UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

IMPLEMENTAR DISPOSITIVOS DE SEGURIDAD PARA EL FILTRADO DE CORREO ELECTRÓNICO UTILIZANDO McAfee Email Gateway (MEG) PARA BANCO WAL-MART

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniero en Computación

P R E S E N T A

Rubén de Jesús Díaz Sánchez

ASESOR DE INFORME

Ing. Gabriela Camacho Villaseñor

Ciudad Universitaria, Cd. Mx., 2016

Índice

INTRODUCCIÓN

El presente es un reporte del proyecto mediante el cual Banco Wal-Mart asegura que su correo electrónico está protegido, de posibles ataques y pérdida de información, gracias al uso de tecnologías de calidad que filtran cada correo entrante y saliente.

El proyecto constó de la integración de dos dispositivos McAfee Email Gateway, en sus versiones 5000 y 4500.

Este trabajo presenta los siguientes capítulos:

En el capítulo I se presenta el planteamiento de la investigación, desde que es el McAfee Email Gateway, sus alcances y limitaciones, además de los antecedentes necesarios para el proyecto.

En el capítulo II se abordan los aspectos relacionados a la empresa, la importancia de tener un área de Seguridad de la Información y el puesto que he desempeñado durante mi estancia en esta empresa.

En el capítulo III Se aborda la implementación de los dispositivos MEG en sus dos versiones 5000 y 4500 (producción y desarrollo respectivamente) y planeación de directivas.

En el capítulo IV se presentan los inconvenientes que salieron cuando el dispositivo ya estaba en producción, las pruebas realizadas para atender dichos problemas y las recomendaciones.

En el capítulo V se presentan las conclusiones del proyecto.

Se debe tener especial atención en el correo electrónico debido a que se ha convertido en uno de los servicios más importantes para el correcto funcionamiento de cualquier entorno empresarial, hoy en día, su capacidad para distribuir de manera instantánea una amplia variedad de volúmenes de información lo convierten en una herramienta básica y en un constante desafío para la seguridad.

Examinemos los problemas de seguridad críticos del correo electrónico a los que se enfrentan las empresas en la actualidad:

- Los ataques a través del correo electrónico entrante son cada vez mayores. Estos ataques se sirven de sofisticadas técnicas de ingeniería social y evolucionan con rapidez.
- El correo electrónico es uno de los principales puntos de pérdida o robo de datos confidenciales, ya sea por un simple descuido o por una acción malintencionada de algún empleado.
- Debido a su importancia operativa y a su gran vulnerabilidad, el correo electrónico se ha visto sometido al control de las entidades reguladoras tanto políticas, como comerciales.
- Cerca del 75 % del volumen global de correo electrónico es spam, con diferencias marcadas entre países y empresas.
- Los ataques de phishing son cada vez más selectivos y efectivos, y están más orientados a obtener datos financieros, McAfee identificó cerca de 2250 URL maliciosas al día en el cuarto trimestre de 2013, y esta cifra se ha ido aumentando con el pasar del tiempo.

La consecuencia inevitable es que la mayoría de organizaciones que usan TI se ven obligadas a invertir demasiado tiempo, dinero para evitar que haya fugas de información confidencial en la organización, demostrando que cumplen las normativas.

Es por ello que el área de Seguridad de la Información de Banco Wal-Mart se encomendó a la tarea de Implementar una herramienta que brinde protección y sobre todo que se adecue a las necesidades del negocio, denominada McAfee® Email Gateway, por sus siglas MEG.

Esta herramienta ayuda a reforzar la seguridad del correo electrónico y a fortalecer las defensas protegiendo contra las amenazas entrantes, salientes, prevención de pérdida de datos, cifrado, funciones avanzadas de cumplimiento de normativas y administración centralizada en un solo dispositivo de fácil despliegue.

OBJETIVOS

Implementar dispositivos de filtrado de correo utilizando McAfee Email Gateway contra amenazas y vulnerabilidades en Banco Wal-Mart.

Objetivos Particulares

- Crear políticas de seguridad, para el manejo óptimo del dispositivo.
- Crear “listas de confianza” de usuarios y dominios para mitigar el riesgo que representa el correo electrónico.
- Crear grupos de trabajo especializado utilizando directorio activo.
- Actualizar el correo electrónico de la empresa.
- Generar reportes, para simplificar las cargas de trabajo, administración, y reducción de costos.

I. MARCO TEÓRICO

En este capítulo podremos ver el planteamiento de la herramienta, y para ello desde que es el McAfee Email Gateway, sus alcances y limitaciones, además de los antecedentes necesarios para poder cubrir el proyecto.

I.1 Definición de McAfee Email Gateway (MEG)

Es un dispositivo de puerta de enlace de seguridad de correo electrónico y gestión de contenidos, que proporciona protección entrante y saliente a la empresa, es una herramienta fácil de implementar y de utilizar, en la ilustración I.1 se encuentra la presentación del producto.

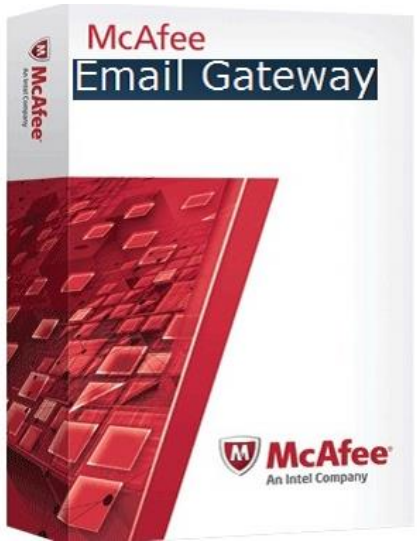


Ilustración I.1 Producto McAfee Email Gateway

Las corporaciones de hoy deben hacer frente a peligros relacionados con sus redes de correo electrónico como:

- Spam [17] correo electrónico no solicitado que es enviado en cantidades masivas a un número muy amplio de usuarios generalmente con el fin de comercializar, ofertar o tratar de despertar el interés con respecto a algún producto o servicio.

- Phishing [16] consiste en el envío de correos electrónicos que, aparentando provenir de fuentes fiables (por ejemplo, entidades bancarias), intentan obtener datos confidenciales del usuario, que posteriormente son utilizados para la realización de algún tipo de fraude.

- Suplantación [11] Ocupar el lugar de otra persona ilegalmente o hacerse pasar por ella contra su voluntad para obtener un beneficio.

- Virus [11] Es un programa que posee la capacidad de crear duplicados de sí mismo, en ocasiones introduciendo ligeras variaciones, y distribuirlos a través de un sistema, para causar un daño.

- Negación de servicio (DoS) [11] tienen como objetivo saturar los recursos de la víctima de forma tal que se inhabilita los servicios brindados por la misma.

Estas amenazas no sólo pueden causar enormes gastos, sino también cuantiosas pérdidas a las empresas.
Con MEG, las empresas pueden ofrecer una protección superior del correo electrónico y documentarla con informes personalizables, paneles de estado en tiempo real y alertas, sin cargo adicional, cuenta con funciones de encriptación y de prevención de pérdida de datos (DLP) [22].

El dispositivo actúa como un sistema firewall específico para cada aplicación, donde un **firewall [1]** es una colección de componentes colocados entre una red interna y una red externa para que solo el tráfico que es autorizado pase. Sólo permite las conexiones válidas y seguras a los servidores de correo electrónico.

En su carácter de proxy, examina cada intento de conexión para detectar y bloquear todas las conexiones que, conocidas o no, puedan causar perjuicios, como se puede observar en la ilustración I.2.

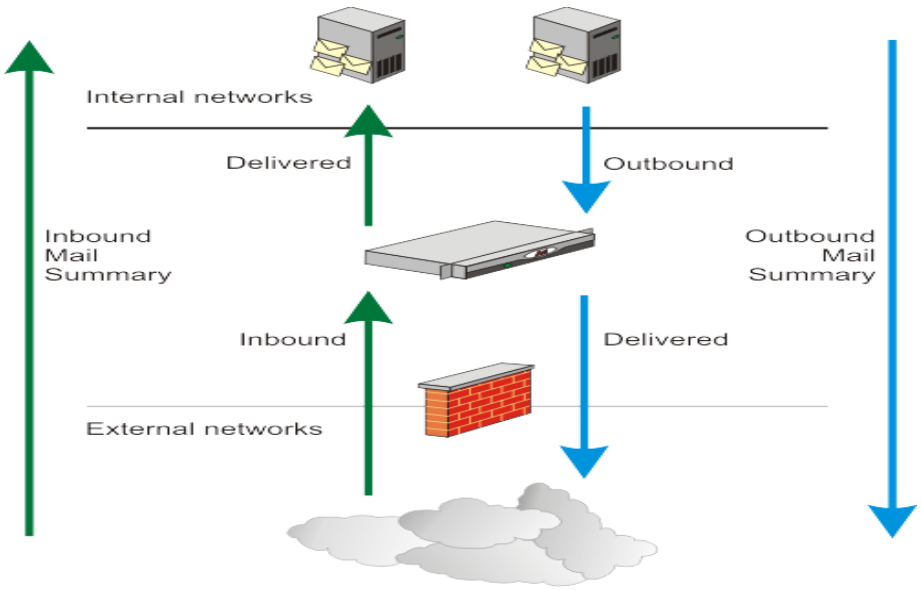


Ilustración 1.2 MEG como Firewall

Proporciona un motor IDS [1] (sistema de detección de intrusos) que examina en tiempo real todo el tráfico de la red que fluye a través de los puertos de correo, uno de sus principales servicios es a través de **protocolo simple de transferencia de correo** (SMTP).

Una sesión SMTP [25] consiste en comandos originados por un cliente SMTP (el agente de inicio, emisor o transmisor) y las respuestas correspondientes del SMTP del servidor (el agente de escucha, o receptor) para que la sesión se abra y se intercambian los parámetros de la sesión a través de TCP puerto 25 (SMTP) o el puerto 587 (Presentación), las especificaciones y muchos servidores soportan ambos. Aunque algunos servidores soportan el puerto 465 para el legado SMTP seguro.

Los protocolos que se utilizan actualmente para correo electrónico exigen que todos los mensajes transmitidos por Internet se envíen en caracteres de texto simple ASCII. El problema causado por este requisito es que cualquier persona con las herramientas adecuadas puede leer un mensaje enviado por otra persona. Las herramientas no sólo permiten a los hackers leer los correos electrónicos de cualquier persona, sino que también les permiten interceptar y alterar los menajes

antes de que lleguen a su destino. La manera más fácil y popular que tienen las empresas de asegurar los mensajes de correo electrónico es utilizando certificados digitales.

Estos certificados permiten dos estrategias esenciales para el cifrado de los mensajes: puede ser "de cliente a cliente" y "de servidor a servidor".

En el cifrado de cliente a cliente, los certificados de seguridad se instalan en las estaciones de trabajo individuales. El mayor beneficio de este método es que el mensaje se cifra antes de salir de la computadora donde se origina y se mantiene cifrado hasta que es recibido (protección de principio a fin).

