas incluyó las siguientes tareas:

- Integración de la Solución con el Directorio Activo para leer los usuarios y grupos del dominio.
- Implementación de Políticas de Control de Contenido Web.
- Creación de Políticas de Seguridad de Correo.
- Pruebas de Control de Contenido Web para garantizar el cumplimiento de la Política del Uso Aceptable del Internet.
- Pruebas de cumplimiento de políticas DLP [1] a nivel de todos los vectores de fuga: web, email, ActiveSync [5] y estaciones de trabajo.

Administración y Presentación de Informes

Se aprovechan todas las ventajas de la herramienta para generación de reportes gerenciales y específicos que servirán como insumo para el equipo que trabajará en la administración de riesgos de perdida de información. Reportes como se muestran en la figura 2.11 se pueden obtener; se lista los tipos:

- Reporte de Incidentes
- Resumen ejecutivo

- Evaluación de riesgo
- Severidad y acción
- Fuentes y destinos
- Tendencias
- Estados
- Localización geográfica
- Web DLP destinos por severidad

Figura 2.11: Administración de informes.

CAPÍTULO 3

3. RESULTADOS OBTENIDOS

LHENRIQUES S.A tomó la decisión de implementar Websense Triton Enterprise [3]. Ésta solución unifica todos los componentes esenciales de la defensa contra amenazas y la prevención de la pérdida de datos (DLP [1]) en un sistema integral de seguridad de contenidos; que combina la seguridad web, la seguridad de correo electrónico, la seguridad móvil y las defensas de DLP [1] con inteligencia de seguridad y una consola de administración unificada.

Se realizaron visitas a LHENRIQUES S.A para conocer su infraestructura, conocer la necesidad de protección de fuga de información y levantar documentación de los activos a proteger. De la información obtenida en el levantamiento de información se elaboró un diseño detallado de red, productos Websense y políticas a implementar; las mismas que, involucraron la protección de la navegación Web, Correo electrónico, estaciones de trabajo y dispositivos móviles.

A continuación, se listan tubularmente los resultados obtenidos luego del análisis de la información recabada en LHENRIQUES S.A:

- Diseño de una solución que abarca control de contenido Web, seguridad en correo electrónico y DLP [1] de los vectores Web, Correo y Endpoints.
- Diseño e implementación de políticas para proteger la navegación de los usuarios en Internet. Esto incluye todo el acceso a la Web 2.0. Control de navegación a sitios improductivos.
- Diseño e Implementación de políticas de seguridad de correo electrónico como anti spam [7], antivirus [7], antimalware.
- Diseño e Implementación de políticas de Prevención de fuga de información [1].
- Implementación de Gateways de Control de tráfico HTTP, HTTPS, FTP, SMTP, ActiveSync [5].
- Generación de informes y presentación de resultados.

3.1. Diseño de la solución

El diseño propuesto por AVP Sistemas que se muestra en la figura 3.1, es acogido por LHENRIQUES S.A y se lo lleva a la implementación.

