ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"SOLUCIÓN DE CONTROL DE CONTENIDO WEB, SEGURIDAD DE CORREO, CIFRADO DE CORREO SALIENTE Y PREVENCIÓN DE FUGA DE INFORMACION (DLP) CONFIDENCIAL A TRAVÉS DE LOS VECTORES WEB, CORREO Y ENDPOINTS"

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del grado de:

INGENIERO EN ELECTRICIDAD ESPECIALIZACIÓN ELECTRÓNICA

JAVIER EDUARDO PACTONG LUCERO

GUAYAQUIL – ECUADOR

AÑO: 2015

AGRADECIMIENTO

Agradezco a Dios por sus bendecirme y guiar mis pasos en cada instante, a mis padres por su apoyo constante en la consecución de mis metas, a mis profesores por su valiosa orientación profesional y a mis amigos por creer siempre en mí.

DEDICATORIA

Dedico este trabajo a mis padres, en especial a mi abuela que con su esfuerzo y sacrificio cada día me han ayudado a convertirme en la persona que soy. A mis amigos, quienes cada día me alentaron a culminar esta etapa profesional.

TRIBUNAL DE SUSTENTACIÓN

M.S.C. César Yépez F.	**Ph.D. Francisco Novillo P.**
PROFESOR DELEGADO	PROFESOR DELEGADO
POR LA SUBDECANA DE LA FIEC	POR LA SUBDECANA DE LA FIEC

DECLARACIÓN EXPRESA

"La responsabilidad por los hechos, ideas y doctrinas expuestas en este Informe me corresponde exclusivamente; y, el patrimonio intelectual de la misma, a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL"

(Reglamento de Graduación de la ESPOL).

.....

Javier Eduardo Pactong Lucero

RESUMEN

En la actualidad el manejo de la información confidencial, constituye uno de los pilares fundamentales de la Seguridad de la Información en las instituciones financieras, en especial las que tienen que cumplir normativas internacionales de seguridad y protección de números de tarjetas de crédito como PCI-DSS [1].

Pacificard S.A. requería proteger la información de su información confidencial del uso indebido por personal interno o externo de la organización, por lo que se implementó una solución de Prevención de Fuga de Información o DLP (Data Loss Prevention) por sus siglas en inglés.

Para realizar la protección del uso indebido de información confidencial se realizó una búsqueda en toda la organización de quienes poseían información de tarjetas de crédito, para minimizar el rango de exposición de la información confidencial, y se procedió a monitorear el uso de las mismas a través de los vectores principales de fuga Web, Correo y PCs (Endpoints).

Una vez detectada la información confidencial, se procedió a la creación de políticas para monitorear y prevenir la fuga de información confidencial a través de los vectores Web, Correo y PCs, así como el control de la navegación Web y el cifrado del correo saliente que contiene información confidencial.

ÍNDICE GENERAL

AGRADECIMIENTO II

DEDICATORIA III

TRIBUNAL DE SUSTENTACIÓN IV

DECLARACIÓN EXPRESA V

RESUMEN VI

ÍNDICE GENERAL VII

ABREVIATURAS IX

INTRODUCCIÓN X

CAPÍTULO 1 1

1. METODOLOGÍA Y SOLUCIÓN TECNOLÓGICA IMPLEMENTADA 1

1.1 Descripción del Proyecto 2

1.2 Soluciones Tecnológicas del Proyecto. 5

1.2.1 Solución de Control de Contenido Web. 5

1.2.2 Solución de Seguridad de Correo 8

1.2.3 Solución de Prevención de Fuga de Información 9

1.3 Metodología del Proyecto 12

1.3.1 Fortalecimiento de la Infraestructura de Seguridad de la Información. 13

1.3.2 Identificación de datos a proteger y riesgos. 13

1.3.3 Acciones de Auditoria. 14

1.3.4 Diseño de Políticas. 16

1.3.5 Aplicación de Políticas. 18

1.3.6 Administración y Presentación de Informes 19

CAPÍTULO 2 21

2. RESULTADOS OBTENIDOS 21

2.1 Diseño de la Solución 22

2.2 Diseño de Políticas 23

2.2.1 Políticas de Seguridad de Contenido Web. 24

2.2.2 Políticas de Seguridad de Correo. 25

2.2.3 Políticas de Prevención de Fuga de Información. 26

2.3 Generación de Informes 27

2.3.1 Informe de Seguridad de Control de Contenido Web. 27

2.3.2 Informe de Seguridad de Correo. 30

2.3.3 Informe de Prevención de Fuga de Información. 30

CONCLUSIONES Y RECOMENDACIONES 33

BIBLIOGRAFÍA 37

ANEXOS 39

ABREVIATURAS

DLP	Data Loss Prevention
PCI-DSS	Payment Card Industry Data Security Standard
PCs	Personal Computers
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
SMTP	Simple Mail Transfer Protocol
URL	Uniform Resource Locator
IPS	Intrussion Prevention System
FTP	File Transfer Protocol
USB	Universal Serial Bus
CD	Compact Disc
MTA	Mail Transfer Agent
VRRP	Virtual Router Redundancy Protocol
OCR	Optical character recognition

INTRODUCCIÓN

La exposición al Internet ha permitido la globalización de las empresas y el acceso de los usuarios a la información de forma fácil y rápida. Dicho acceso ha expuesto a las organizaciones a nuevas y variadas formas de robar información confidencial y sensible con el objetivo de beneficiarse y causar daño, originados ya sea debido al mal uso de la información o al desconocimiento del manejo de la misma por parte de los usuarios internos o externos.

El buen manejo de la información confidencial o sensible se ha vuelto mandatorio en entidades financieras, que requieren cumplir regulaciones internacionales como PCI-DSS [1] para proteger información de números de tarjetas de crédito o proteger información confidencial de estados financieros o clientes.

En relación a la preocupación creciente de las empresas de proteger la información confidencial se ha establecido estrategias de protección, las cuales requieren de un conocimiento claro y detallado del flujo de información que se maneja dentro y hacia fuera de las organizaciones, lo cual conlleva a un manejo y control adecuado de la información que circula a través de protocolos HTTP, HTTPS, SMTP o Endpoints (PCs).

La metodología y estrategias implementadas para proteger la información confidencial, se detalla en el Capítulo 1.

En el Capítulo 2 se detallan los resultados obtenidos de la metodología implementada.

CAPÍTULO 1

1. METODOLOGÍA Y SOLUCIÓN TECNOLÓGICA IMPLEMENTADA

En base a la necesidad de cumplimiento de la normativa PCI-DSS [1], respecto a protección de números de tarjetas de crédito se realizó un diseño de ingeniería para cubrir las brechas de seguridad de la información en los vectores Web, Correo y Endpoints.

Se realizó un levantamiento de información inicial de las herramientas y políticas que poseía la organización, tanto para filtrado estático de URLs Web, como para antispam.

Del levantamiento de información se realizó un diseño de ingeniería para una solución unificada de control de contenido Web 2.0, seguridad de correo, cifrado de correo saliente y Prevención de Fuga de Información en los vectores Web, Correo y Endpoints.

El enfoque del diseño de ingeniería es revisar los flujos de tráfico Web, SMTP que conllevan o transportan información confidencial o sensible de números de tarjetas de crédito.

De la misma forma se identificó en cuales PCs de la organización se maneja información confidencial de números de tarjetas de crédito, para minimizar el rango de exposición y la cobertura de la solución a implementarse.

1.1 Descripción del Proyecto

Después de analizar con la organización el flujo de datos que se enviaba por el Internet y en base al análisis del diagrama inicial mencionado en la Figura 1.1.se definió los 3 vectores de fuga de información principales los cuales fueron Web, Correo y PCs.

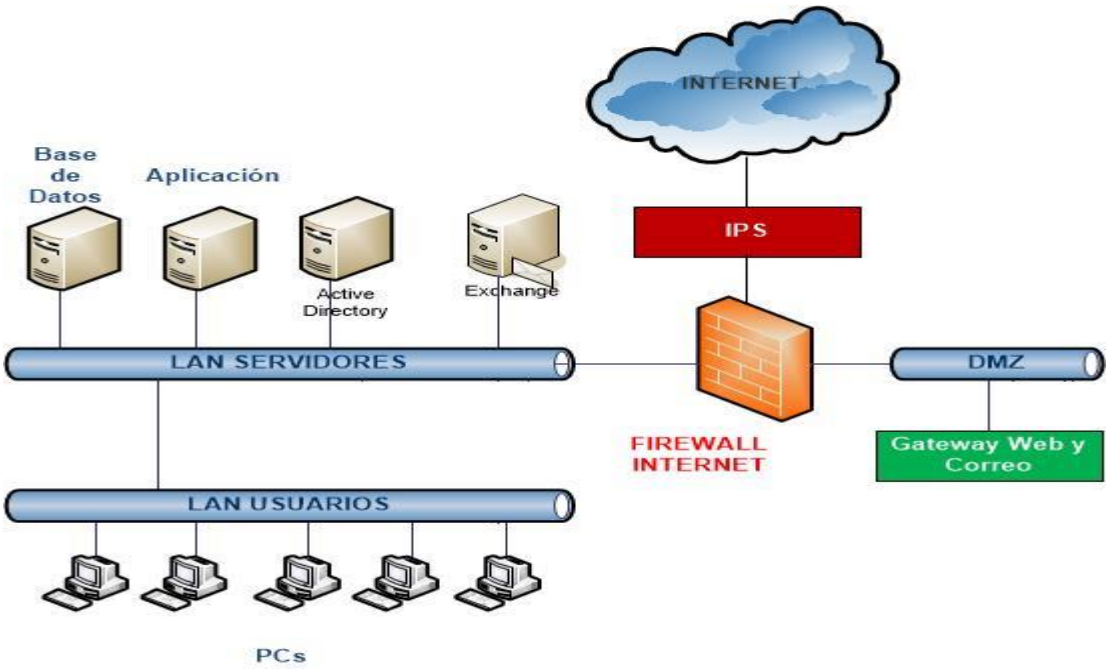


Figura 1.1: Diagrama Inicial de la Organización

El Proyecto tuvo como objetivo realizar un diseño de ingeniería e implementación para cubrir las brechas de seguridad de la información en los 3 vectores, con la finalidad de proteger tráfico saliente HTTP, HTTPS, SMTP de la organización hacia el Internet, así como la protección de números de tarjetas de crédito.