Por su parte, en el cifrado de servidor a servidor, se requiere que los certificados de seguridad se instalen en los servidores de correo. Los mensajes se protegen sólo de servidor a servidor, no desde el cliente al servidor, la estrategia de un MEG ofrece los beneficios del cifrado de Servidor a Servidor.

I.1.1 Dispositivos de hardware [13]

La flexibilidad de implementación es un sello distintivo de McAfee Email Gateway, ya que puede ser instalado como equipo virtual, o como dispositivo de hardware en cualquiera de sus *cuatro tamaños distintos EG-4000, EG4500, EG5000 y EG5500*, como se observa en la ilustración I.3, en el Anexo 1 encontraras las especificaciones físicas y técnicas de los dispositivos.

Ilustración I.3 Dispositivos Hardware

La manera en que trabaja se basa en la creación de normas y políticas de inspección, como podemos observar en la ilustración I.4.

Esta herramienta permite a los administradores crear una variedad de normas que controlen el uso del correo electrónico en la red, desde verificar si la dirección de correo electrónico o el dominio están permitidos o el análisis completo de los mensajes.

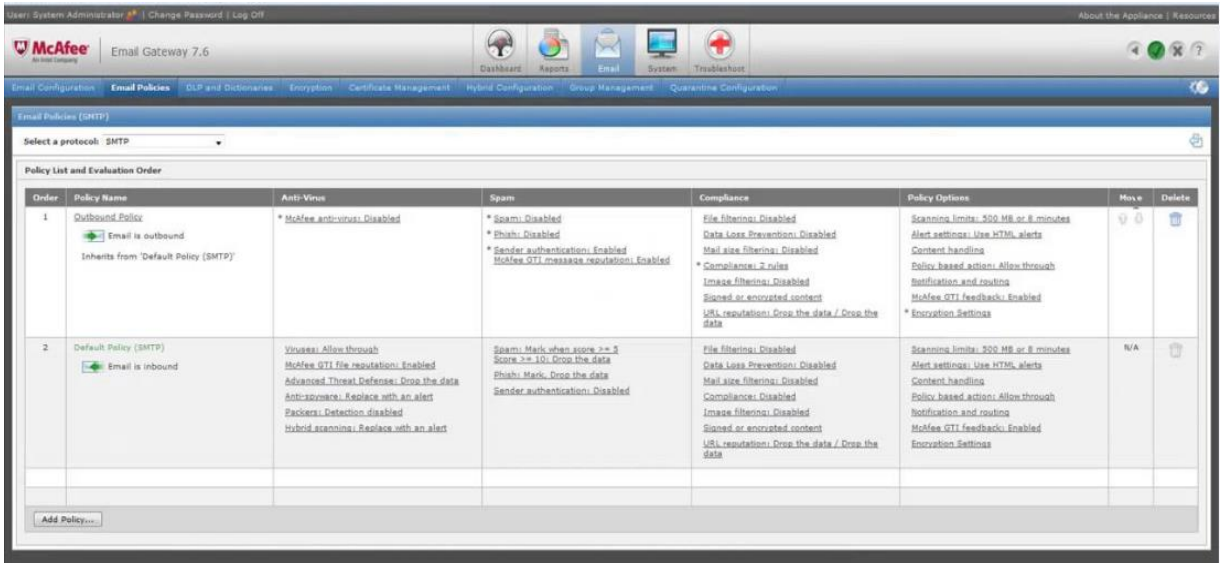


Ilustración I.4 Administrador de Políticas

Nota: Siempre se aplicarán las normas vigentes para el momento en que el mensaje llega al dispositivo, se examina cada correo electrónico que pasa por el equipo a fin de detectar amenazas.

Posee herramientas adicionales, como el filtrado de mensajes, colas y diccionarios, para bloquear los mensajes dañinos, ofreciendo muchas opciones para responder a los archivos o contenido no autorizados cuando éstos intenten ingresar a la red.

I.1.2 Colas de espera [13]

Los mensajes que pueden ingresar pasan por colas de espera que los preparan para ser inspeccionados. Las colas de espera son las siguientes:

- *La Cola de espera Separación*, que divide el mensaje de correo electrónico en sus partes lógicas (información de encabezado, asunto, cuerpo, adjuntos, etc.)
- *La Cola de espera Extracción de contenido*, que identifica los formatos y extrae texto del cuerpo del mensaje para que pueda ser analizado según las normas.

- La Cola de espera Reconstrucción es la última en procesar un mensaje de correo electrónico, y su tarea consiste en re ensamblar el mensaje. Si cualquiera de las colas anteriores realizó alguna acción—como reescribir una línea de Asunto o eliminar palabras ofensivas—re ensambla el mensaje con las partes editadas que están almacenadas en la base de datos y lo prepara para su entrega final.

Aunque las colas de espera no son entidades físicas como las particiones de disco, son subsistemas que procesan mensajes de una manera ordenada. Cada cola de espera “se activa” a intervalos periódicos para determinar si hay nuevos mensajes que procesar.

I.1.3 Diccionarios [13]

Incluye originalmente cinco diccionarios como opción predeterminada:

1. Pornografía
2. Confidencial
3. Sam
4. Código móvil malicioso
5. URL

Los administradores pueden crear tantos diccionarios como puedan requerir para aplicar normas, pero para ello se requiere tener conocimiento claro de las especificaciones de la empresa, para poder definir qué tan permisivos puede ser, también hay que contemplar los aspectos sociales, ya que dependiendo de la región y su vocabulario, podemos descartar palabras que en otras regiones o contextos sean motivo de bloqueo.

I.1.4 Supervisión de Mensajes [13]

El filtrado de mensajes permite al administrador configurar y aplicar reglas y normas para evitar que el contenido malicioso o que contenga alguna violación a los estándares establecidos por la empresa ingresen en la red.

La creación de normas de filtrado es un proceso que se realiza en dos pasos. Primero, deben crearse reglas de Filtrado, especificar cada tipo de archivo y la

respuesta que se dará a cada tipo de archivo. Segundo, las reglas deben aplicarse a los usuarios o grupos de usuarios— a fin de crear normas (véase Anexo 2 Mejores prácticas de Filtrado de Contenido).

Puede haber ocasiones en que un solo mensaje es marcado para una acción por más de una norma de supervisión de correo. Por lo tanto, se sigue un orden de prioridad:

1. Las normas que contengan reglas generadas por el sistema actúan en los mensajes antes que las normas que contienen reglas generadas por el usuario.
2. Las normas que se aplican a individuos tienen prioridad sobre las normas que se aplican a los miembros de un grupo.
3. La prueba final de prioridad se fundamenta en las acciones de la norma.
    - Re enrutar tiene la primera prioridad
    - Excluir
    - Colocar en cuarentena
    - Reenviar
    - Copiar, reescribir asunto y registrar. (Comparten el mismo nivel de prioridad porque ninguna de ellas impide la implementación de las demás.)

I.1.5 Filtrado de URL [13]

Las funciones de filtrado de URL son parte del filtrado de contenido que McAfee realiza a nivel global, pues basándose en las estadísticas de envió, recepción y reputación, es que pueden catalogar si un sitio representa un riesgo a los usuarios. Por tal motivo se encuentran disponibles en forma de diccionarios que contiene URL no permitidos, este diccionario es constantemente actualizado por McAfee, pero también se pueden ingresar datos de manera manual, colaborando de esta forma con McAfee, ya que al momento de que un usuario decide que el sitio es malo, la reputación de este puede comenzar a verse afectada. Cuando se analiza un mensaje

de correo electrónico, se tienen que buscar los URL que coincidan con las entradas del diccionario de URL y mantiene un contador de las apariciones.

I.1.6 Filtrado de mensajes cifrados [13]

El cifrado basado en clientes y las firmas digitales, además de constituir valiosos recursos que refuerzan la seguridad del correo electrónico, gracias al empleo de certificados digitales conocidos y firmados única y especialmente por la empresa se puede garantizar realmente provino del remitente indicado y que no fue manipulado durante la transmisión, también brindan protección contra virus, códigos maliciosos y contra las acciones de empleados inescrupulosos.

Una de las ventajas que se obtienen con la tecnología de un MEG es que se cuenta con un cifrado a nivel de dispositivo.

El hecho de aplicar el cifrado en el dispositivo, en lugar de en los equipos de usuarios, evita que tengan que determinar las necesidades de cifrado y acaba con el recurrente problema de que los usuarios olviden cifrar los datos confidenciales.

I.1.7 Bloqueo de spam [13]

Las herramientas del Gateway sólo bloquean los mensajes que consideren que son spam, basándose en puntuaciones, mismas que McAfee le va dando a cada parte de un mensaje, desde el encabezado, la cantidad de destinatarios, la frecuencia de envió, bien sea porque el mismo mensaje se ha entregado a miles de usuarios en todo el mundo o porque el encabezado del mensaje contiene palabras claves que se han detectado en la mayoría del spam conocido, el equipo ya cuenta con una configuración definida pero muy básica, y cuenta con un rango de calificaciones para spam bastante holgado, es trabajo de cada administrador configurar los parámetros de evaluación, ya que McAfee desconoce las necesidades de cada usuario o empresa.

Aun después de que la herramienta esté funcionando, surgirá inevitablemente la siguiente pregunta:

¿Por qué sigue entrando spam a mi red?

Algunos casos no serán detectados porque son muy recientes y no han circulado lo suficiente para ser identificados por los servidores de bloqueo. La lucha será constante, y las sofisticadas herramientas que se utilizan en la actualidad simplemente no pueden bloquear el spam en un 100%, ilustración I.5.

Existen muchos grupos de noticias orientados a los negocios en la web que son enviados a miles de usuarios. No obstante, la convergencia de correo electrónico y publicidad hace que los encabezados de los mensajes parezcan forjados o ilegítimos (véase ilustración I.5).

Hay organizaciones que prefieren crear una norma corporativa que impida recibir cualquier boletín informativo a menos que una persona o grupo (por ej., Recursos Humanos) de la organización otorgue un permiso expreso.
Para esto McAfee ha apostado en la actualización de sus motores de spam, por medio de sitios que identifican y evalúan los correos en base a su encabezado, contenido y medio de propagación, adicional, los usuarios que usan la tecnología McAfee juegan un papel importante a la hora de identificar un posible correo spam, ya que pueden actualizar sus diccionarios para bloquearlos.
Al actualizar un diccionario de manera local se está generando un nuevo registro en las bases de McAfee, con lo que los usuarios vamos agregando registros y actualizando la base de firmas.

Ilustración I.5 SPAM

I.2 Antecedentes

I.2.1 Definición de Seguridad Informática [11]

En el libro Fundamentos de Seguridad Informática de las M. C. María Jaquelina López y M.C. Cintia Quezada, dice: “El término seguridad de la información se refiere a la prevención y a la protección, a través de ciertos mecanismos, para evitar que ocurra de manera accidental o intencional la transferencia, modificación, fusión o destrucción no autorizada de la información”.