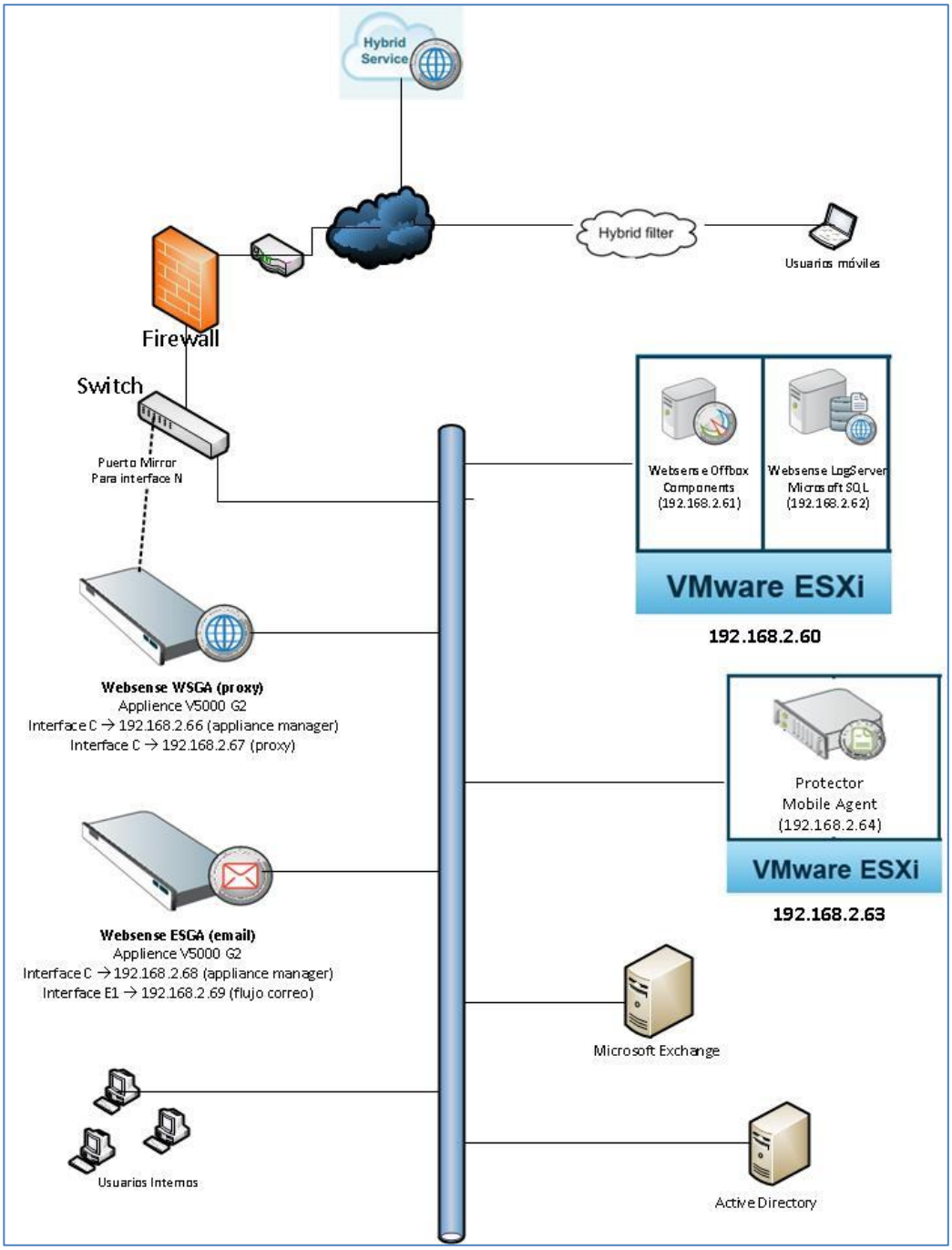

Figura 3.1: Diagrama de diseño final

Los componentes que forman parte de la solución son los siguientes:

3.2. Componentes físicos:

- 2 Appliances Websense v5000 [4] g2. Uno destinado a Gateway de Web y otro para Gateway de correo electrónico.
- 2 servidores Servidor HP-DL 380p. Uno se usó para virtualizar los equipos Windows donde se alojaron los componentes Websense OffBox.

3.3. Componentes lógicos:

- Hypervisor Vmware vsphere 6 se ejecuta en los 2 servidores físicos HP.
- Servidor Windows 2012 R2 estándar para Websense Triton Console, componentes OffBox de Web, Correo y Websense DSS.
- Servidor Windows 2012 R2 estándar para Websense Logserver Web y Correo, Bases de datos Websense y repositorio de forense DLP [1]. Además, en este mismo servidor se instaló Microsoft SQL Server.
- Un appliance virtual Websense Protector Mobile Agent para análisis de Trafico Microsoft ActiveSync [5].
- Agentes Websense Endpoint [8] para control de fuga de información en las estaciones de trabajo.

3.4. Consola de administración unificada.

Luego de la instalación y configuración de la plataforma Websense Triton Enterprise [3], se obtiene la consola de administración unificada Triton que apreciamos en la figura 3.2. En esta consola se presentan todos los elementos de la solución unificados y compartiendo información, como son las políticas DLP [1] que es lo importante para el caso de LHENRIQUES S.A.

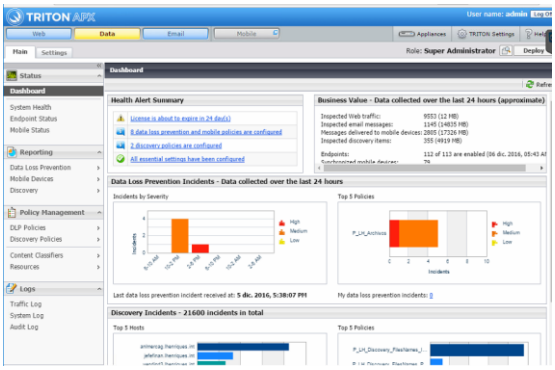

Figura 3.2: Consola unificada de administración Triton

3.5. Diseño de Políticas

Luego del análisis de la información obtenida en entrevistas con personal tecnología quienes expresaron la necesidad de la empresa, se definen políticas para protección Web, Correo y Prevención de fuga de información [1].