En base de que el pilar fundamental para implementar una solución de Prevención de Fuga de Información, consiste en proteger la navegación y el correo corporativo, se incluyó dentro del proyecto soluciones para control de contenido Web, Seguridad de Correo y Cifrado de Correo como primera medida de protección frente a amenazas externas.

Dado que la organización ya poseía herramientas de seguridad como Firewalls e IPS, tal como se indica en la Figura 1.1, no se incluyó estas herramientas de protección y en su lugar se realizó una integración de la nueva plataforma con las herramientas de Firewall e IPS ya existentes. Dicha integración consistió en crear reglas en el Firewall e IPS que permitan el tráfico HTTP, HTTPs y SMTP solo en los gateways de Web y Correo. El resto de los usuarios de la organización fueron configurados para que utilicen solo los gateways de Web y de Correo.

Basado en el volumen de tráfico detectado a través de las estadísticas del firewall de la organización, se detectó que el 90% del flujo de paquetes de la red del cliente correspondía a los protocolos HTTP, HTTPS y SMTP. Esta información inicial permitió el diseño de una infraestructura de Prevención de Fuga de Información para tráfico de red HTTP, HTTPS y SMTP con los siguientes criterios:

- Bloquear a nivel del firewall la entrada o salida de tráfico de usuarios para protocolos diferentes a HTTP, HTTPs, SMTP.
- Enrutar todo el tráfico HTTP, HTTPS a un cluster Activo-Pasivo de gateways de red para realizar la inspección de contenido Web y Prevención de Fuga de Información DLP en tráfico HTTP y HTTPS.
- Enrutar todo el tráfico SMTP a un cluster Activo-Pasivo de gateways de red para realizar la inspección de correo y Prevención de Fuga de Información DLP en tráfico SMTP.
- Controlar la salida de envío de información confidencial en las PCs con sistema operativo Windows a través del uso de un agente de software.

El diseño tuvo como objetivo inspeccionar, proteger y evitar la fuga de información clasificada por la organización como confidencial en especial la información de números de tarjetas de crédito. La clasificación de esta información confidencial fue realizada por la organización en base a los criterios de cumplimiento de la normativa PCI-DSS [1], cuyo objetivo es proteger la información confidencial de números de tarjetas de crédito, así como criterios específicos del negocio como información de clientes, etc.

En base a los criterios anteriormente mencionados se realizó un diseño de ingeniería para cubrir las necesidades la organización con los siguientes componentes:

- Consola de Administración de la Solución.
- 2 Gateways en cluster Activo-Pasivo para Control de Contenido Web y DLP Web.

- 2 Gateways en cluster Activo-Pasivo para Control de Correo y DLP Correo.
- Agente de Software para control de DLP en 600 PCs que tienen sistema operativo Windows.

1.2 Soluciones Tecnológicas del Proyecto.

1.2.1 Solución de Control de Contenido Web.

Las soluciones de filtrado de contenido Web o content filtering [2] tienen como objetivo controlar el contenido Web que se muestra a los usuarios en los browsers como Internet Explorer, Mozilla Firefox o Google Chrome. De esta manera se reduce el riesgo de exposición de los usuarios a ataques en páginas Web que contienen información maliciosa como virus, troyanos o malware.

Las soluciones de control de contenido utilizan las siguientes tecnologías basados en el análisis del protocolo HTTP y HTTPS:

- Web mining [11] tecnología basada en minería de datos para extraer información del contenido de las páginas Web.
- Man in the middle [12]. Esquema utilizado para interceptar la comunicación de los usuarios, con el objetivo de obtener el certificado digital para abrir una sesión HTTPS.
- Esquemas de reputación basados en análisis estadísticos de tráfico.
- Recolección y análisis de tráfico basada en la nube para realizar clasificación de URLs.

A diferencia de las soluciones estáticas para filtrado URL, el filtro de contenido se enfoca como bien su nombre lo indica en revisar el contenido ya sea estático o dinámico como video, aplicaciones, independiente de la URL donde se encuentre alojado.

El nivel de granularidad y control que tienen las soluciones de filtro de contenido permitió a la organización crear políticas de control de navegación basadas en las siguientes categorías [3]:

- Reputación Web: DNS dinámicos, exploits emergentes, contenido sospechoso.
- Filtros de Seguridad: Botnets, Malware avanzado, Keyloggers.
- Control de Ancho de Banda: Streaming, Videos Educacionales, Videos de Entretenimiento, Internet Radio and TV. Todas estas categorías se mencionan en la Figura 1.2.
- Categorías de Productividad.
- Categorías básicas: material adulto, educación, entretenimiento, gobierno, Information Technology.
- Categorías de redes sociales como Facebook, Linkedin, Twitter, YouTube. De acuerdo a la Figura 1.3 las categorías pueden ser tan granulares que incluso se puede llegar a bloquear chat dentro de redes sociales.

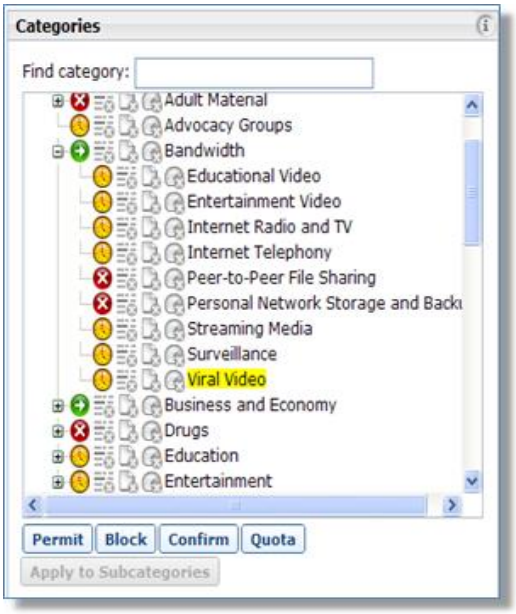


Figura 1.2: Categorías de control de video

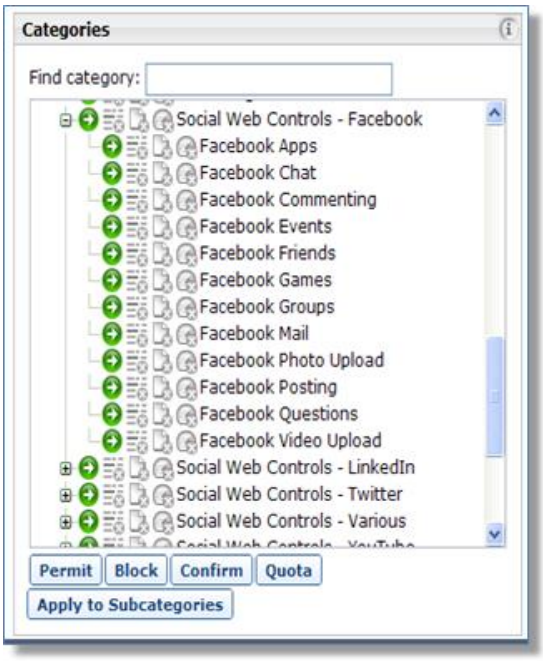


Figura 1.3: Categorías de control en redes sociales

1.2.2 Solución de Seguridad de Correo

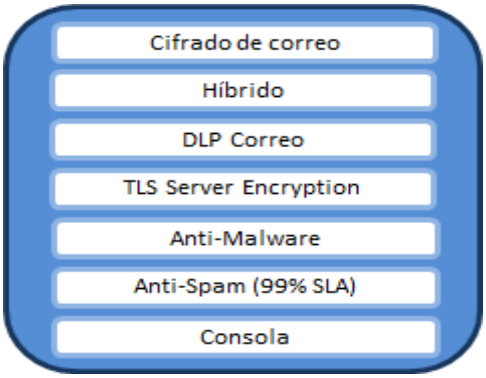


Figura 1.4: Funcionalidades Gateway de Correo

La solución de seguridad de correo consistió en 2 Gateways de correo con las funcionalidades descritas en la Figura 1.4:

- Antispam [4].
- Antivirus [5].
- Cifrado de correo saliente hacia el Internet.
- Protección híbrida para control de spam en la nube del Internet.

Se realizó la configuración el servidor de Correo Microsoft Exchange, de tal forma que el Gateway de Correo funcione como Mail Transfer Agent MTA [6] de todos los correos corporativos que se dirigen hacia el Internet.

En base al funcionamiento del protocolo SMTP se han desarrollado los siguientes métodos de protección del correo corporativo:

- Análisis de la reputación del correo entrante basado en la IP origen, utilizando listas negras.
- Análisis del contenido del correo por palabras claves.
- Análisis en la nube del Internet del contenido del correo para detectar envío masivo de correos.

1.2.3 Solución de Prevención de Fuga de Información

Los componentes de la Solución de Prevención de Fuga de Información [8] del proyecto comprenden:

- Diseño e Implementación de una metodología para el manejo de información de números de tarjetas de crédito.
- Implementación de soluciones tecnológicas que permitan descubrir información de números de tarjetas de crédito dentro de la organización.
- Implementación de tecnologías de huella digital o fingerprinting [9] para identificar información de números de tarjetas de crédito.
- Implementación de soluciones tecnológicas que ejecuten la definición de políticas de Prevención de Fuga de Información a través de los vectores Web, Correo y PCs.