La seguridad de la información engloba todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad (conocida como la tríada CIA, del inglés: “Confidentiality, Integrity, Availability”, como se observa en la Ilustración I.6).

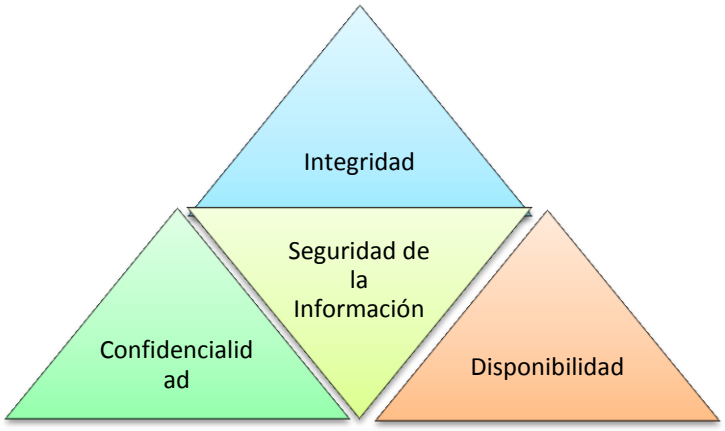


Ilustración 1.6 Seguridad de la Información tríada CIA [11]

A continuación se explican brevemente los principios básicos de la seguridad de la información.

1. Confidencialidad.- Condición que garantiza que la información es accedida solo por las personas autorizadas según la naturaleza de su cargo o función dentro de la organización.
2. Integridad.- Condición que garantiza que la información es consistente o coherente.

3. Disponibilidad.- Condición que garantiza que la información puede ser accedida en el momento en que es requerida.

El costo de las infracciones a la seguridad de la información en términos monetarios y credibilidad empresarial son altos.

Todas las organizaciones necesitan usar seguridad de información para prevenir la divulgación de propiedad intelectual.

Los proveedores de servicios de correo electrónico no están obligados a proporcionar seguridad de información al nivel que lo hacen las empresas.

Las organizaciones deben educar a sus empleados sobre la seguridad de información con respecto al correo empresarial. Los empleados nunca deben enviar información empresarial a cuentas de correo electrónico personales, incluso si trabajan en casa.

I.2.2 Seguridad de la Información y Protección de Datos [6]

En seguridad de la información se deben distinguir dos propósitos de protección, la seguridad de la Información y la Protección de Datos (véase figura I.7).

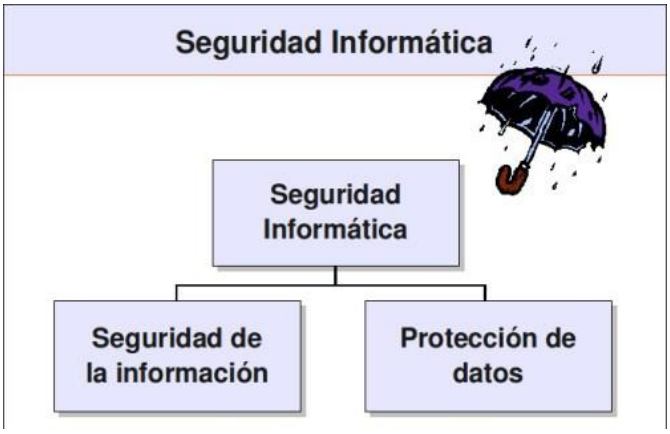


Ilustración 1.7 Propósitos de Seguridad de la Información

Se debe distinguir entre los dos, porque forman la base y dan la razón, justificación en la selección de los elementos de información que requieren una atención especial dentro del marco de la Seguridad Informática y normalmente también dan el motivo y la obligación para su protección.

En el caso de la Protección de Datos, el objetivo de la protección no son los datos como tal, sino el contenido de la información sobre personas, para evitar el abuso de esta.

I.2.3 Criptografía [15]

Es la ciencia que estudia los métodos y procedimientos para modificar los datos, con objeto de alcanzar las características de seguridad.

I.2.4 Tipos de Cifrado [15]

I.2.4.1 Criptografía de clave secreta

Se incluyen en esta familia el conjunto de algoritmos diseñados para cifrar un mensaje utilizando una única clave conocida por los dos interlocutores, de manera que el documento cifrado sólo pueda descifrarse conociendo dicha clave secreta.

I.2.4.2 Criptografía de clave pública

Utilizan dos claves distintas para cifrar y para descifrar el mensaje. Ambas claves tienen una relación matemática entre sí, pero la seguridad de esta técnica se basa en que el conocimiento de una de las claves no permite descubrir cuál es la otra clave.

Cada usuario cuenta con una pareja de claves, una la mantiene en secreto y se denomina clave privada y otra la distribuye libremente y se denomina clave pública. Para enviar un mensaje confidencial sólo hace falta conocer la clave pública del destinatario y cifrar en mensaje utilizando dicha clave. En este caso los algoritmos asimétricos garantizan que el mensaje original sólo puede volver a recuperarse utilizando la clave privada del destinatario como podemos observaren la Ilustración I.8. Dado que la clave privada se mantiene en secreto, sólo el destinatario podrá descifrar el mensaje.

Ilustración 1.8 Criptografía de Clave Pública

Al hablar de estos temas es común encontrarnos con términos como amenazas, vulnerabilidades, ataques, certificado Digital, entre otros, los cuales definiré a continuación.

Un ataque [3] consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio.
Una vulnerabilidad consistirá en cualquier debilidad que puede explotarse para causar pérdida o daño al sistema y puede ser aprovechado por un atacante para violar la seguridad. Es tarea de los administradores y usuarios el detectarlas, valorarlas y reducirlas.
Los tipos de ataque pueden ser pasivos o activos [11].
Los ataques activos son acciones iniciadas por una persona que amenaza con interferir el funcionamiento adecuado de una computadora o hace que se difunda de un modo no autorizado. En el ataque pasivo se intenta obtener información o recursos de una computadora personal sin interferir con su funcionamiento.

A continuación se muestran las diferentes categorías de ataque.

a) Interrupción El principal daño de este ataque es que pierde o deja de funcionar un punto del sistema. Este ataque atenta contra la disponibilidad.
b) Intercepción El principal daño es que se accede a la información por parte de personas no autorizadas, utilizan privilegios no adquiridos. Este ataque atenta contra la confidencialidad.
c) Suplantación El principal daño es la sustitución de algo, se hace pasar por alguien. Se crean nuevos objetos dentro de un sistema. Este ataque atenta contra la autenticación.

d) Modificación La información ha sido alterada sin permiso. El principal daño es el acceso no autorizado que cambia la información para su beneficio. Este ataque atenta contra la integridad.

Las amenazas [3] son eventos que pueden causar alteraciones a la información, ocasionándole pérdidas materiales, económicas, de información y de prestigio. Aunque todas las amenazas tienen la característica de ser las posibles causantes de destrucción a los sistemas, pueden provenir de diferentes orígenes: desastres naturales, errores de hardware, de software, de red y amenazas humanas.

IDS Sistemas Detectores de Intrusos. Este tipo de sistema detecta tráfico malicioso en la red. Monitorea los paquetes en la red y alerta si hay una actividad maliciosa. Además detectan gran cantidad de tipos de ataques.

I.3 Directorio Activo de Microsoft [14]

Es una base de datos distribuida que permite almacenar información relativa a los recursos de una red con el fin de facilitar su localización y administración. El directorio activo contiene información sobre las propiedades y la ubicación de los diferentes tipos de recursos dentro de la red.

Los servicios de directorio también ofrecen la ventaja de suponer un único punto de entrada para los usuarios a la red de toda la empresa. Los usuarios pueden buscar y

usar recursos en la red. Igualmente, puede administrar toda la red con una vista lógica y unificada de la organización.

Una de las ventajas que ofrece el Directorio Activo es que puede utilizar LDAP (Protocolo Ligero de Acceso a Directorios, por sus siglas en inglés Lightweight Directory Access Protocol), un protocolo de acceso estándar que permitirá la consulta de información contenida en el directorio. Sin embargo, también puede utilizar ADSI (Interfaces de Servicio de Directorio Activo, por sus siglas en inglés, Active Directory Services Interface), un conjunto de herramientas ofrecidas por Microsoft, que tienen una interfaz orientada a objetos y que permiten el acceso a características que no están soportadas por LDAP.

I.3.1 Protocolo Liviano de acceso a directorios (LDAP) [14]

Cada vez que uno escucha las palabras “computadora”, “administración” e “información” en la misma oración, inmediatamente sabe que hay una base de datos relacionada. Los directorios son bases de datos especializadas que mantienen un registro de la información distribuida en una red. Las características principales de los directorios LDAP son:

- Independencia ya que permite que cualquier aplicación de otra plataforma que sea compatible con LDAP obtenga acceso a los datos
- Datos relativamente estáticos que casi nunca se modifican
- Operaciones de lectura extremadamente rápidas, porque los datos son leídos frecuentemente pero casi nunca se modifican
- Relativamente seguro, lo que permite delegar de manera segura las autorizaciones de lectura y modificación de acuerdo con las necesidades, utilizando Interfaces de control de acceso
- Basado en normas, con el uso de un esquema, disponible para todas las aplicaciones que utilicen el directorio
- Capaz de crear múltiples réplicas maestras, lo que proporciona directorios con capacidad de auto recuperación

I.3.2 Almacenamiento de LDAP [14]

Los servidores LDAP generalmente se optimizan para numerosas operaciones de lectura, pero no están preparados para almacenar datos que se modifican con frecuencia. La decisión de usar un directorio LDAP puede depender de que las siguientes preguntas tengan respuestas afirmativas:

- ¿Se necesita obtener acceso a los datos desde diferentes plataformas?
- ¿Se necesita obtener acceso a los datos desde múltiples computadoras o aplicaciones?
- ¿Se producen pocos cambios al día en los registros que se almacenarán?
- ¿Tiene sentido almacenar los datos en una base de datos plana en lugar de una base de datos relacional?

I.4 Configuración del MEG

Para la configuración se ofrecen una variedad de herramientas tanto para crear como para aplicar normas de correo electrónico que van desde retrasar la entrega de mensajes grandes a horas de menor tráfico hasta reenviar o enviar como copia oculta mensajes dirigidos a individuos o dominios específicos y prohibir palabras “muy expresivas” o “de adultos” en el correo todo basándose en consultas al directorio activo de la empresa, también se cuenta con un asistente de configuración el cual nos va guiando paso a paso hasta lograr la instalación planeada.

I.4.1 Programa de limpieza

A medida que pasa el tiempo, se acumulan muchos archivos y datos. Por tal motivo se recomienda permitir que el equipo elimine regularmente del sistema lo innecesario.