3.6. Políticas de Seguridad de Contenido Web.

Se muestran en la figura 3.3 las políticas Web implementadas, donde se aprecia que han sido asociadas a grupos de Active Directory relacionados con áreas de trabajo de la organización.

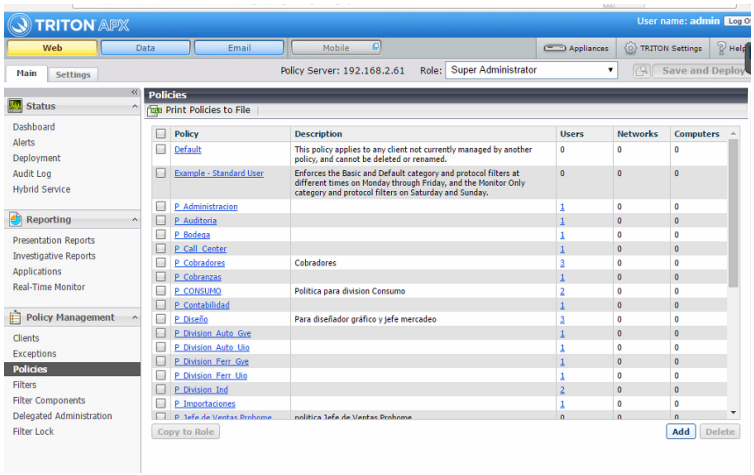

Figura 3.3: Políticas Web Implementadas

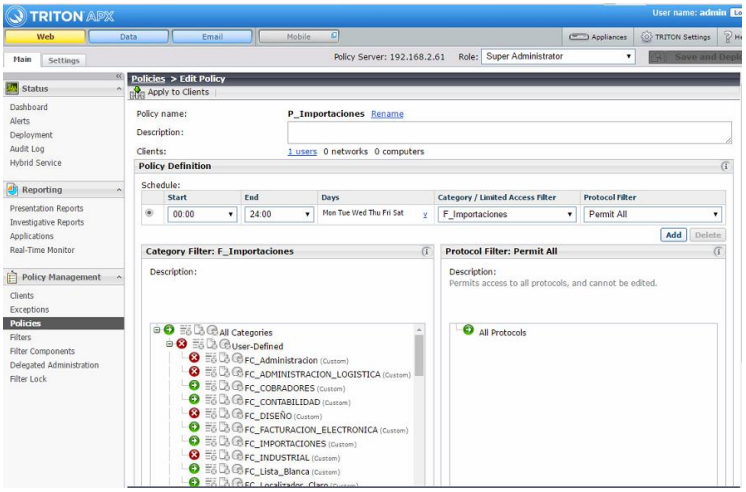

Figura 3.4: Detalle de Política Web

En la figura 3.4 se observa el detalle de una política Web configurada. En la parte superior de la misma se encuentra la sección referente al horario de aplicación, en la parte inferior las categorías y los protocolos que se habilitarán o bloquearán. El resultado final de la aplicación de ésta política es, bloquear o permitir a usuarios el acceso a internet basado en categorías y protocolos Web, aplicable en determinados horarios.

3.7. Políticas y seguridad en correo electrónico

En lo relacionado a la seguridad de correo electrónico, se encuentran dos configuraciones a destacar y que forman el pilar de la seguridad en este vector. En la figura 3.5 se muestra el control de correo electrónico basado en la conectividad desde y hacia internet. Es aquí donde se configura los niveles de conexión, la seguridad y los límites de conexión SMTP.