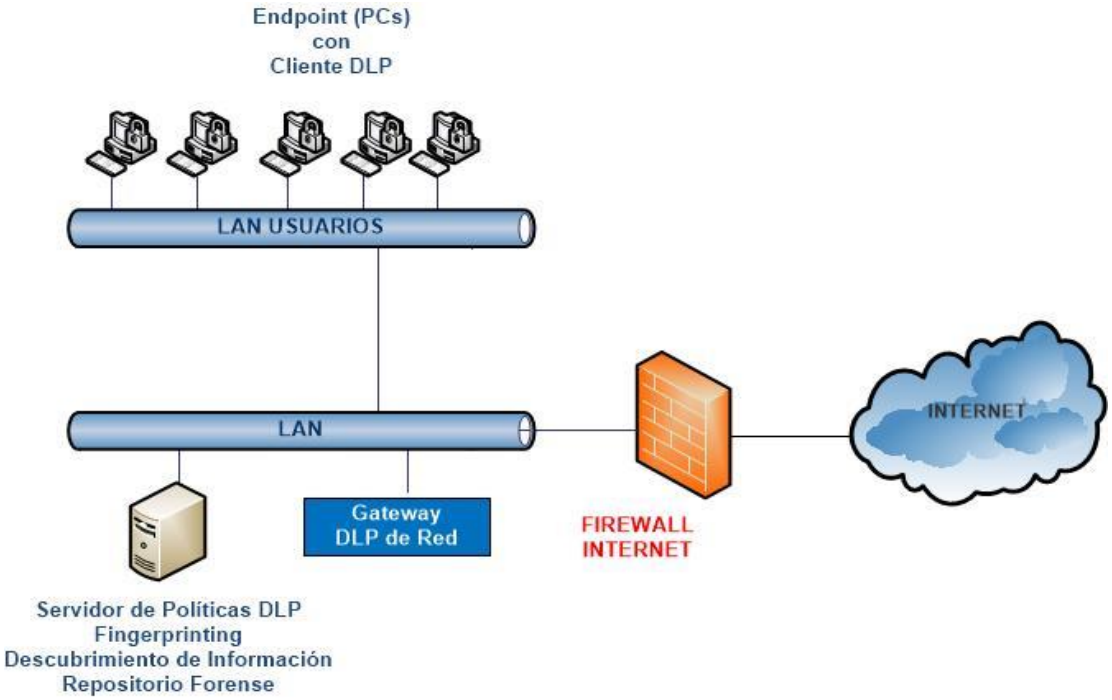


Figura 1.5: Arquitectura Solución Tecnológica DLP.

Las componentes descritas en la Figura 1.5 de la Arquitectura de la Solución Tecnológica de Prevención de Fuga de Información son las siguientes:

- Servidor de Políticas DLP que incluye las siguientes funcionalidades: Motor de Políticas, Huella Digital, Descubrimiento de Información Confidencial y Repositorio Forense.
- Gateway DLP de red. Encargado de realizar el cumplimiento de las Políticas DLP para tráfico HTTP, HTTPS y SMTP.
- Software o Agente DLP para PCs. Encargado de realizar el cumplimiento de las Políticas DLP para todas las aplicaciones

entre las cuales se encuentran Print Screen de pantallas, impresión, medios removibles.

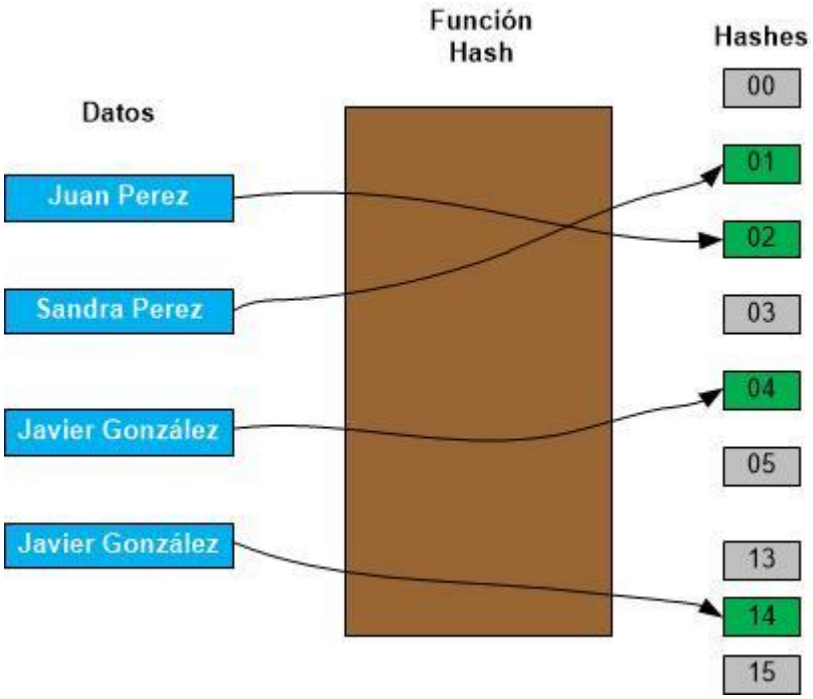


Figura 1.6: Función HASH.

El reconocimiento o detección de información confidencial se basa en las siguientes tecnologías:

- Análisis de patrones de datos para detectar expresiones regulares.
- Análisis de patrones de datos para detectar palabras claves.
- Tecnología de huella digital o fingerprinting [9]. La tecnología de huella digital consiste en realizar una función hash [13] de la información a proteger, por definición está función hash es única y es utilizada para mapear información digital de tamaño

arbitrario a datos digitales de tamaño fijo. Una vez realizado el hash de la información confidencial es comparado con el hash generado por cada paquete de datos que intenta salir de la organización. Dentro de los diferentes tipos de funciones HASH tenemos MD5 o SHA-1 utilizados ampliamente en tecnologías de cifrado simétrico y asimétrico.

1.3 Metodología del Proyecto

Figura 1.7: Etapas de un Proyecto DLP

En la Figura 1.7 se describe las etapas y metodología de un Proyecto de Prevención de Fuga de Información (DLP), los cuales tienen los siguientes puntos:

- 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.
- Aplicación de Políticas.
- Administración de la Solución DLP y Presentación de Informes.

1.3.1 Fortalecimiento de la Infraestructura de Seguridad de la Información.

En virtud de que la solución de Prevención de Fuga de Información debe ser instalada en una red con una infraestructura de Seguridad de la Información robusta, el fortalecimiento de la misma en los vectores Web y Correo se convierte en una parte fundamental del proyecto.

Basado en esta necesidad inherente a todo proyecto de Prevención de Fuga de Información, se realizó el fortalecimiento de la red utilizando soluciones de Control de Contenido Web y Correo. Dentro de la implementación de ambas soluciones se realizó el diseño de Políticas de Uso Aceptable del Internet y del Correo.

Este fortalecimiento constituye un complemento fundamental del proyecto, ya que no puede existir Prevención de Fuga de Información en una red que tenga brechas de seguridad.

1.3.2 Identificación de datos a proteger y riesgos.

Esta fase del proyecto fue desarrollado por la organización direccionada al cumplimiento de la normativa internacional PCI-DSS [1], la cual se enfoca en la protección de números de tarjetas de crédito.

Dentro de esta tarea se realizó una huella digital [9] en bases de datos y servidores de archivos, de la información confidencial de números de tarjeta de crédito a proteger.

1.3.3 Acciones de Auditoria.

Es importante recalcar que las Acciones de Auditoria se realizan de acuerdo al estado de los datos, tal como se indica en la Figura 1.8. Dependiendo del estado de la información existen 3 tipos:

- Data en Reposo. Por ejemplo información almacenada en bases de datos, repositorios o almacenamientos.
- Data en Uso. Información que se copia y pega constantemente o a la cual se tiene acceso a través de aplicaciones.
- Data en Movimiento. Información que se encuentra circulando a través de tráfico de red como HTTP, HTTP o SMTP.

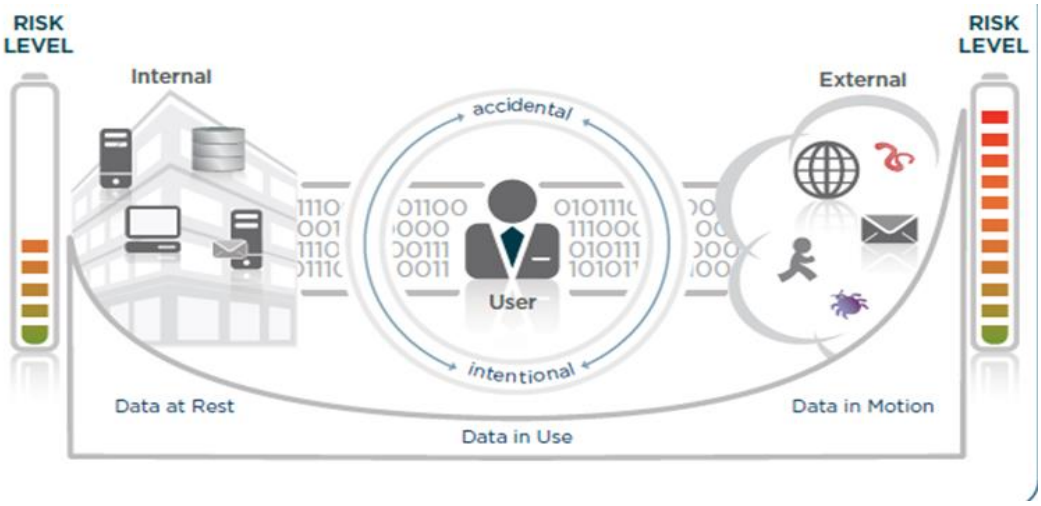


Figura 1.8: Acciones de Auditoria.

La Data en movimiento, es la información que varía dentro de la organización y se intercambia con clientes y asociados, se encuentra expuesta a un mayor nivel de riesgo, por consecuencia las acciones de auditoria y controles implementadas por la organización son mucho mayores. El diseño de ingeniería de la solución de Prevención de Fuga de Información se enfocó en proteger la Data en movimiento de la organización a través de políticas de control y acciones de auditoria destinadas a proteger los números de tarjeta de crédito de la Entidad Financiera a través de los vectores Web, Correo y PCs.

Dentro de las tareas de Auditoria se realizó un descubrimiento de la información confidencial de números de tarjetas de crédito dentro de la organización.