Los administradores deben especificar tres opciones:

- El archivo que se limpiará
- El intervalo de limpieza - o cuánto tiempo puede permanecer un archivo en el disco
- Un ciclo de limpieza - con qué frecuencia ejecuta la limpieza

Aunque el MEG es un herramienta muy potente, no debemos dejar a un lado que requiere mantenimiento o limpieza, en la mayoría de los casos, los administradores querrán mantener una "ventana continua" de datos en el disco duro

I.4.2 Cuarentena

Aunque se puede lograr una cifra muy baja de falsos positivos, algunos administradores se sienten más cómodos si configuran la acción de las herramientas de spam en "Colocar en cuarentena" en lugar de "Excluir", a fin de que el Programa de limpieza borre los mensajes después de un número *n* de días. Cuando los usuarios reportan que el correo electrónico que están esperando aún no ha llegado, los administradores pueden buscar el mensaje en la cola de espera de cuarentena, entonces se puede mover a la cola de espera de salida para su entrega inmediata, existen diferentes tipos de cuarentena:

- Filtrado de contenido
- Filtrado de adjuntos
- Supervisión de correo
- Antivirus
- Filtrado de mensajes cifrados
- Anti-spam
- Fuera de horario

I.4.3 Entrega fuera de horario

Los administradores pueden crear normas que retrasen temporalmente la entrega de correos electrónicos grandes, de modo que se envíen fuera de las horas de alto nivel de tráfico. De esta manera, durante las horas pico, el ancho de banda no es afectado por uno o más archivos grandes.

I.4.4 Marcación de mensajes

En esta tecnología se ofrece la posibilidad de agregar "mensajes de pie de página" al final de los mensajes salientes enviados en formato de texto plano. Los administradores pueden crear diversas normas que se apliquen a personas y grupos

de cualquiera de los dominios de la empresa, para que se agreguen los mensajes requeridos (véase ilustración I.9).

AVISO LEGAL

El contenido de este correo electrónico y sus anexos es confidencial o legalmente privilegiado. Puede también se privilegie. Si le fue enviado por error, sea tan amable de borrarlo sin revisarlo y por favor hágalo saber al remitente. Por este medio usted queda notificado de que está estrictamente prohibida cualquier divulgación, distribución, copia u otro uso del mensaje o sus anexos. El correo electrónico no es un medio de comunicación 100% seguro, por lo que no garantizamos que las comunicaciones de Internet sean oportunas, seguras,libres de error o virus.

Ilustración 1.9 Ejemplo de marcación de mensajes

I.5 Administración

La administración es relativamente muy sencilla gracias a lo amigable de su interfaz de usuario que proporciona una forma intuitiva de la búsqueda de información y la configuración de las opciones en la cual a simple vista podemos obtener un panorama general del comportamiento de nuestro dispositivo (véase ilustración I.10).

Ilustración 1.10 Administración de Interfaz de Usuario

A — Área de Navegación

El Área de navegación contiene cuatro áreas: usuario, información del usuario, iconos, barra de pestañas, y controles de soporte.

B — Barra de información del usuario Que usuario está conectado y que perfil tiene.

C — Sección de iconos

Tablero: Con este icono se puede revisar el comportamiento del dispositivo.

Reportes: Usa el icono de reportes para ver actividad en el sistema como actualizaciones recientes o el status de los mensajes que han ingresado.

Email: Usa el icono de email para administrar amenazas, cuarentenas y otros aspectos de la configuración del mail.

Sistema: Usa este icono para configurar cuestiones directas del dispositivo.

Solucionador de problemas: Proporciona una visión general del aparato, y se pueden realizar pruebas de validación.

D — Barra de Pestañas

Aquí se pueden observar las diferentes actividades a realizar en cada apartado.

E — Botones de Control o Soporte

Son acciones para aplicar al área de contenido, como actualizar, notificación de cambio, regresar.

I.5.1 Copia de respaldo y Restauración

Los administradores pueden crear una copia de respaldo de los valores de configuración del dispositivo en caso de que se produzca una falla de disco. La copia de respaldo sólo se debe utilizar para restaurar los datos en el mismo dispositivo.

Cuando guarda una configuración de respaldo en el disco, utiliza un método automático de asignación de nombres, identificando el nombre, número de versión, número de última actualización y fecha del dispositivo. La información de la copia de respaldo se cifra, almacena en un formato de archivo patentado que sólo se puede leer por el MEG y no se puede ver en Texto plano (véase ilustración I.11).

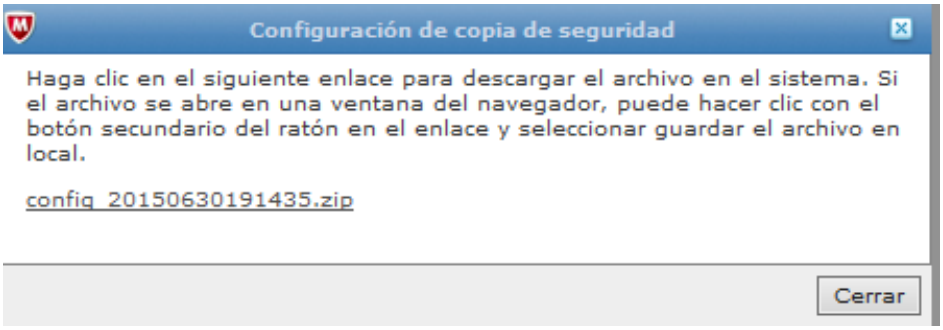


Ilustración 1.11 Copia de respaldo

Al igual que se puede obtener la copia de respaldo es muy sencillo utilizar la función Restaurar para restaurar los datos de la configuración solamente en el mismo dispositivo.

En el apartado de administración del sistema, se pueden configurar estas actividades para obtenerlas de manera automática o manual.

I.5.2 Gestión de Componentes y Licencias.

Cuando se instala por primera vez, incluye un Certificado de seguridad "firmado por sí mismo" que sirve para cifrar las sesiones Web para los administradores que manejan sus dispositivos.

El dispositivo protege los mensajes en tránsito mediante dos métodos: crear canales cifrados de comunicación (SSL) o crear datos de mensaje cifrados (S/MIME o PGP).

En la tabla Administrador de licencias muestran todas las Licencias de producto que se han instalado (*Véase ilustración I.12 y Aanexo 3 licencias disponibles para MEG*).

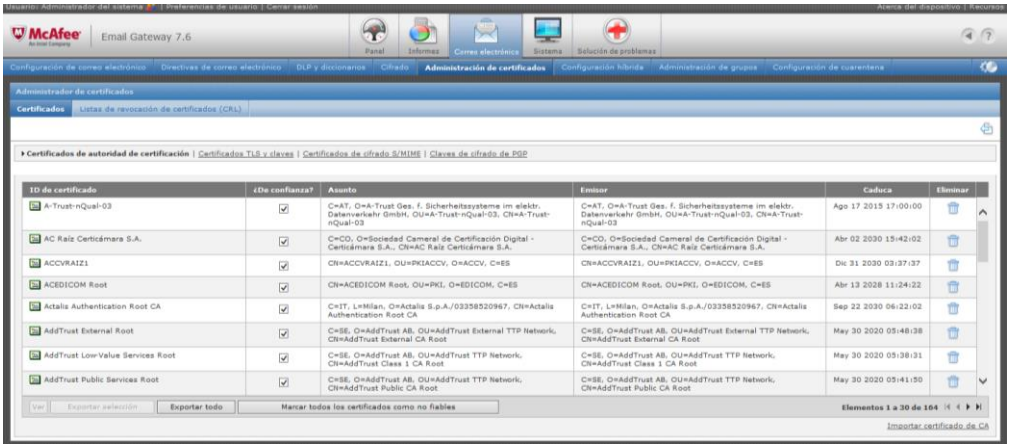


Ilustración 1.12 Administrador de Licencias

Los administradores pueden elegir buscar manualmente los nuevos archivos de definiciones de virus, spam, etc., en cualquier momento.

Si se informa que están disponibles nuevos archivos, los administradores pueden descargar e instalar manualmente las nuevas actualizaciones, o configurar para que el dispositivo realice esta actividad de manera automática cada cierto tiempo definido por el usuario, todo esto lo puede localizar en el apartado de sistema, gestión de componentes, como se muestra en la Ilustración I.13.

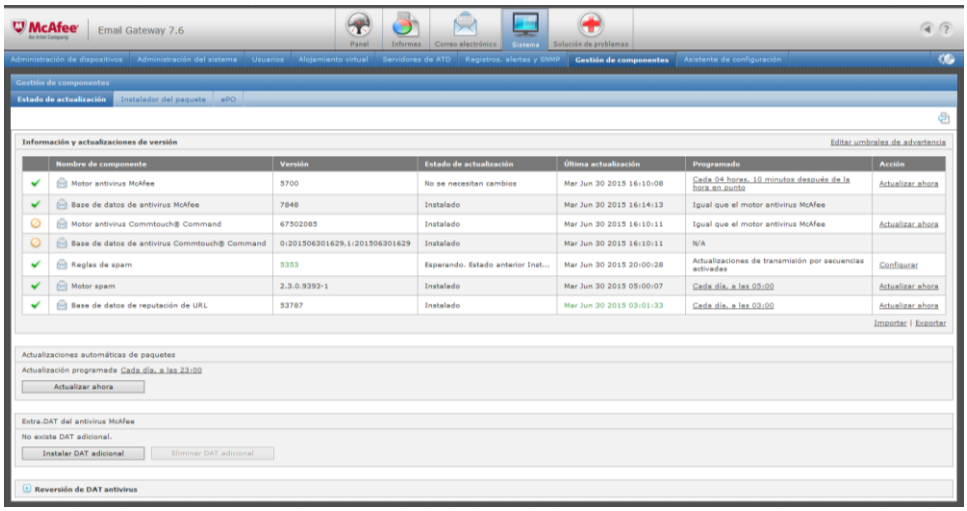


Ilustración 1.13 Administrador de componentes

I.5.3 Informes y supervisión

Las herramientas de informes y supervisión son las que hacen que sea un dispositivo tan poderoso y útil. A través de sus registros, los administradores pueden determinar exactamente cuáles procesos examinaron un mensaje e incluso si recibió o no el mensaje, existen distintos tipos de informes programados, como lo podemos ver en la Ilustración I.14.

Puede generar informes diarios en formato HTML con información detallada sobre los mensajes que procesa cada día. Adicionalmente, los informes se pueden comprimir como archivos “CSV” (valores separados por comas), para su análisis en aplicaciones de terceros.

Los informes abarcan dos amplias categorías: el correo electrónico que procesa y la actividad interna.