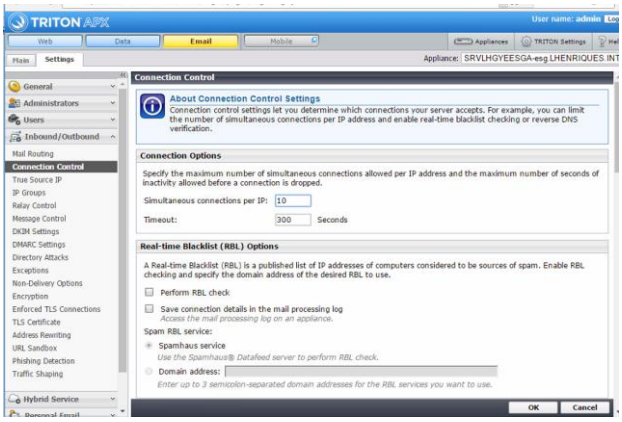

Figura 3.5: Configuración de seguridad email

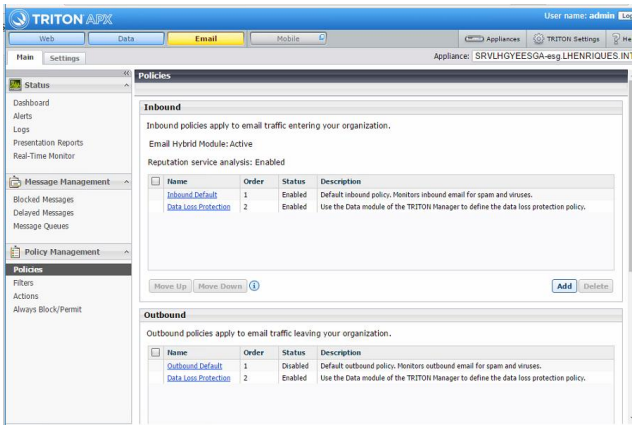

Figura 3.6: Políticas de Seguridad Email implementadas

En la figura 3.6 encontramos las políticas de seguridad email específicamente, estas se basan en control del contenido del correo electrónico, este control se basa en: anti spam [7], antivirus [7], anti phishing [2].

3.8. Políticas para control de fuga de información

Para detener la de fuga de información se crearon políticas de control como se aprecia en la figura 3.7. Estas políticas contienen reglas que realizan análisis de contenido basado en clasificadores; estos a la vez, fueron implementadas con la información proporcionada por los dueños de la información y personal técnico de LHENRIQUES S.A.

Las reglas antes mencionadas realizan el análisis de contenido con los clasificadores; éstos últimos, definen el control basado en el origen y el destino de los datos. Al final, es la acción, la que permite definir si el dato pasa o es bloqueado y si es bloqueado define si guarda o no información forense. En la tabla 1 se puede apreciar un resumen de reglas implementadas.

Clasificador	Aplicable a:	Vector de aplicación	Acción
Basado en huella digital de archivos. Figura 3.8	Toda la organización excepto Gerente General	Web Email Mobile Email Endpoint [8]	Bloquear almacenando información forense
Basado en huella digital de base de datos. Figura 3.9	Toda la organización excepto Gerente General	Web Email Mobile Email Endpoint [8]	Bloquear almacenando información forense
Basado en propiedades de archivos. Figura 3.10	Toda la organización excepto Gerente General	Web Email Mobile Email Endpoint [8]	Bloquear almacenando información forense
Basado en diccionario de palabras. Figura 3.11	Toda la organización excepto Gerente General	Web Email Mobile Email Endpoint [8]	Bloquear almacenando información forense