1.3.4 Diseño de Políticas.

Figura 1.9: Diseño de Políticas

Parte fundamental del proyecto fue el diseño de Políticas de Prevención de Fuga de Información para los vectores Web, Correo y PCs. De acuerdo a lo indicado en la Figura 1.9 el Diseño de Políticas se enfocó en las siguientes premisas:

- 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 el enfoque principal era proteger los números de tarjetas de crédito.
- Dónde se encuentra la información a proteger. Dentro de esta etapa se realizó el descubrimiento de información de número de tarjetas de crédito dentro de toda la organización.

- Cómo se va a enviar esta información, es decir a través de que medio tecnológico se va a enviar la información. Dentro de los diferentes medios tenemos aplicaciones Web, correo corporativo e incluso el transporte de la información a través de medios USBs removibles, CDs o impresión.
- Acciones a tomar para el envío de información. Dentro de las múltiples acciones a definir se pueden encontrar bloquear el envío de información a través del vector Web, cifrar correos que tengan información confidencial o sensible o cifrar información de números de tarjetas de crédito que se copie a medios removibles como USBs o CDs.

Figura 1.10: Diagrama de Flujo de Creación de Políticas.

La Figura 1.10 resume el Diagrama de Flujo que se debe seguir para la creación de una Política de Prevención de Fuga de Información, enfocada siempre a que Área de la Organización posee la información a proteger.

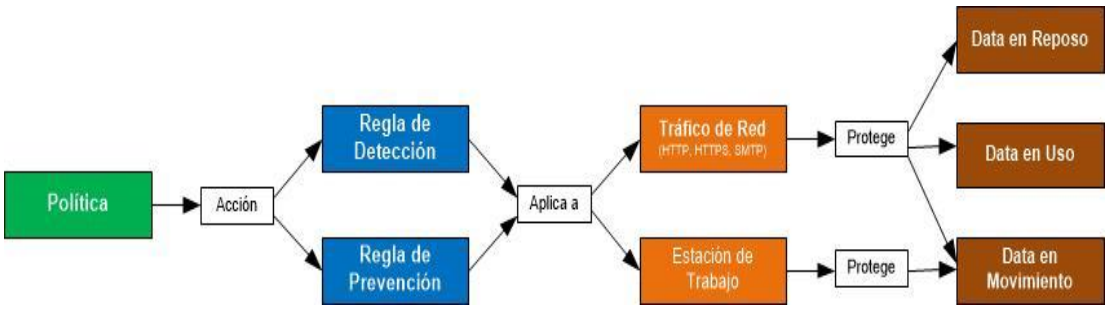


Figura 1.11: Diagrama de Flujo de Ejecución de Políticas.

Desde el punto de vista del tipo de política de Prevención de Fuga de Información se establece el diagrama de Flujo de la Figura 1.11, donde se indica reglas de detección y reglas de Prevención. Las reglas de detección especifican como detectar contenido sensible utilizando expresiones regulares, palabras claves o tecnología de fingerprinting [9]. Las reglas de detección especifican como debe ser tratada la información confidencial.

1.3.5 Aplicación de Políticas.

Después del diseño de Políticas en la Solución Tecnológica de Prevención de Fuga de Información, se realizó la implementación de las mismas en los vectores Web, Correo y PCs.

La Aplicación de Políticas incluyó las siguientes tareas:

- Despliegue del certificado digital en las computadores de la organización, a través de Políticas de Directorio Activo.

- Integración de la Solución con el Directorio Activo para leer los usuarios y grupos del dominio.
- Implementación de Políticas de Control de Contenido Web.
- Implementación de Políticas de la Plataforma de Seguridad de Correo.
- Creación e Implementación de Políticas de cifrado para correo saliente.
- Integración de políticas de DLP de correo con la solución de cifrado de correo saliente.
- Pruebas de Control de Contenido Web para garantizar el cumplimiento de la Política del Uso Aceptable del Internet.
- Pruebas de cifrado de correo saliente.
- Pruebas de cumplimiento de políticas DLP a nivel de los vectores Web y Correo.
- Pruebas de cumplimiento de políticas DLP a nivel del vector Endpoints.

1.3.6 Administración y Presentación de Informes

Dentro de la Administración y Presentación de Informes se realizó un resumen ejecutivo de los incidentes de Fuga de Información por nivel de severidad y acción tomada. Dicho resumen ejecutivo se puede apreciar en la Figura 1.12, donde podemos mencionar los incidentes por nivel de severidad y por acción tomada.

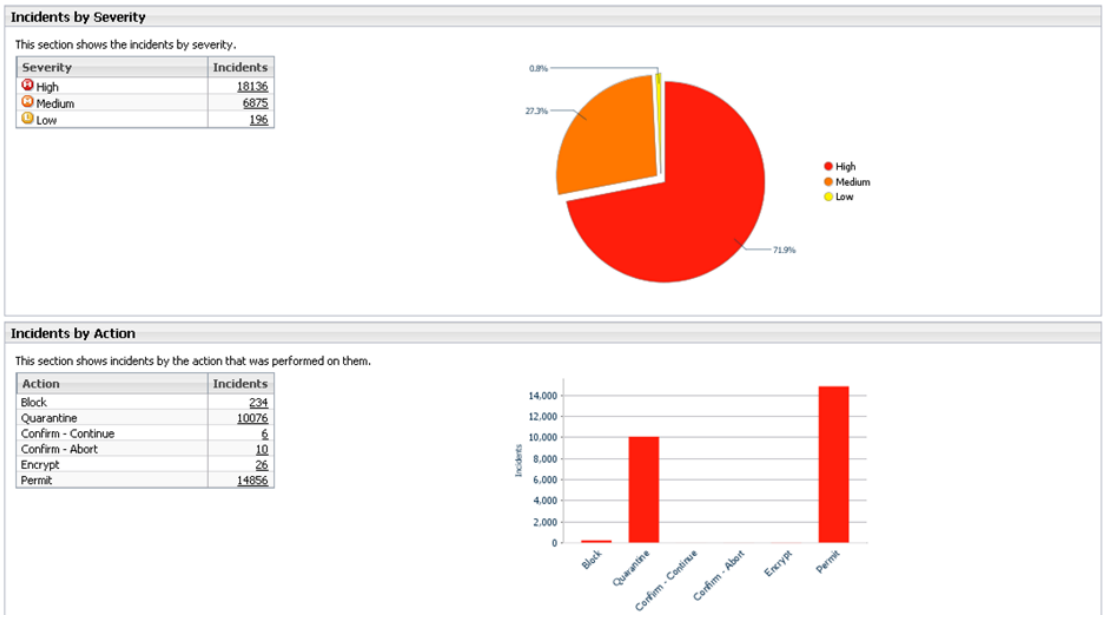


Figura 1.12: Administración de informes.

CAPÍTULO 2

2. RESULTADOS OBTENIDOS

Los resultados obtenidos del proyecto fueron los siguientes:

- Diseño de una solución de Control de Contenido Web, Correo, Cifrado de Correo y DLP de los vectores Web, Correo y Endpoints.
- Diseño e Implementación de Políticas de Uso Aceptable del Internet dentro de la organización para proteger la navegación a Internet de los usuarios.
- Diseño e Implementación de Políticas de Control en Redes Sociales como Facebook, Twitter, Linkedin.
- Diseño e Implementación de Políticas de Control de Videos en YouTube.
- Diseño e Implementación de políticas de Antispam para proteger el servidor de correo.
- Diseño e Implementación de políticas de cifrado para correo saliente.
- Detección de fuga de información confidencial a través de los vectores Web, Correo y Endpoints.

- Diseño e Implementación de políticas de Prevención de Fuga de Información a través de los vectores Web, Correo y endpoints.
- Cumplimiento con normativas internacionales de protección de tarjetas de crédito PCI-DSS.
- Implementación de Gateways de Control de tráfico HTTP, HTTPS, FTP, SMTP.
- Generación de informes y presentación de resultados.

2.1 Diseño de la Solución

En base al reporte de las estadísticas del firewall de la organización, donde se detectó que el 90% del tráfico correspondía a protocolos HTTP, HTTPS y SMTP se realizó un diseño de ingeniería enfocado a proteger tráfico HTTP, HTTPS y SMTP. El resto de protocolos fueron bloqueados a nivel del Firewall Perimetral y se enrutó todo el tráfico HTTP, HTTPS y SMTP a Gateways de Red que realizarían las funcionalidades de inspección de contenido Web, Correo, Cifrado de Correo y DLP.

Para garantizar la disponibilidad de la navegación Web, así como del correo corporativo se incluyó como parte del diseño un clúster de 2 equipos Activo-Pasivo para cada servicio. El cluster funciona con el protocolo VRRP [2] garantizando que el equipo Activo siempre tenga la IP Virtual.

Los componentes de la solución tal como se indica en la Figura 2.1 y en el ANEXO del fabricante Websense son los siguientes:

- Consola de Administración de la Solución Triton Enterprise.

- 1 Cluster de 2 Gateways V5000 Activo-Pasivo para Control de Contenido Web y DLP Web.
- 1 Cluster de 2 Gateways V5000 Activo-Pasivo para Control de Correo y DLP Correo.
- Agente de Software para control de DLP en 600 PCs que tienen sistema operativo Windows.
- Suscripción de Software Triton Enterprise para 600 usuarios.