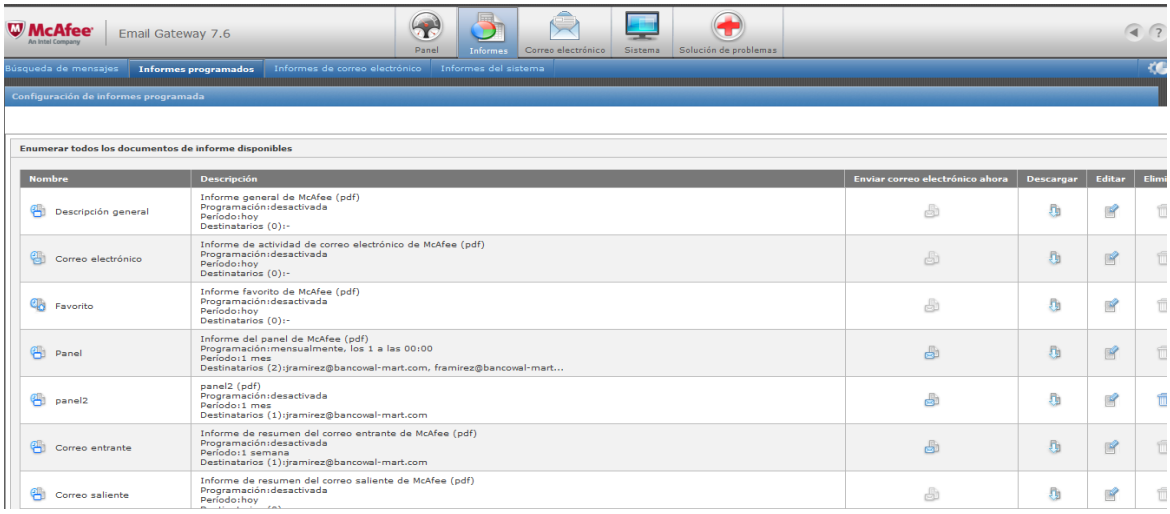
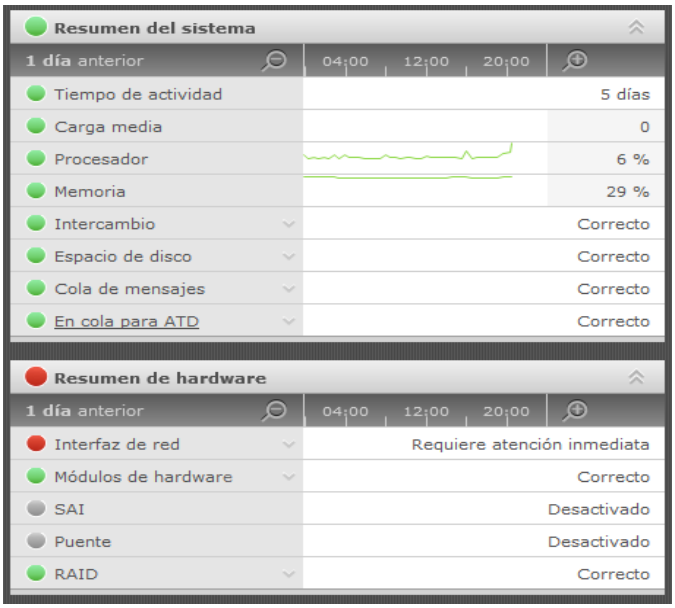


Ilustración 1.14 Informes programados

I.5.4 Monitor de Salud del equipo

El monitor de salud es un subsistema que examina el funcionamiento general del dispositivo al ejecutar una serie de pruebas para asegurarse de que todos los servicios y procesos estén funcionando correctamente, se activa a intervalos definidos por el usuario y se ejecuta automáticamente en segundo plano para probar los diversos subsistemas del dispositivo, (véase Ilustración I.15).



Saludable: todo funciona correctamente

Requiere Atención

Requiere Atención Inmediata

Deshabilitado: el servicio no está activo.

Ilustración 1.15 Monitor de Salud

I.5.4.1 Administrador de Alertas

El dispositivo supervisa continuamente sus subsistemas principales, así como su capacidad para comunicarse con los servidores de correo internos. Si alguna de las funciones deja de funcionar correctamente, generará un alerta.

Las alertas que puede enviar son los siguientes:

• **Información:** Esta alerta sólo tiene carácter informativo.

• **Notificación:** Proporciona información sobre un proceso o servicio.

• **Advertencia:** Una advertencia requiere de "mayor atención". Significa que se justifica una acción administrativa.

• **Error:** Un error es un alerta grave que genera mensajes de error cuando un proceso no se ejecuta de la manera esperada.

• **Crítico:** Un alerta crítico es aún más grave, y se genera cuando un error afecta todo el dispositivo.

• **Apagado**: (Este alerta está reservado para funciones futuras).

• **Reiniciar:** (Este alerta está reservado para funciones futuras).

Las alertas, por sí solas, no hacen nada, pero sirven para que el administrador este enterado en tiempo real del estado de su equipo.

I.5.5 La línea de comandos

Cualquier administrador puede obtener acceso a muchas de las funciones disponibles a través de la Interfaz gráfica de usuario (GUI) desde la línea de comandos utilizando uno de dos métodos:

- **Desde la consola:**

Si al dispositivo están conectados un teclado y un monitor, el monitor muestra una solicitud de inicio de sesión.

- **Desde una Secure Shell:**

El administrador también puede obtener acceso a la línea de comandos desde una estación de trabajo que utilice una aplicación Secure Shell (mediante el puerto 22).
Algunos de los comandos que se pueden utilizar son:

Comando HELP Se puede obtener acceso a la ayuda en pantalla.

Comando EDIT Se utiliza para modificar valores de configuración.

Comando RUN Permite Ejecutar comandos específicos a discreción.

Debido a que éste ejecuta una compleja consulta SQL de la base de datos, se recomienda sea ejecutado durante las horas de menor tráfico.

El Comando SET Se utiliza para iniciar, detener, habilitar e inhabilitar servicios, configurar el puerto en serie, y desbloquear las cuentas de usuario que hayan sido bloqueadas debido a excesivos intentos fallidos para iniciar sesión.

Comando SHOW Muestra información acerca del sistema, los servicios.

I.5.6 Solucionador de Problemas (Troubleshoot)

Proporciona una visión general de las características dentro del McAfee Email Gateway que le ayudan a solucionar problemas del aparato, el cual incluye muchas herramientas de diagnóstico para la identificación de problemas.

Se puede utilizar esta página para comprobar si el aparato puede llegar a otros dispositivos a través de la red y descartar problemas físicos con las conexiones, adicionalmente se pueden hacer pruebas de email, revisar el estado del hardware, la capacidad de disco, el estado de los procesadores, como se puede observar en la Ilustración I.16.

Los datos utilizados aquí se actualizan cada 10 minutos.

Ilustración 1.16 Solucionador de problemas

En la Ilustración I.17 podemos ver cuales son los indicadores del solucionador de problemas, pues con ellos podremos conocer si el dispositivo esta trabajando de manera correcta, o requiere alguna asistencia.

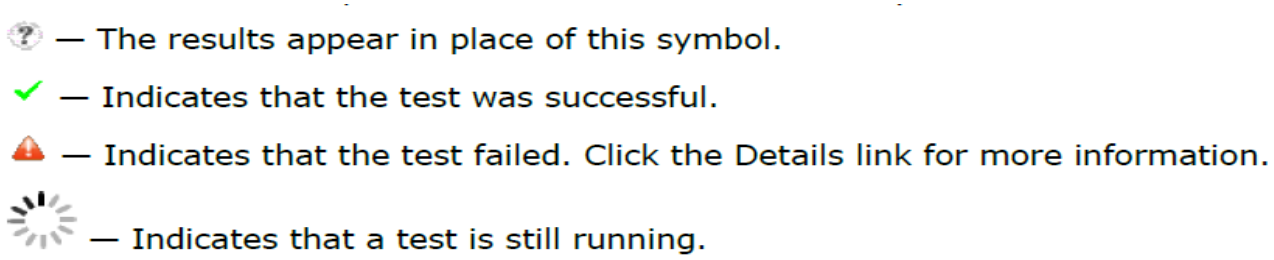


Ilustración 1.17 Indicadores de Troubleshoot

II. MARCO CONTEXTUAL

Durante este capítulo vamos a encontrar los aspectos relacionados a la institución, la importancia de tener un área de Seguridad de la Información y el puesto que he desempeñado durante mi estancia en esta empresa.

II.1 Empresa

BANCO WAL-MART DE MEXICO ADELANTE, SOCIEDAD ANONIMA INSTITUCION DE BANCA MULTIPLE

Ilustración II.1 Logo Banco Wal-Mart

II.1.1 Visión [2]

Contribuir a mejorar la calidad de vida de las familias mexicanas.

Asegurar la alineación completa entre Banco y Retail para ser el socio financiero más confiable de WALMEX.

II.1.2 Misión [2]

Ser el mejor proveedor de servicios financieros para todos los clientes de las tiendas, clubes y restaurantes de Grupo Wal-Mart, a fin de contribuir a elevar su calidad de vida, apoyando al crecimiento del Grupo, la rentabilidad de sus accionistas y el crecimiento de nuestros asociados.

Ser un Banco rentable con presencia nacional que tenga un impacto positivo en las vidas de las familias en las que WALMEX tenga presencia.

La compañía siempre ha operado basándose en tres Principios Básicos que son nuestros valores.

II.1.3 Valores [23]

- ✓ **Respeto por el Individuo**

Para tener respeto por el individuo, necesitas creer en la gente

- El reto y preocupación de la compañía es mantener motivados a los asociados
- Cada vez que el asociado tenga una idea o inquietud puede con toda confianza expresarla
- Motivar a la gente para que puedan alcanzar sus metas
- Si todos conocemos las metas de la compañía, podemos trabajar mejor
- Es nuestra responsabilidad proteger la información y manejarla de manera inteligente. **No podemos revelar datos confidenciales**

- ✓ **Servicio al cliente**

Podemos dar un servicio excepcional si:

- Damos respuesta a todas las peticiones rápidamente
- Tratamos a los clientes como si estuvieran en casa (hospitalidad activa)
- Usamos el nombre del cliente siempre que sea posible
- Agradecemos al cliente haber elegido algún producto del Banco

- ✓ **Búsqueda de la Excelencia**

Nos permite alcanzar resultados extraordinarios, siempre enfocados

- Orientación a resultados
- Mejora Continua
- Trabajo en equipo
- Tomar riesgos
- Control de Gastos

II.1.4 Código de Conducta [23]

Documento interno basado en la Declaración de Ética de Wal-Mart, que contiene los **principios y valores éticos** de la Compañía.
Marca las pautas de comportamiento que debes llevar a cabo dentro y fuera de la empresa.

II.1.4.1 ¿Por qué Banco Wal-Mart debe contar con un Código de Conducta?

En México, todos los bancos por ley están obligados a contar con un documento que norme la conducta de los directivos y demás personal del banco, entre los asociados, hacia los clientes y hacia los asociados de otros formatos, asegurando que todos se **comporten con altos estándares éticos y guardar la confidencialidad de la información**, Asimismo, es obligación del banco difundir el **Código de Conducta** entre todos los asociados y a todos los niveles, basados en los principios de la Circular Única de Bancos, Arts. 142, 164 y 170.

II.1.5 Historia [23]

10 de noviembre de 2006 Se constituyó mediante autorización de la Secretaria de Hacienda y Crédito Público.

22 de noviembre de 2006 Se otorga la autorización oficial para la constitución de la entidad financiera, bajo la aprobación de la Comisión Nacional Bancaria y de Valores.