Tabla 1. Reglas de control de fuga de información implementadas

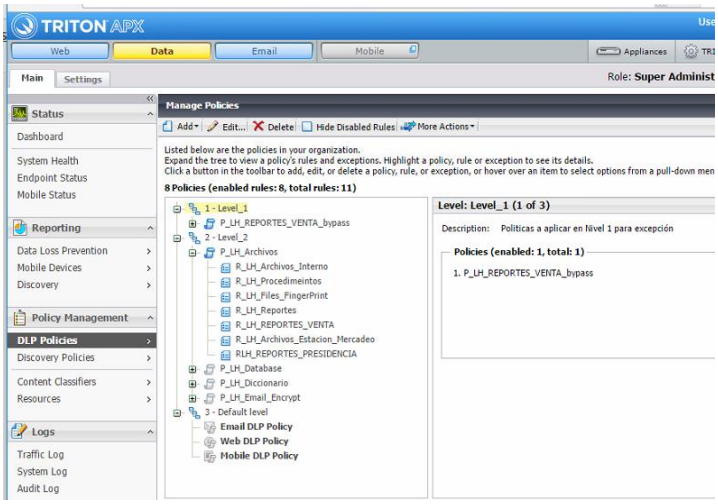

Figura 3.7: Políticas Data Lost Prevention

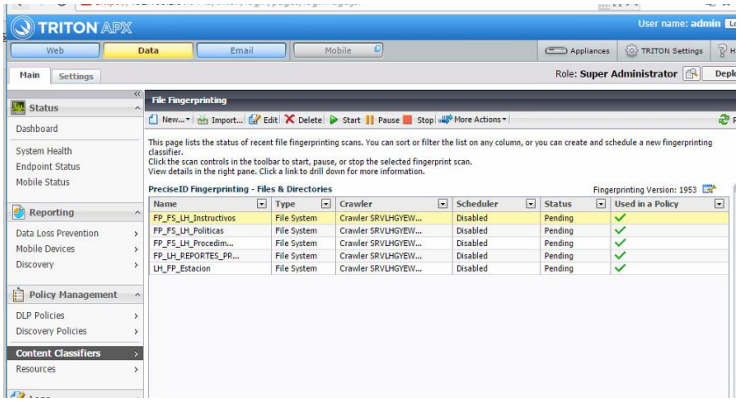

Figura 3.8: Clasificador basado en huella digital de archivos

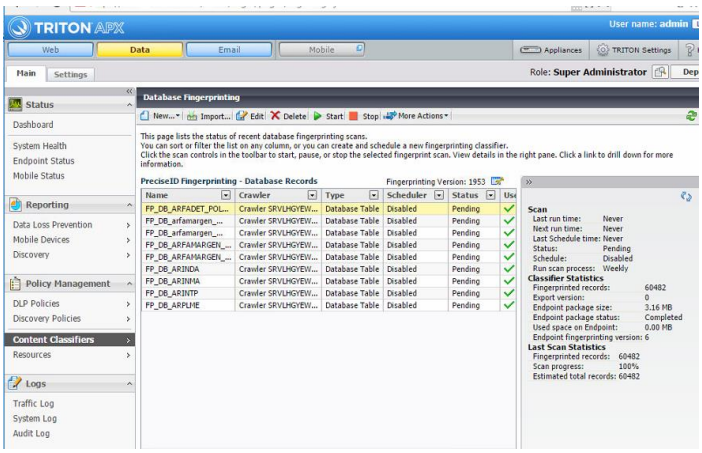

Figura 3.9: Clasificador basado en huella digital de base de datos

Las figuras 3.8 y 3.9 muestran en detalle los clasificadores que fueron creados en la empresa, basados en fingerprint (huella digital) de archivos y bases de datos respectivamente. Estos clasificadores son usados en las reglas para identificar posibles fugas totales o parciales de los datos de donde se obtuvo la huella.

Los clasificadores basados en propiedades de archivos, como los que se observa en la figura 3.10, son utilizados para identificar posibles fugas de archivos basado en su nombre, tamaño, tipo, entre las propiedades más comúnmente usadas.