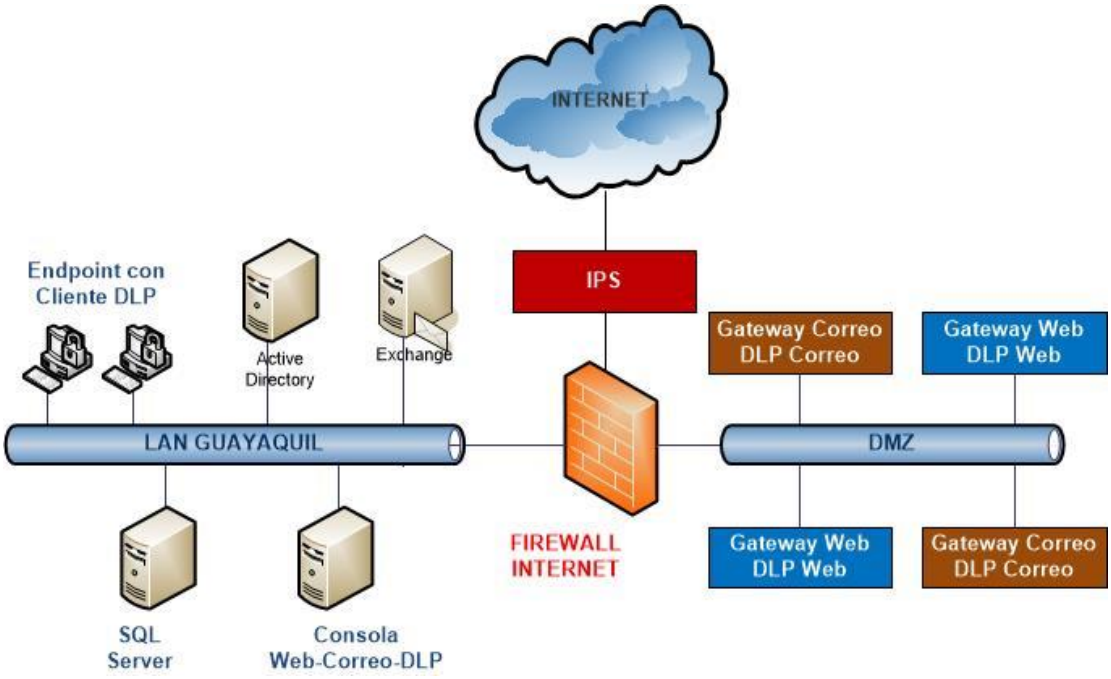


Figura 2.1: Diagrama de la Solución Implementada.

2.2 Diseño de Políticas

En base al análisis de las necesidades de la organización y del tráfico saliente de la organización se realizó el diseño de políticas para los vectores Web, Correo y Prevención de Fuga de Información.

2.2.1 Políticas de Seguridad de Contenido Web.

De acuerdo a las necesidades de la organización se crearon las políticas de control de navegación, tal como se indica en la Figura 2.2:

- **Política Default.** Se restringió el acceso a la navegación de páginas con contenido pornográfico, material adulto, apuestas, categorías de riesgos de seguridad, control de ancho de banda, herramientas peer to peer (Bit Torrent, Emule, Kazza).
- **Política de Protocolos.** Permite el acceso a herramientas de mensajería instantánea como Skype, Windows Live Messenger.
- **Política VIP.** Permite el acceso a redes sociales como Facebook, Twitter, Linkedin, YouTube.

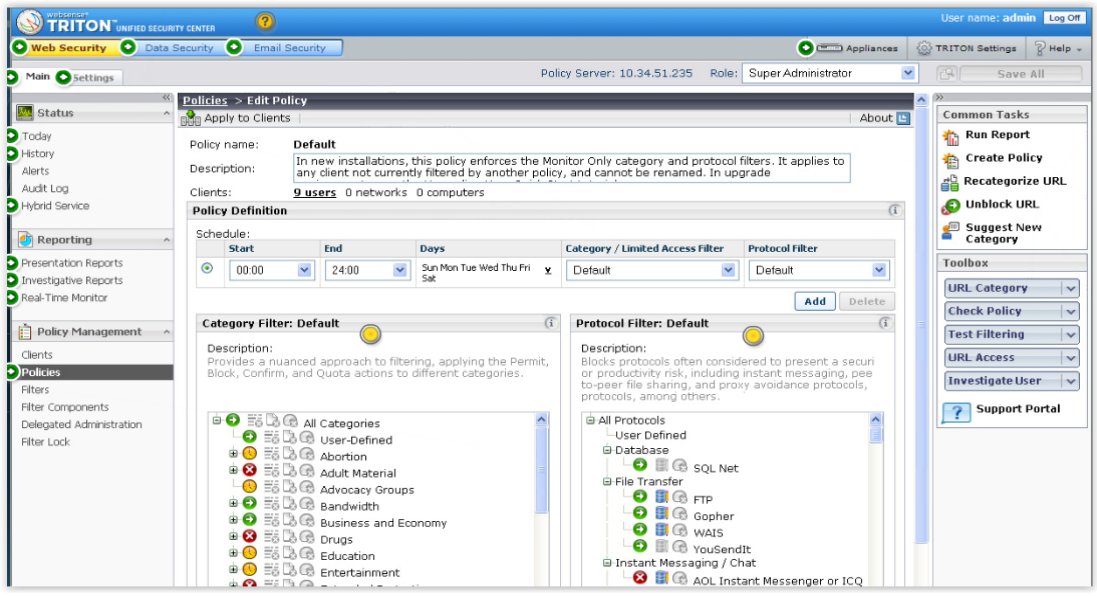


Figura 2.2: Políticas de control de contenido

2.2.2 Políticas de Seguridad de Correo.

Se realizaron definiciones de Políticas para todo el Correo Corporativo saliente y entrante, enfocados en garantizar el servicio de correo, tal como se indica en la Figura 2.3. Dichas políticas incluyeron:

- Protección del correo saliente hacia el Internet
- Cambio en los registros MX [7] para direccionar el tráfico entrante hacia la nube del proveedor.
- Políticas para cifrado de correo saliente que contenga información de números de tarjetas de crédito.
- Políticas de Prevención de Fuga de Información integradas con cifrado de correo saliente que contenga información confidencial.

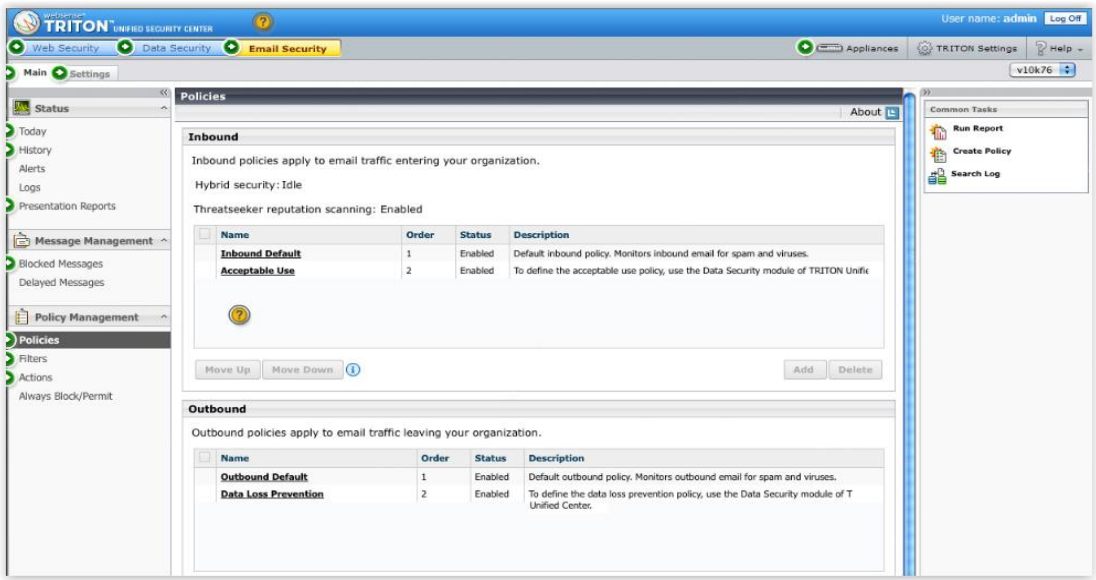


Figura 2.3: Políticas de Seguridad de Correo

2.2.3 Políticas de Prevención de Fuga de Información.

Se realizaron definición de Políticas de Prevención de Fuga de Información para proteger los números de tarjetas de crédito en los vectores Web, Correo y PCs. En la Figura 2.4 se puede notar las diferentes plantillas de Prevención de Fuga de Información que están configuradas, dentro de las cuales se incluye la de cumplimiento PCI-DSS [1].

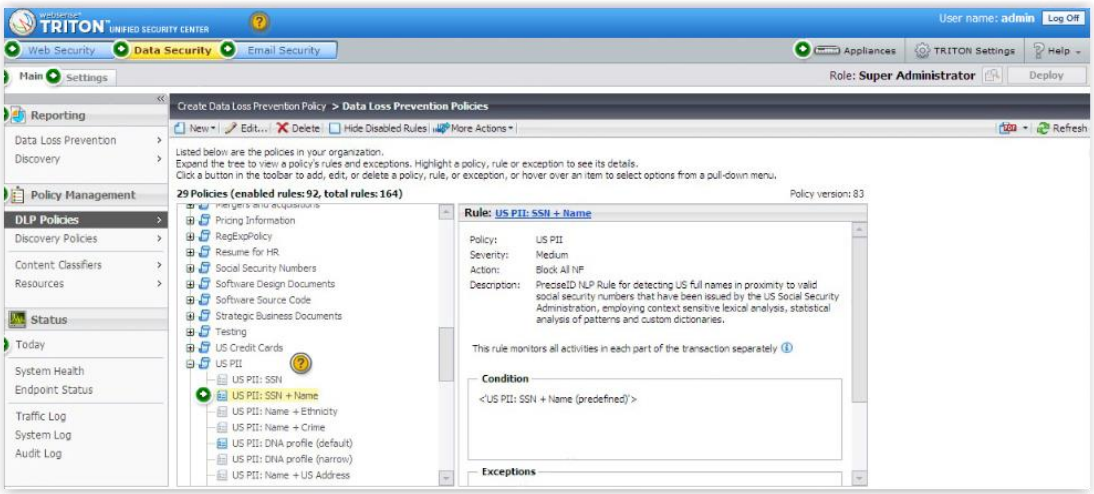


Figura 2.4: Políticas de Prevención de Fuga de Información

Las políticas de la organización se configuraron de acuerdo al detalle de la Tabla 1. El objetivo principal de las políticas fue proteger la Fuga de Números de Tarjetas de Crédito a través de los vectores Web, Correo y PCS:

Área de la Organización	Información	Destino	Canal de Transmisión	Acción
Toda la Organización	Números de Tarjetas de Crédito	Respaldo Personal Web	Web	Bloquear
Financiero/ Legal	Números de Tarjetas de Crédito	Socio de negocios	Correo Corporativo	Cifrar
Servicio al Cliente	Números de Tarjetas de Crédito	USB/CDs	Medios Removibles	Cifrar
Toda la Organización	Números de Tarjetas de Crédito	Imprimir/PC	Impresora/Print Screen	Bloquear

Tabla 1: Listado de Políticas

2.3 Generación de Informes

Después de implementadas y probadas las políticas de Seguridad de Control de Contenido Web, Seguridad de Correo y Prevención de Fuga de la Información en los vectores Web, Correo y PCs se realizó la generación de informes de los diferentes módulos de la solución para comprobar el correcto funcionamiento.