1 de octubre de 2007 La CNBV entrega el oficio con la certificación de Banco Wal-Mart de México Adelante, S.A. Institución de Banca Múltiple para el inicio de operaciones.

7 de noviembre de 2007 Se inauguran las primeras unidades de Banco Wal-Mart para atención al público: Toreo (Oficinas Corporativas) en el Distrito Federal y Toluca, Zinacantepec y Alfredo del Mazo en el Estado de México.

7 de marzo de 2011 A cuatro años de su creación Banco Wal-Mart abrió la cuenta **Un Millón** en una de sus sucursales de la Ciudad de México.

Junio de 2015 Comisión Nacional Bancaria y de Valores anuncia la venta de Banco Wal-Mart Adelante a Grupo Financiero Inbursa.

II.2 Seguridad de la Información [2]

Podemos entender como seguridad, un estado de cualquier sistema (informático o no) que nos indica que ese sistema está libre de peligro, daño o riesgo. Entendiendo como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo.

La ***información*** es el activo más importante que tiene la organización, por lo cual, todos los que trabajamos en Banco Wal-Mart tenemos la obligación de cuidar la información a la que tenemos acceso.

- Wal-Mart ha sido por muchos años la empresa más exitosa del mundo, y producto de este éxito también es objeto de robo.
- La Seguridad de la información es responsabilidad de todos y **¡comienza contigo!**

Banco Wal-Mart mantiene procedimientos diseñados para proteger la información confidencial sobre el Usuario y el uso por parte de este, de cualquiera de los productos y Servicios proporcionados.

En el margen de crecimiento de este proyecto, se tomaron consideraciones de vital importancia para la seguridad Informática, siempre basándonos en estándar de seguridad ISO270001, como es el mantener el ciclo de Seguridad siempre presente para que en ningún momento se vea expuesta la criticidad de la información. En la siguiente Ilustración podemos ver cómo fue que el proyecto fue tomando forma desde su planeación hasta que por fin lo podemos ver en ejecución.

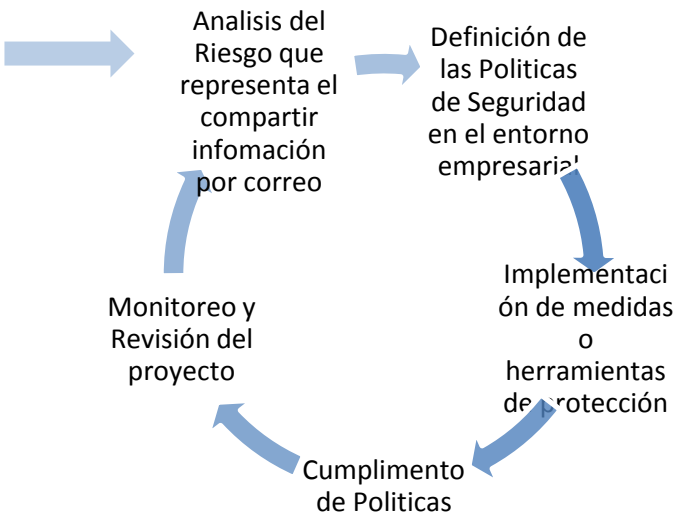


Ilustración II.2 Ciclo de vida de un proyecto en seguridad

Cabe señalar que siempre se debe contar con un esquema de mejoras continuas, para no quedarnos atrás de la vanguardia o de las nuevas amenazas.

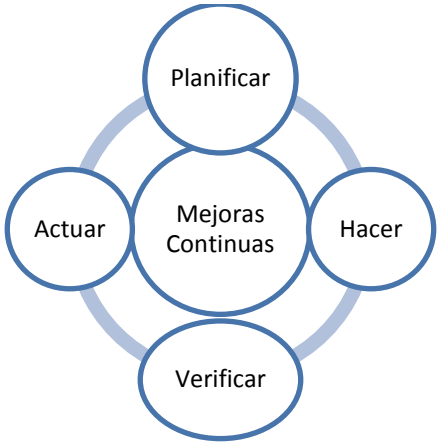


Ilustración II.3 Plan de mejoras continúas en Seguridad

II.2.1 Uso de Información [2]

Todos los datos que se recaben del Usuario serán tratados con absoluta confidencialidad, siendo utilizados para las finalidades para las que han sido solicitados, atendiendo lo dispuesto por los contratos celebrados y lo dispuesto por la legislación mexicana.

II.2.2 Protección de la información personal y comercial [2]

En nuestro negocio diario, podemos estar expuestos a información personal y comercial acerca de los asociados, clientes, miembros, proveedores y nuestra propia compañía.

Es nuestra responsabilidad proteger esta información de conformidad con las leyes correspondientes, nuestras políticas y los principios de la compañía.

La información puede ser física (en papel) o electrónica.

Se debe administrar dicha información de forma segura a lo largo de su ciclo de vida y de conformidad con los requisitos de administración de registros de Wal-Mart. La información de la compañía se divide en tres clases.

II.2.3 Clasificación de la información [2]

a) Información Privada

Información personal de los Asociados (expedientes de contratación, recibos de nómina, evaluaciones, incapacidades, enfermedades, asesorías).

Sólo el personal autorizado tiene acceso a esta información.

b) Información Confidencial (Información de Clientes).

Se prohíbe revelar u obtener información de clientes y sus operaciones. Está protegida por Secreto Bancario.

Queda estrictamente prohibido ingresar a las cuentas de los clientes sin autorización del titular. **Hacerlo es un DELITO**.

c) Información Comercial (Información de la **Compañía**).

Ningún Asociado podrá revelar información sobre productos, procesos, controles, políticas, estrategias y tecnologías desarrolladas por y para Banco Wal-Mart. Así como traer información de otros trabajos.

II.2.4 Consideraciones [2]

Se puede hacer uso de documentos emitidos por entidades regulatorias, metodologías, estándares y/o mejores prácticas internacionales o locales aplicables

en materia de Seguridad de la Información; las cuales incluyen pero no se limita a las siguientes:

- Ley de Instituciones de crédito (LIC)
- Disposiciones de carácter general aplicables a las instituciones de crédito Circular Única de Bancos (CUB)
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)

II.2.5 Estructura Organizacional de Seguridad de la Información

Ilustración II.4 Organigrama de Seguridad de la Información

II.3 Puesto: Operador SOC

El negocio se encuentra expuesto a vulnerabilidades, riesgos y amenazas por el simple hecho de estar conectado a internet, y los incidentes que pueden impactar son cada vez más comunes.

Existen regulaciones, normas, estándares y controles que deben cumplirse a fin de garantizar las operaciones y los servicios de las TIC's.

El Operador SOC, monitorea y apoya en la administración de los controles para la protección de la Información y la administración de usuarios, mediante el uso de las

herramientas de seguridad implementadas, así mismo colabora con la ejecución de mantenimiento e instrumentación de mejoras para mantener los controles de seguridad actualizados.

Principales responsabilidades.

a) Verificación de identidades de usuario mediante un Administrador de Identidades
b) Detección y prevención de intrusiones en la red de computadoras y telecomunicaciones mediante IPS
c) Restricción de tráfico en la red
d) Asegurar la protección de la información
e) Asignación de facultades a usuarios en sistemas de información para el perfilamiento en aplicaciones bancarias
f) Protección contra virus y/o códigos maliciosos para prevenir infecciones en la infraestructura bancaria
g) Identificación de archivos no autorizados
h) Restricción de navegación por internet para evitar infecciones de virus/malware
i) Protección de correo electrónico externos mediante herramientas de filtrado para prevenir fuga de información
j) Restricción de uso de medios removibles para evitar fuga/divulgación de información no autorizada
k) Consultoría y diseño de arquitecturas de seguridad
l) Fortalecimiento “Hardenning”
m) Postura de seguridad
n) Gestión de respaldos

Para todo lo anterior se apoya de tecnologías como:

Firewalls, redes virtuales y privadas (VPN), Filtrado de URL, DLP (Data Loss Prevention), cifrado de contenido.

III. IMPLEMENTACIÓN Y DEFINICIÓN DE POLÍTICAS

En este capítulo se aborda la implementación de los dispositivos MEG en sus dos versiones 5000 y 4500 (producción y desarrollo respectivamente), desde el planteamiento de la problemática, la configuración del dispositivo y planeación de directivas acorde a las necesidades del negocio.

III.1 Problemática [25]

Hoy en día, el correo electrónico es indispensable y uno de los servicios más importantes para el correcto funcionamiento de cualquier entorno empresarial.

La capacidad de este para distribuirse de manera instantánea y con amplios volúmenes de información lo convierte en una herramienta básica y en un constante desafío para la seguridad.

Una de las preocupaciones, es que una vulnerabilidad proporcionará una entrada en los sistemas y facilitara la adquisición de datos.

El perímetro de la red es, para la mayoría de las empresas, relativamente seguro. Los sistemas de protección firewalls, cuando se combinan con unas cuantas herramientas adicionales como los Sistemas de detección de intrusos (IDS), constituyen una línea de defensa efectiva. De hecho, los firewall han demostrado tanta eficacia, que la mayoría de los atacantes han cesado en sus intentos de vulnerarlos [4].

Es entonces que han aprendido a utilizar el correo electrónico real y sus protocolos para realizar sus ataques. Actualmente, los sistemas de correo electrónico son ampliamente utilizados para irrumpir en las redes corporativas.

Las principales amenazas que causan daño en las empresas si se les permite ingresar a la red son [3]:

- Las intrusiones ocurren cuando los usuarios no autorizados obtienen acceso a la infraestructura de la organización. Para quienes promueven y utilizan spam,

esto por lo general consiste en internarse en un servidor de correo para enviar correos masivos o recolectar direcciones de correo electrónico.

- Los promotores del spam a menudo intentan evitar que las herramientas de bloqueo los detecten encubriendo los URL con varias técnicas de codificación. Utilizan este método para representar los caracteres del documento HTML en una de tres formas:
    - Como números decimales
    - Como números hexadecimales
    - Como nombres, en algunos casos

Suponiendo que de 20 a 40% de todo el correo electrónico que entra a un dominio puede ser falso, es fácil entender que, cada día, los administradores deben examinar una gran cantidad de spam para seleccionar los mensajes legítimos que se deben agregar a la lista de confianza y que en escenarios de gran volumen, se pueden necesitar varias personas para examinar todos lo cual implica un gasto económico y de tiempo significativo [9].

El 86% de los negocios piensa que la información y la tecnología de la información son importantes para ser competitivos, Departamento de Industria y Comercio del Reino Unido.

Muchos negocios ya lo usan para mejorar su método de trabajo y confían en el para sus operaciones [9].

Estas son las principales razones.

- Es relativamente económico
- Mandar copias de un mensaje a varias personas es fácil y rápido
- Permite transferir fácilmente datos como informes, presentaciones y otros archivos
- Es cómodo
- Nunca Descansa

El 81% de los negocios que utilizan el email lo adopta para aumentar su eficacia, pero tienden a descuidar la seguridad de la información, Departamento de Industria y Comercio del Reino Unido.