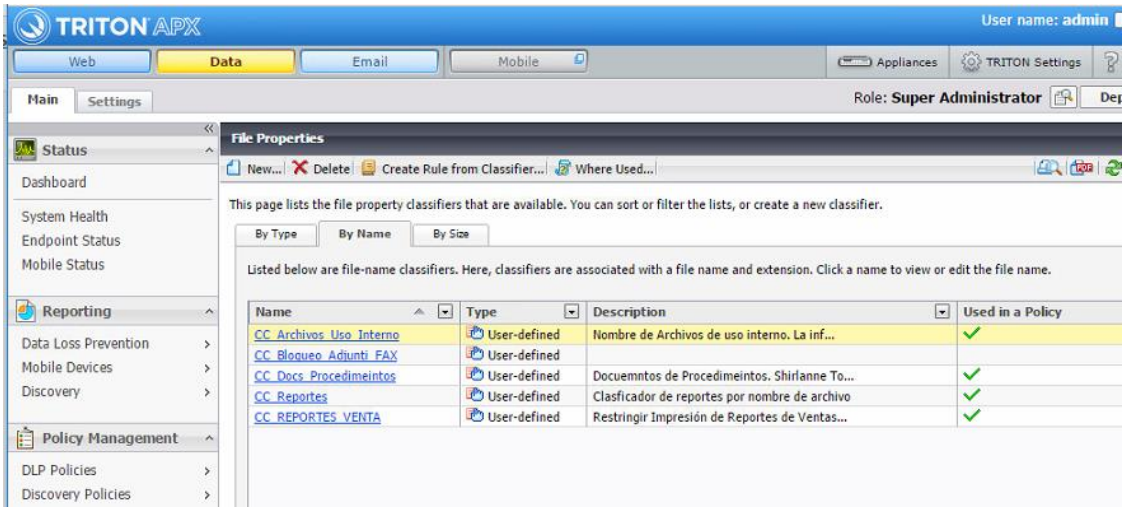

Figura 3.10: Clasificador basado en propiedades de archivos

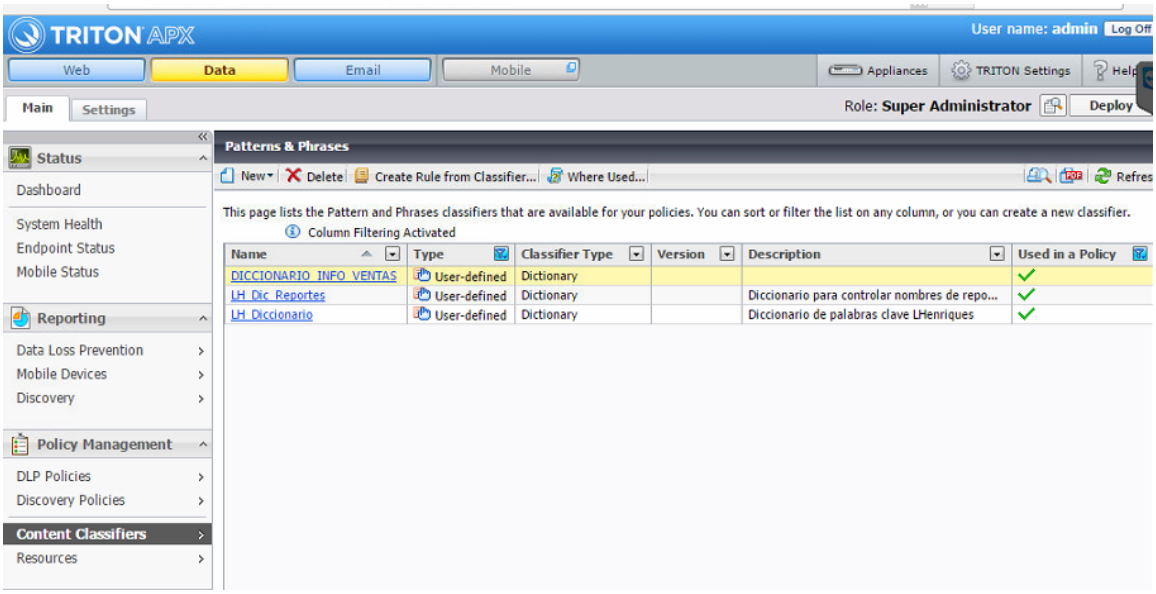

Figura 3.11: Clasificador basado en diccionarios

Los clasificadores basados en diccionario como nos muestra la figura 3.11, fueron usados por la empresa para detener fuga basando la identificación en las palabras agregadas en los diccionarios.

3.9. Generación de informes y reportes

Ya en funcionamiento total la nueva herramienta Websense Enterprise, con todas las reglas anteriormente definidas tanto en el control Web, Email y DLP [1]; lo siguiente fue la generación de informes, reportes y mostrar el comportamiento del control de contenido en tableros en tiempo real.

3.10. Tableros en tiempo real de incidentes de perdida de datos.

Desde la consola Triton se puede acceder a los tableros en tiempo real de Web (figura 3.12), Email (figura 3.13) y reporte de incidentes DLP [1] (figura 3.14). Los dos primeros tableros permiten observar las posibles infracciones a las políticas que se pueden estar cometiéndose cada uno de estos vectores. El reporte de incidentes DLP [1] nos muestra las violaciones de control de fuga de información, la acción tomada sobre la misma y nos proporciona un link para llegar a los detalles del incidente (figura 3.15) e información forense del mismo (figura 3.16). En la información forense se encontrará el detalle de la información del incidente que ha violado las reglas DLP [1].