2.3.1 Informe de Seguridad de Control de Contenido Web.

Los informes de Seguridad de Control de Contenido incluyeron:

- Categorías principales bloqueadas por tipo de tráfico. Tal como se muestra en el Figura 2.5, la categoría de Productividad es la que tiene mayor cantidad de tráfico HTTP y HTTPS.
- Categorías principales bloqueadas por tiempo de navegación. En la Figura 2.6 se muestra que la mayor cantidad de tráfico bloqueado corresponde a Redes Sociales y Social Networking.
- Reportes investigativos. En la figura 2.7 se muestra un reporte investigativo por tipo de URLs clasificadas como riesgo alto.

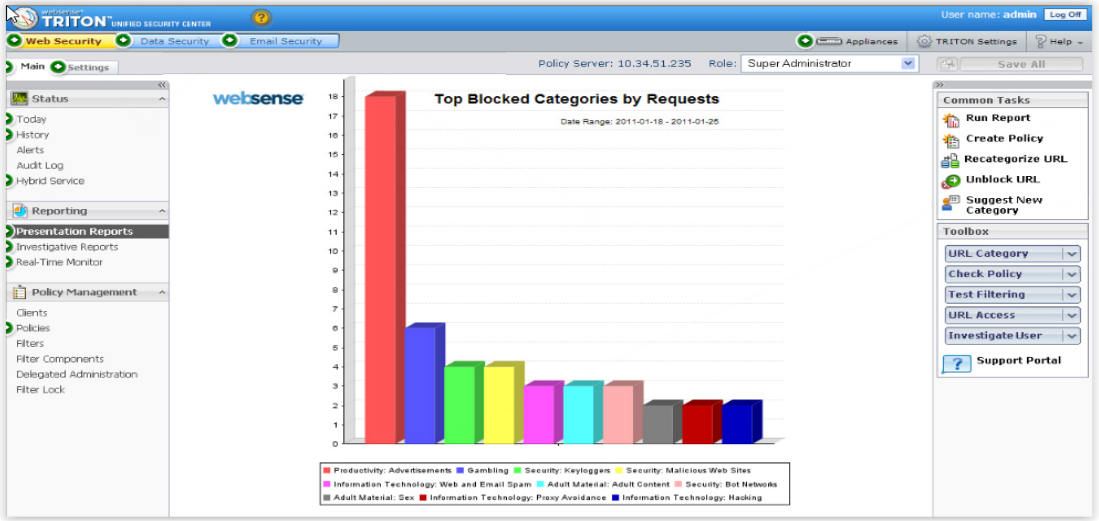


Figura 2.5: Categorías principales bloqueadas por usuarios.

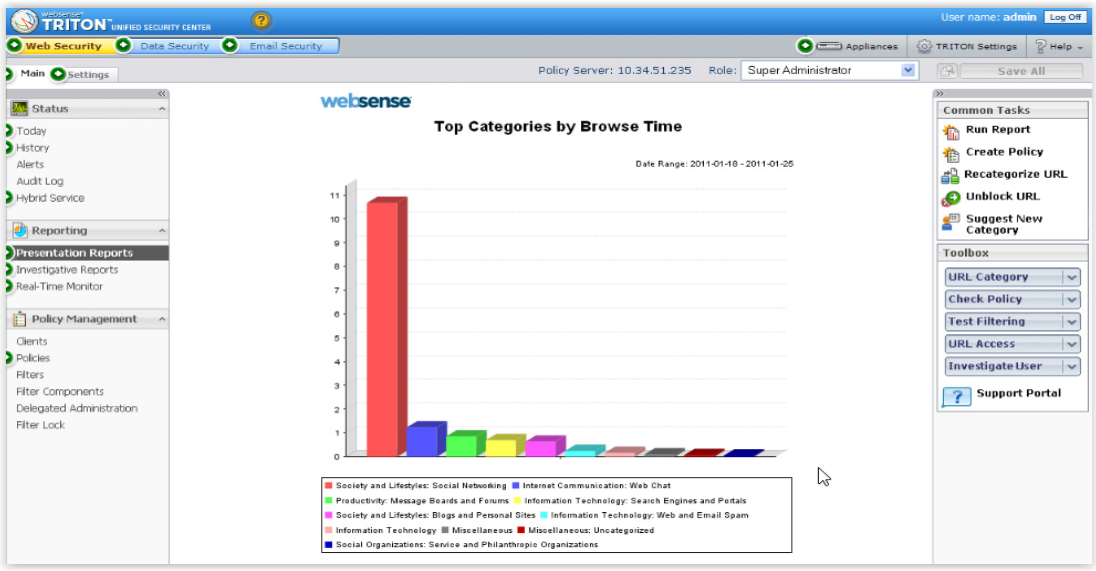


Figura 2.6: Categorías principales bloqueadas por tiempo de navegación.

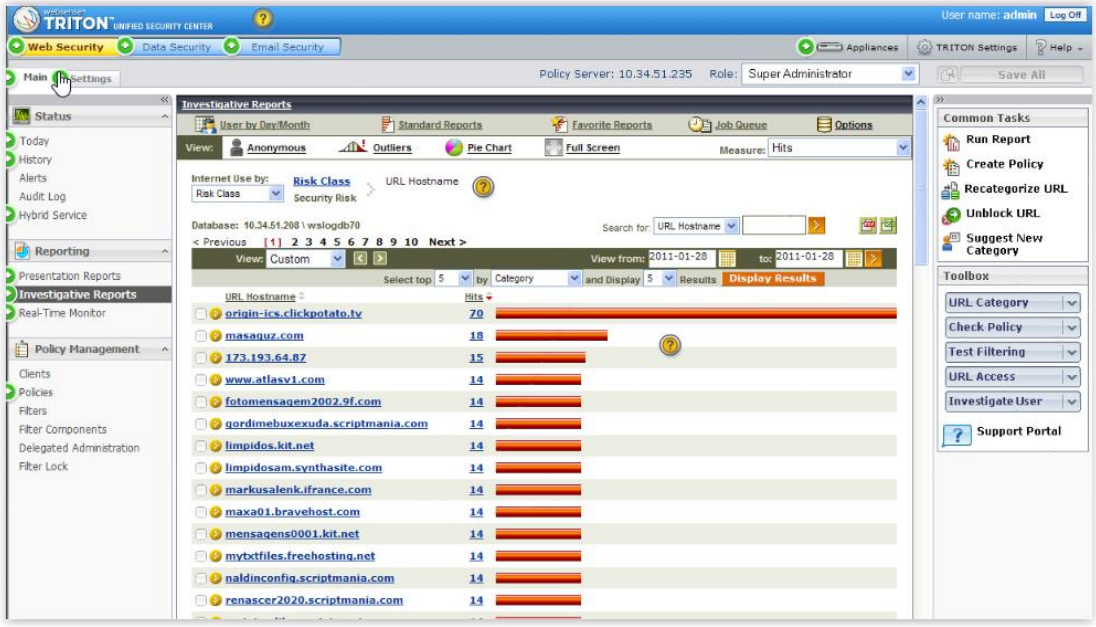


Figura 2.7: Reportes Investigativos.

2.3.2 Informe de Seguridad de Correo.

El informe de la Figura 2.8 de Seguridad de Correo incluyó el reporte principal de virus detectados.

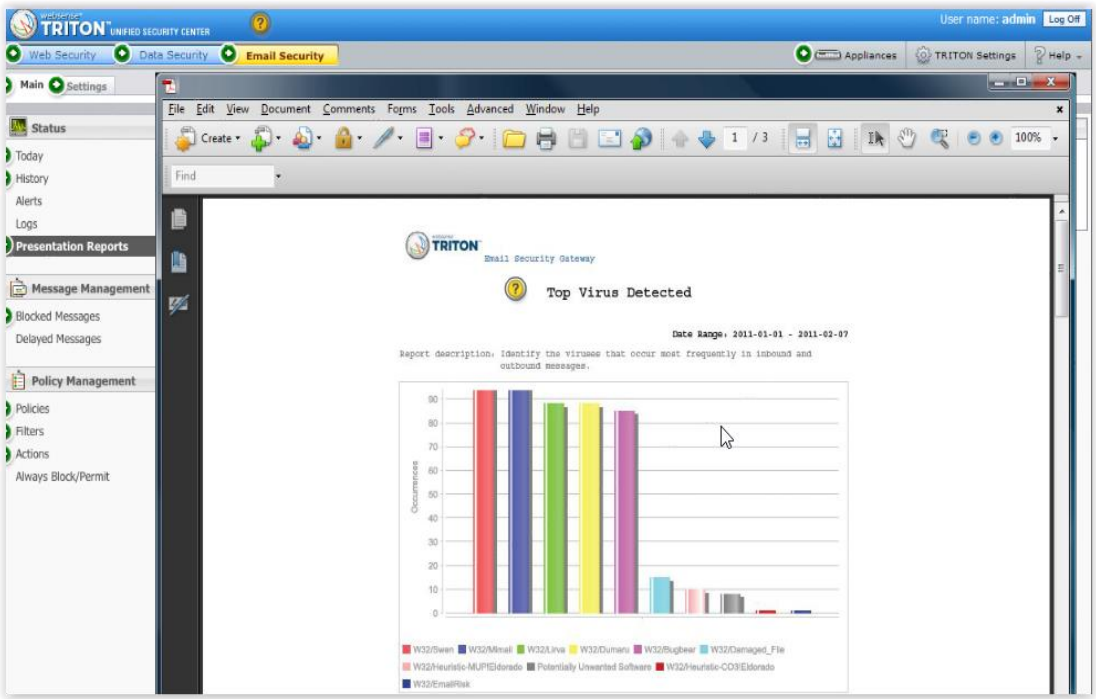


Figura 2.8: Informe de Seguridad de Correo

2.3.3 Informe de Prevención de Fuga de Información.

Los informes de Prevención de Fuga de Información incluyeron:

- Listado de incidentes. En la figura 2.9 se muestra el detalle de incidentes de acuerdo a los siguientes parámetros: política infringida, canal, destino y nivel de severidad.