El correo electrónico empresarial es una herramienta de trabajo y propiedad de la institución, por lo que debes hacer uso responsable de éste y únicamente para temas de trabajo.

III.2 Configuración del Dispositivo.

El asistente de configuración es muy sencillo y práctico para usar, pues nos va guiando paso a paso tal como podemos observar en la Ilustración III.1.

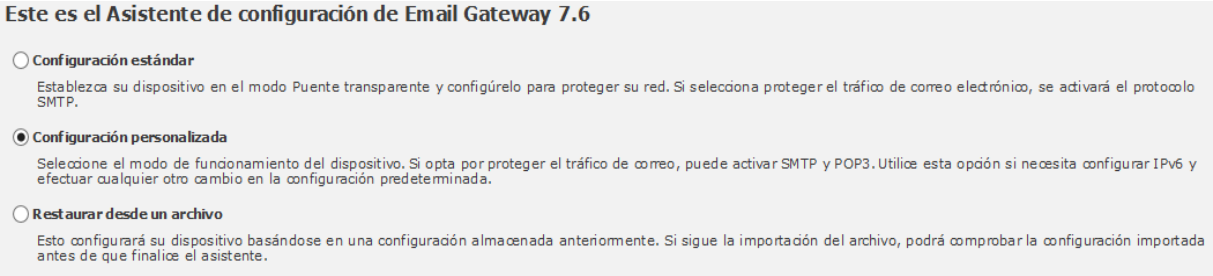


Ilustración III.1 Asistente de configuración MEG

Para empezar tenemos que indicar que tarea vamos a efectuar, ya sea una configuración básica, personalizada, gestionado por alguna consola o solo se trata de una restauración del dispositivo desde un archivo de configuración, en la configuración básica se tiene que ingresar los parámetros de red tal y como se muestra en la siguiente ilustración III.2.

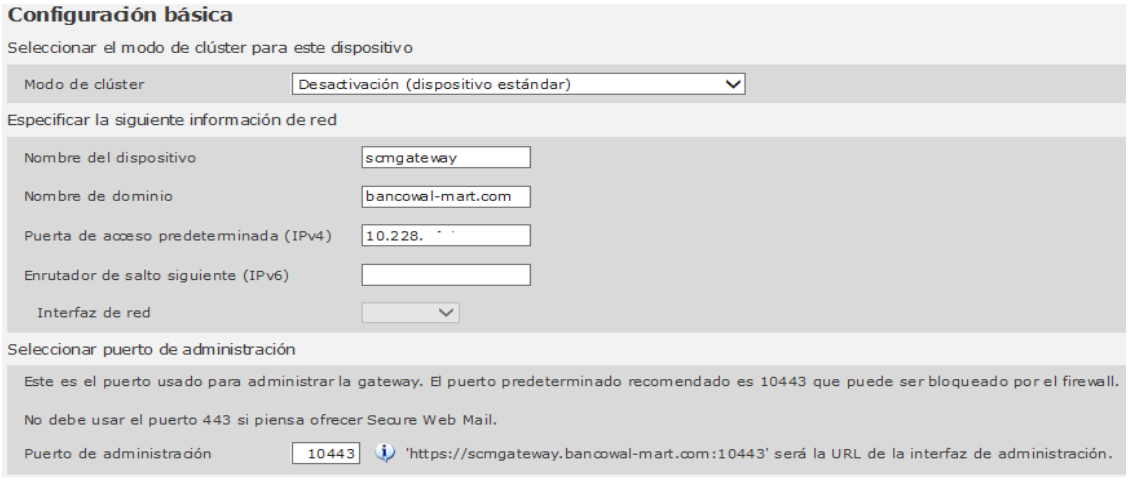


Ilustración III.2 Parámetros de red

Se tiene que configurar todo lo relacionado al correo electrónico de la empresa, dominios, protocolos (véase Ilustración III.3).

Ilustración III.3 Configuración de correo electrónico

Despues se tiene que configurar la zona horaria en la que el dispositvo radicara, como se muestra en la ilustración III.4.

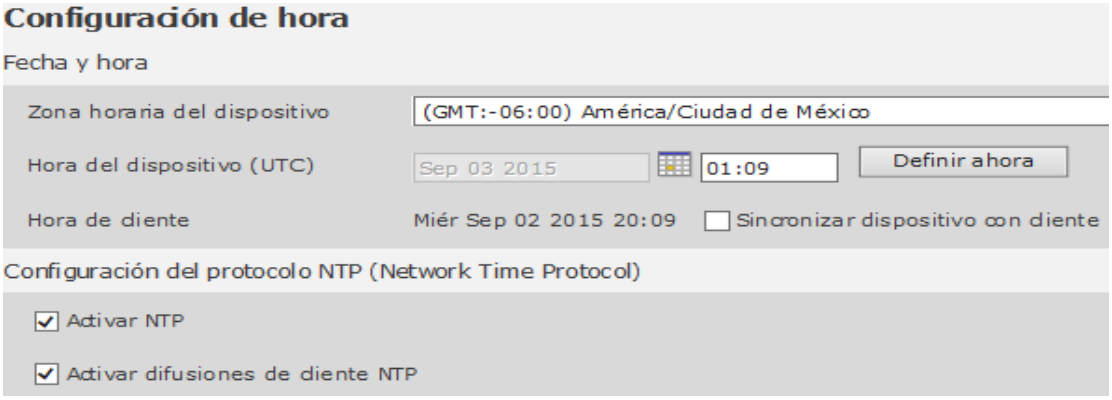


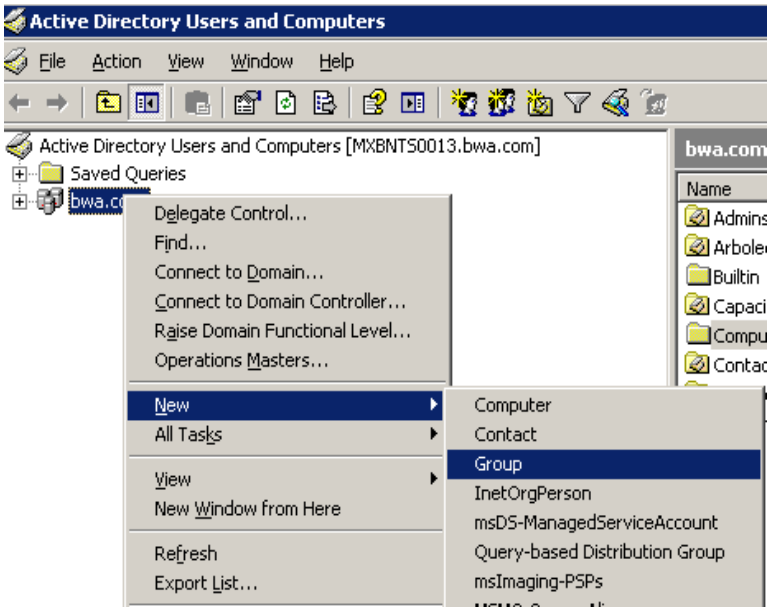
Ilustración III.4 Configuración de hora

III.3 Creación de grupo en Directorio Activo

Se creó un grupo en el Directorio Activo del servidor de dominio de la empresa, el cual tendrá el nombre de "**Usuarios sinEmail**", en este se colocaran a todas aquellas personas que acorde a su perfil y funciones, no puede mandar ni recibir correos de dominios Externos, todo correo que intente mandarse a un dominio que no sea **@bancowal-mart.com** y pertenezca a un usuario miembro de este grupo, será bloqueado por el MEG conforme a la política de Restringe Usuarios sin Email, la cual realiza una consulta a nivel LDAP para ver si algún remitente o destinatario están dentro de dicho grupo.

Los pasos a seguir fueron los siguientes:

1. En el Directorio Activo en **Herramientas Administrativas**, en **Usuarios y Computadoras del Directorio Activo.**



2. Se selecciona el dominio al que pertenecerá el grupo, en este caso bwa.com, clic derecho **Nuevo**, **Grupo,** como se muestra en la Ilustración III.5.

Ilustración III.5 Creación de grupo en AD

3. Se indica el **Nombre** del grupo y una breve **Descripción** para saber qué hace, y se define el **Tipo** y **Alcance** del grupo (véase Ilustración III.6).

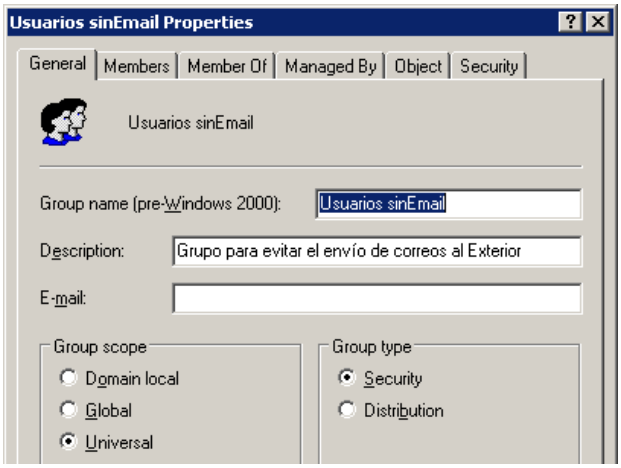


Ilustración III.6 Parámetros de nuevo grupo

4. En el apartado de **Miembros**, se pueden **Agregar** o **Remover** usuarios según se desee, como se muestra en la Ilustración III.7.

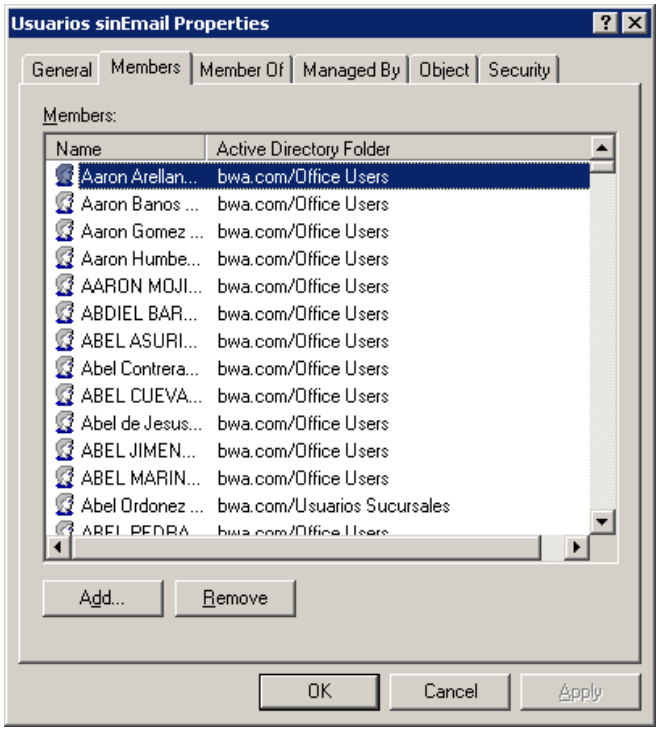


Ilustración III.7 Agregar o remover usuarios del grupo

III.4 Como configurar LDAP en McAfee Email Gateway 7.x [12]

Se puede configurar McAfee Email Gateway (MEG) 7.x para agregar una conexión entre el dispositivo y cualquier Servidor LDAP en el entorno.
Si se configura MEG 7.x con LDAP, se puede utilizar de la siguiente manera:

- Autenticación del remitente
- Enmascaramiento de direcciones.
- Selección de Políticas
- Selección de rutas de entrega del correo

El dispositivo MEG 7 soporta los siguientes tipos de servidores LDAP:

- Microsoft Active Directory
- Lotus Domino
- Generic LDAP Server v3
- Microsoft Exchange

Antes de poder usar el dispositivo con LDAP, primero debemos configurar los parámetros del Servidor AD donde se encuentra en LDAP en el MEG.