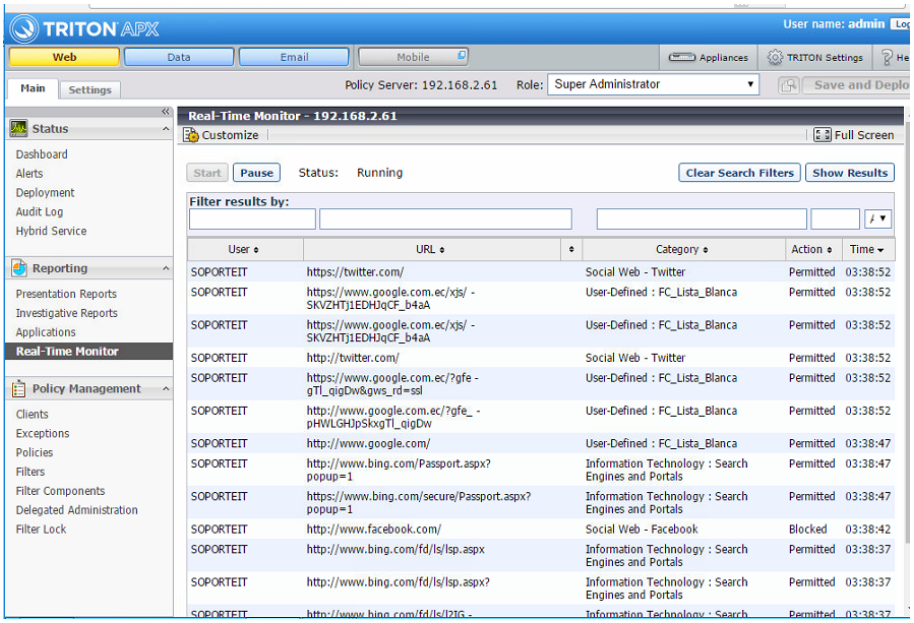

Figura 3.12: Tablero en tiempo real control web

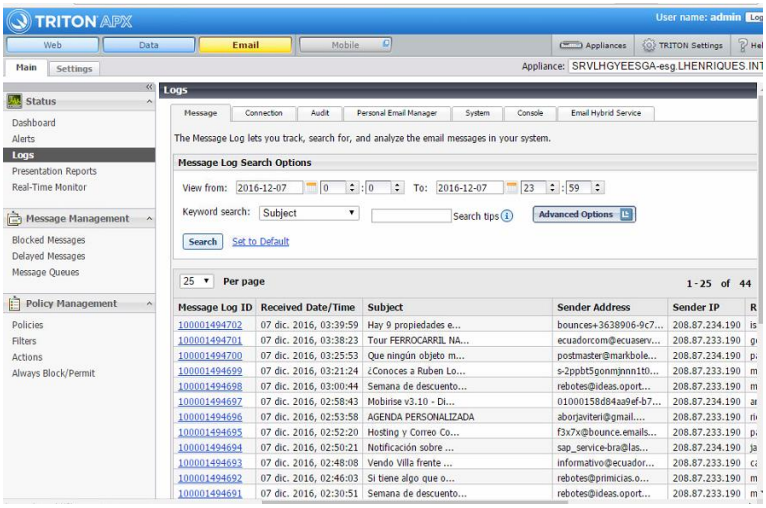

Figura 3.13: Tablero en tiempo real control email

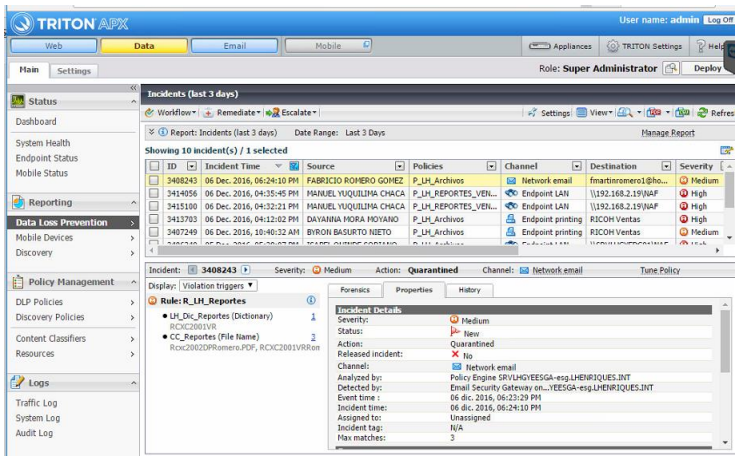

Figura 3.14: Tablero reporte incidentes Data Lost Prevention

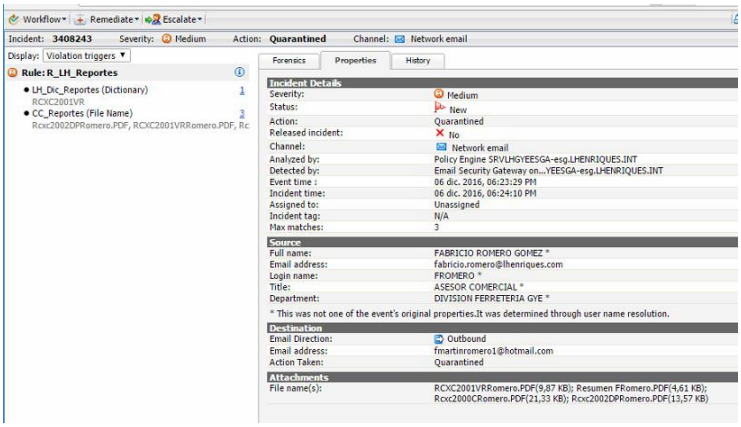

Figura 3.15: Detalle de incidente Data Lost Prevention

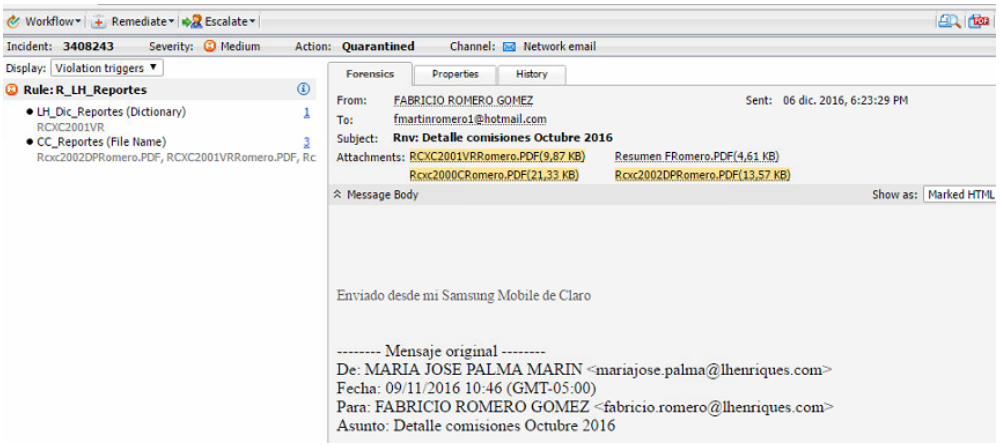

Figura 3.16: Informe forense de incidente de fuga de información

CONCLUSIONES Y RECOMENDACIONES

Las empresas necesitan soluciones de prevención de fuga de información [1] para proteger su reputación en la mayoría de casos y en otros casos cumplir con las normativas y estándares.

Con el desarrollo de este proyecto, se logró el involucramiento del personal interno de la empresa que no conocían al momento que eran dueños o custodios de información sensible y que ésta debía ser protegida. Al mismo tiempo que fueron tomando conciencia de los activos que custodiaban, fueron adquiriendo conocimientos sobre prevención de fuga de información [1] y cómo la nueva herramienta los ayudaría.

Los usuarios estaban activamente involucrados en solicitar protección para nueva información; con esto, se logra demostrar cómo un proyecto de control de fuga de información puede cambiar la cultura que tiene una empresa en la protección de su información sensible. Todos estos cambios quedan plasmados en nuevos documentos de políticas de la empresa para controlar el flujo de la información y la protección de la misma.

El proyecto logró cumplir los objetivos y alcances planteados al inicio del mismo, esto es: Protección de navegación Web, protección sobre flujo de mensajes de correo electrónico y control de fuga de información.

Como recomendación principal, se sugiere a la empresa que mantenga la política de control de fuga de información dentro de un proceso continuo de revisión. Los tableros de visualización de incidentes ayudan con información importante para realizar afinamiento de la herramienta.