- Resumen Ejecutivo de eventos. En la figura 2.10 se muestra el resumen ejecutivo de eventos por nivel de riesgo y acción ejecutada.
- Tendencias de incidentes. En la figura 2.11 se muestra la tendencia de incidentes de fuga de información, donde se detalla que conforme la herramienta aumenta en su periodo de funcionamiento los niveles de incidentes bajan drásticamente en la organización.

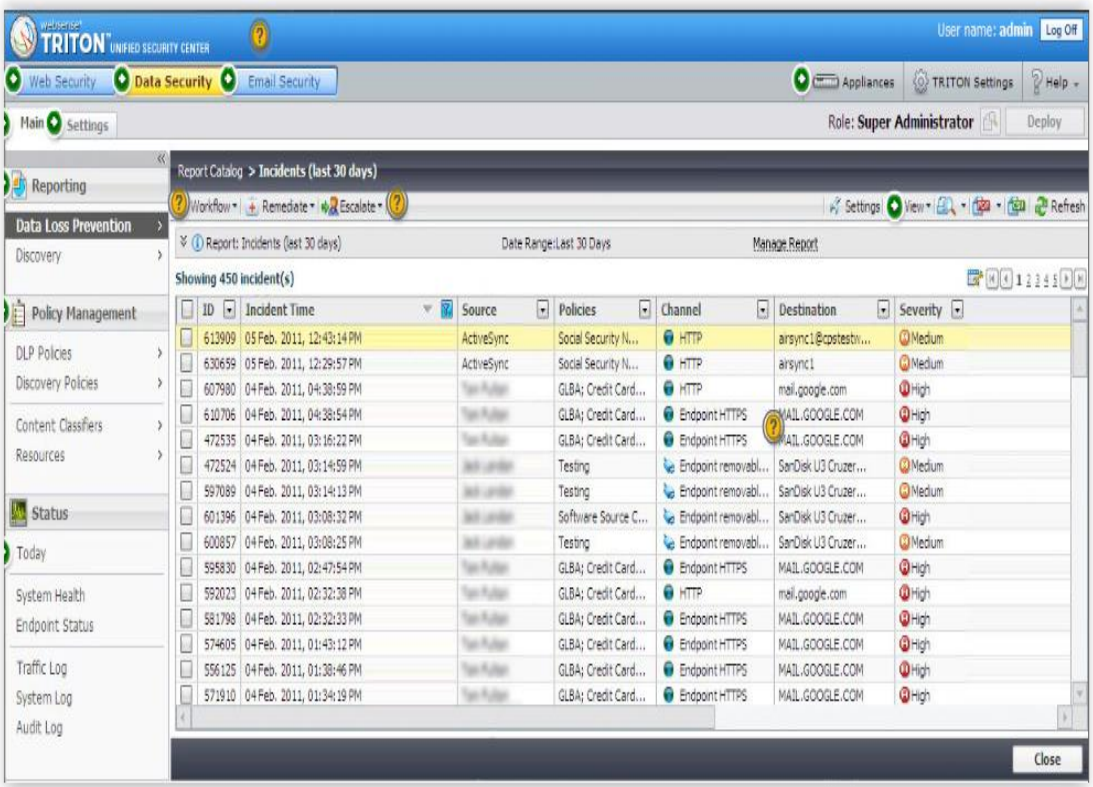


Figura 2.9: Listado de Incidentes

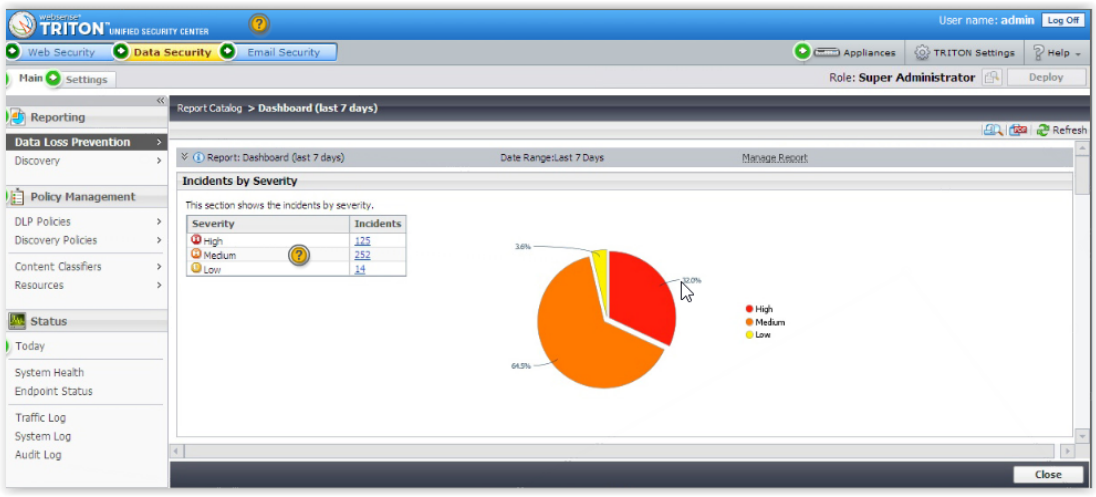


Figura 2.10: Resumen Ejecutivo de Eventos

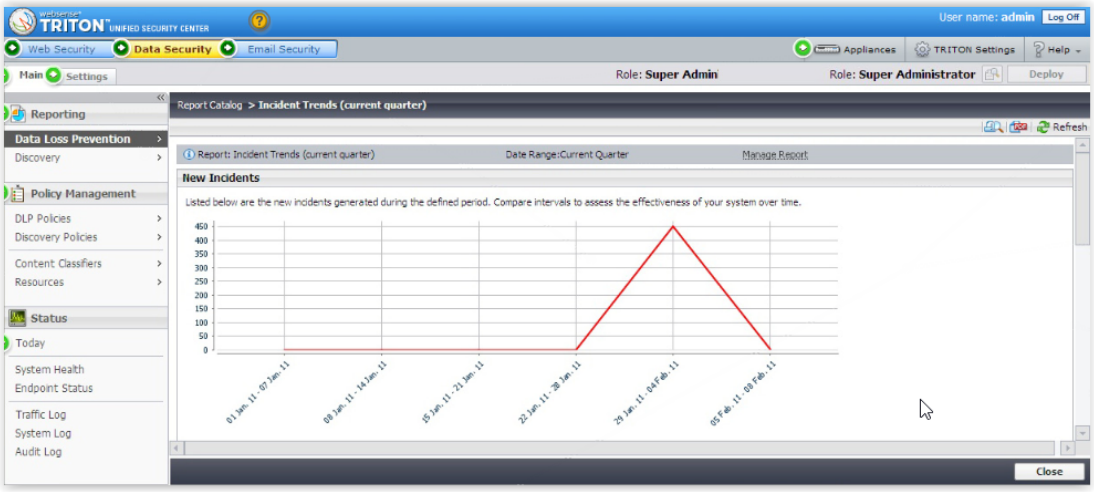


Figura 2.11: Tendencias de Incidentes.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. Las organizaciones requieren de soluciones de Prevención de Fuga de Información que permitan proteger la información confidencial o sensible contra ataques internos o externos.

2. La base de una buena implementación de una solución de Prevención de Fuga de Información radica en un conocimiento completo del flujo de información confidencial a través de los diferentes protocolos de red y activos de seguridad de la información.

3. En base al conocimiento del flujo de información confidencial se elaboran estrategias de protección de la información confidencial. Dicha estrategia debe ser cambiante y dinámica debido a que las necesidades de las organizaciones varían con el tiempo, por lo que un proyecto de Prevención de Fuga de Información no puede ser estático y está supeditado a las necesidades del negocio.

4. Dado que las soluciones de Prevención de Fuga de Información se instalan sobre la infraestructura de la organización, es mandatorio reforzar las plataformas y activos de seguridad de la información con herramientas enfocadas a proteger los vectores principales de tráfico como son los protocolos HTTP, HTTPS, SMTP y aplicaciones en estaciones de trabajo.

5. Un proyecto de Prevención de Fuga de Información afecta directamente la forma como la organización maneja su información confidencial o sensible, por lo que es importante tener un sponsor del proyecto que se reúna con todas las áreas del negocio para establecer prioridades en cuanto a la implementación de una política de Prevención de Fuga de Información.

6. Las organizaciones financieras en especial las que procesan, almacenan y/o transmiten datos de tarjetahabientes (números de tarjetas de crédito) requieren de forma mandatoria soluciones de Prevención de Fuga de Información para cumplir como normativas internacionales como PCI-DSS [1], las cuales radican fundamentalmente en la protección del número de tarjeta de crédito contra un atacante externo o interno.

7. Se cumplió con el objetivo principal de la organización de proteger los números de tarjetas de crédito en los vectores Web, Correo y PCs, así como la protección de los usuarios frente a amenazas en la navegación Web y correo corporativo.

8. Las tecnologías implementadas como parte de la solución basan su funcionamiento en el análisis del tráfico de protocolos HTTP, HTTPS, SMTP y

en la utilización de tecnologías de Fingerprinting para detección de archivos mediante la función HASH.

Recomendaciones

1. Es necesario en vista de la exposición de las empresas del sector financiero, gobierno o del sector comercial, una estrategia para proteger la información confidencial o sensible que estas organizaciones poseen. De esta necesidad de proteger la información sensible o confidencial nace la recomendación de tener estrategias de protección de la información para evitar que la misma caiga en manos de un atacante.
2. En función de que es imposible implementar un proyecto de Prevención de Fuga de Información en toda la organización al mismo tiempo, se recomienda iniciar con las áreas más importantes de la organización a manera de un pequeño piloto. Una vez que el piloto se encuentre completamente funcional se puede extender el proyecto de Prevención de Fuga de Información a las diferentes áreas de la organización.
3. Se recomienda realizar un levantamiento inicial de los activos de seguridad de la información, así como diagramas de red, equipos de seguridad y networking para reutilizar las infraestructuras existentes en la organización.
4. Como parte integral de todo proyecto de Seguridad de la Información, se recomienda realizar en toda organización campañas de educación y concientización, enfocadas a preparar a los empleados frente al uso de información confidencial o sensible de la organización. Con esta recomendación se disminuirá el riesgo de exposición de la organización frente a

ataques de ingeniería social [10], los cuales tienen como objetivo conseguir información confidencial de forma maliciosa.

5. En vista del creciente uso de los smartphones y tablets, así como del riesgo de la pérdida de los mismos, se recomienda proteger los correos que se descargan en estos dispositivos, de tal forma que se evite la sincronización de correos confidenciales.
6. De la misma forma se recomienda extender los vectores de cobertura de fuga de información a los vectores de mensajería instantánea y servidores de escaneo OCR.

BIBLIOGRAFÍA

[1] PCI-DSS.
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3_05Nov13_Final_ES-LA.pdf .

[2] Content Filtering
Michael Whitman and Herbert Mattord, Principles of Information Security, Cengage Learning 4th Ed, 2012

[3] Categorías de control de contenido Web.
http://www.websense.com/content/websense-url-categories.aspx

[4] Antispam
Simson Garfinkel and Gene Spafford, Web Security, Privacy & Commerce, O´Reilly Media Ic 2nd Ed, 2002.

[5] Antivirus.
Gustavo Talaván, PC Como usarla en forma segura, Imaginador 1era Ed, 2006.

[6] Mail Transfer Agent (MTA).
David Wood, Programming Internet Email, O´Reilly 1st Ed, 1999.

[7] Registro MX
José María Barceló Ordinas y Jorgi Íñigo Griera, Protocolos y Aplicaciones Internet, UOC 1era Ed, 2008

[8] Solución de Prevención de Fuga de Información.
Asaf Shabtai and Yuval Elovici and Lior Rokach, A Survey of Data Leakage Detection and Prevention Solutions, Springer 1st Ed, 2012.

[9] Huella Digital (Fingerprinting)
Asaf Shabtai and Yuval Elovici and Lior Rokach, A Survey of Data Leakage Detection and Prevention Solutions, Springer 1st Ed, 2012.

[10] Ingeniería Social
Christopher Hadnagy, Ingeniería social. El arte del hacking personal, Anaya Multimedia-Anaya Interactiva 1st. Ed, 2011.

[11] Web Mining.
Anthony Scime, Web Mining: Applications and Techniques, Idea Group 1st Ed, 2005.

[12] Man in the middle

David Kim and Michael G. Solomon, Fundamentals of Information System Security 2nd Ed, 2014.

[13] Función Hash
Stallings, Data and Computer Communications 8th Ed, 2007.

[14] VRRP
Ayikudy Srikanth and Adnan Onart, VRRP: Increasing Reliability and Failover with the Virtual Router Redundancy Protocol 1st Ed, 2002.

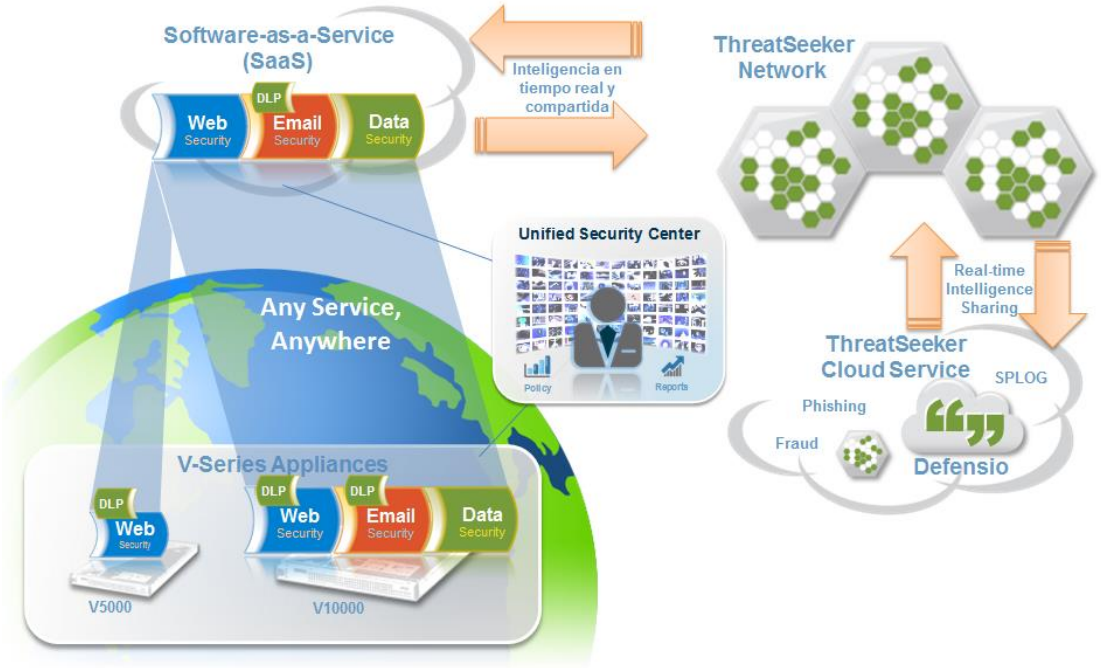
ANEXOS

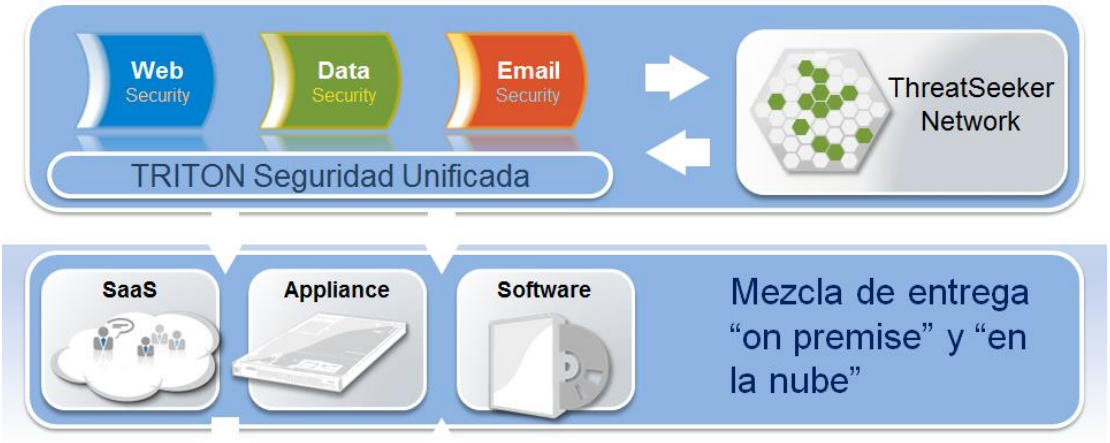
GATEWAYS DE SEGURIDAD WEB, CORREO Y DLP

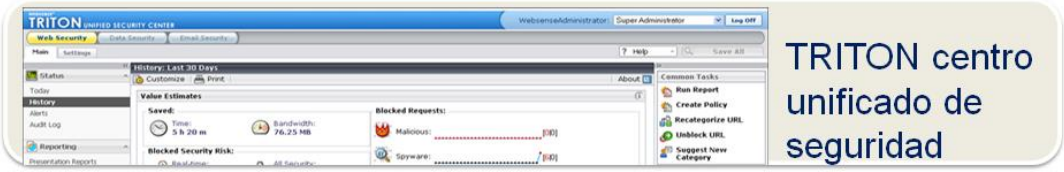
HARDWARE SPECIFICATIONS	
MAX USERS/APPLIANCE: 2,000	**DIMENSIONS:** 1U form factor, 15.5"D x 17.1"W x 1.67"H (39.5cm D x 43.43cm W x 4.24cm H)
PROCESSOR: Quad-core HT Xeon	**HARDWARE SUPPORT:** Globally available 24/7 by phone; next business day on-site included; 4-hour on-site optional.
MEMORY: 8GB RAM, 2* SATA (500GB total)	**REGULATORY & COMPLIANCE:** FCC / ICES / EN55022 / VCCIBSMI / C-Tick / SABS / CCC / MIC Class A and UL60950-1 / Verified to comply with RoHS Directive / Energy consumption and noise emissions in accordance with ISO 9296
INTERFACE: 4 * 10/100/1000 Base-T	
POWER SUPPLY: 250W	
WEIGHT: 27 lbs (12.25kg)	

Possible Software Combinations for V5000 Appliance	Web Security			Email Security	
	Web Security Gateway Anywhere	Web Security Gateway	Web Security	Email Security Gateway Anywhere	Email Security Gateway
Web Security					
Option 1	X				
Option 2		X			
Option 3			X		
Email Security					
Option 1				X	
Option 2					X
Web & Email Security					
Option 1			X	X	
Option 2			X		X

SOFTWARE TRITON ENTERPRISE FABRICANTE WEBSENSE







COMPONENTES SOFTWARE TRITON ENTERPRISE