Se recomienda siempre ejecutar un proyecto DLP [1] no solo desde la perspectiva de la implementación de una herramienta tecnológica, se debe tener una visión global que involucre a todos los dueños y custodios de la información de la organización, esto debe incluir a la alta gerencia. El proyecto debe concluir con campañas educativas y concienciación a todo el personal sobre el uso de información sensible de la organización.

BIBLIOGRAFÍA

[1]I. Andrade, "DLP: Tecnologías para la prevención de la fuga de información | Revista .Seguridad", Revista.seguridad.unam.mx, 2015. [En línea]. Disponible en: http://revista.seguridad.unam.mx/numero25/dlp-tecnolog-para-la-prevenci-n-de-la-fuga-de-informaci-n. [Accedido: 20- Nov- 2016].

[2]M. Rivero, "¿Qué es el Phishing? | InfoSpyware", Infospyware.com, 2009. [En línea]. Disponible en: https://www.infospyware.com/articulos/que-es-el-phishing/. [Accedido: 20- Nov- 2016].

[3]F. Websense, "Suite TRITON® APX", Forcepoint, 2016. [En línea]. Disponible en: https://www.forcepoint.com/es/product/content-security/triton-apx-suite. [Accedido: 20- Nov- 2016].

[4]F. Websense, "KB Article | Forcepoint Support", Support.forcepoint.com, 2016. [En línea]. Disponible en: https://support.forcepoint.com/KBArticle?id=V-Series-Appliances-Certified-Product-Matrix. [Accedido: 20- Nov- 2016].

[5]"¿Qué es Exchange Active Sync? | One.com", One.com, 2016. [En línea]. Disponible en: https://www.one.com/es/support/faq/que-es-exchange-active-sincronizar. [Accedido: 20- Nov- 2016].

[6]F. Websense, "Forcepoint® Web Filter & Security", Forcepoint, 2016. [En línea]. Disponible en: https://www.forcepoint.com/es/product/web-filtering/websense-web-filter-security. [Accedido: 20- Nov- 2016].

[7]S. Izquierdo, "AntiSpam – AntiVirus | Abartia Team", Abartiateam.com, 2016. [En línea]. Disponible en: http://www.abartiateam.com/antispam-antivirus. [Accedido: 20- Nov- 2016].

[8]F. Websense, "TRITON AP-ENDPOINT", Forcepoint, 2016. [En línea]. Disponible en: https://www.forcepoint.com/es/product/data-insider-threat-protection/triton-ap-endpoint. [Accedido: 20- Nov- 2016].

[9]F. Websense, "TRITON® AP-DATA", Forcepoint, 2016. [En línea]. Disponible en: https://www.forcepoint.com/product/data-insider-threat-protection/triton-ap-data. [Accedido: 20- Nov- 2016].