III.4.1 Configurar el Servidor LDAP [12]

1. Inicie sesión en la consola Web de Email Gateway.
2. Selecciona **Email**, **Administración de grupos**, **Servicios de Directorios**.
3. Clic **Agregar Servidor**, se desplegara una pantalla como la Ilustración III.8.
4. Especifica el **nombre del servicio**, **direcciones del servidor**, **Puerto del Servidor** (si el servidor LDAP está o no corriendo con los puertos predeterminados).
5. En la lista desplegable **Tipo de Servidor**, seleccione el tipo de Directorio.
6. Específica el **DN** (nombre de dominio), **usuario** y **contraseña**.

Ilustración III.8 Configuración LDAP

7. Para modificar las consultas predeterminadas, selecciona la consulta y da clic en **Editar Consulta** véase Ilustración III.9.

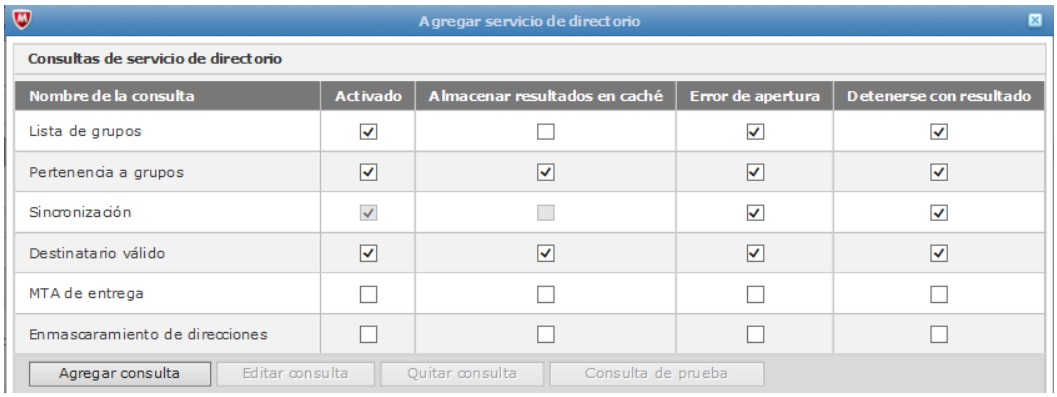


Ilustración III.9 Consultas LDAP

8. La pantalla de editar Consulta permite modificar los Consultas primaria y secundaria que están predeterminadas, como se muestra en la Ilustración III.10.

    - La consulta primaria es la consulta que será enviada sobre todo cuando se activa una consulta específica.

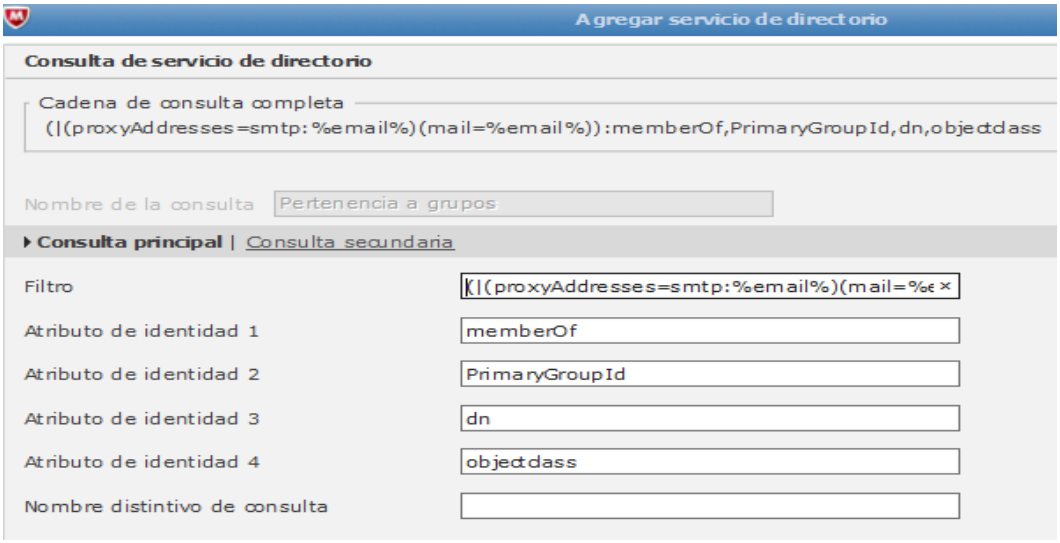


Ilustración III.10 Parámetros de consulta LDAP en MEG

9. Clic en una consulta individual para probar que está trabajando, (véase Ilustración III.11).

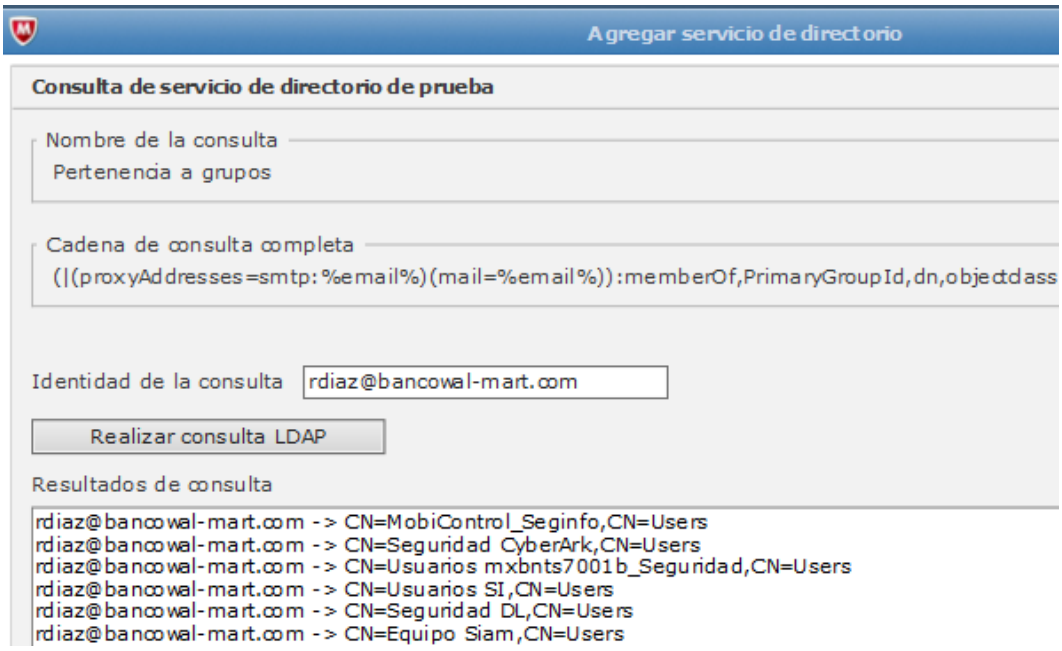


Ilustración III.11 Prueba de consulta exitosa

10. Clic **Finalizar** para completar la configuración

III.4.2 Configurar el Dispositivo para usar LDAP [12]

1. Crear una Política de Email que use LDAP, (véase Ilustración III.12):
    a. Clic **Email**, **Políticas de Email**
    b. Clic **Agregar Política** y especificar el nombre
    c. Selecciona la Dirección Email apropiada

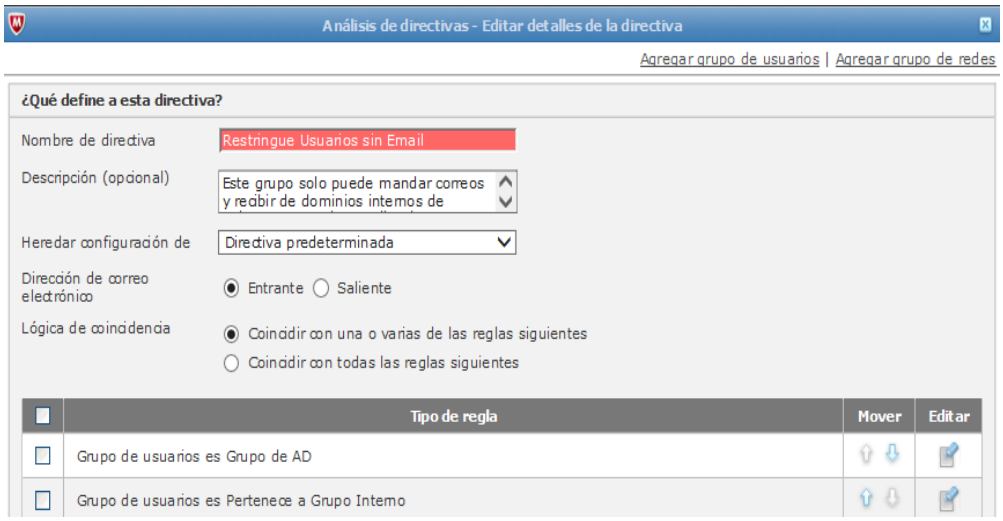


Ilustración III.12 Creación de Directiva para consultas mediante LDAP

    d. Clic **agregar regla** y prepara el tipo de regla como **Consulta LDAP**

Ilustración III.13 Regla para consultar LDAP

e. Selecciona el **Operador**
f. Clic **Aceptar** para guardar la política y **Aplicar** los cambios

III.5 Definición de directivas para MEG Junio y Julio 2014

Las directivas de correo en MEG son elementos que permitirán regular, filtrar o detener los correos electrónicos entrantes y salientes.

En los dispositivos MEG existe una directiva predeterminada (General), que para mí sirvió de referencia para crear nuevas directivas, por tal motivo no se eliminó, ni modifico.

Es importante mencionar que el orden de las directivas corre un papel importante a la hora de instalar y accionar el dispositivo, para que puedan cubrir los filtrados deseados.

Me base en las necesidades del negocio para poder crear las directivas y tener el menor impacto posible.

III.5.1 Directiva No. 1 Suplanta Identidad

Objetivo: Bloquear todo correo entrante y saliente entre dominio @bancowal-mart.com, esto debido a que si fuese un correo legítimo, Este es procesado internamente en Exchange, no pasan por el Servidor Email Gateway, (véase Ilustración III.14).

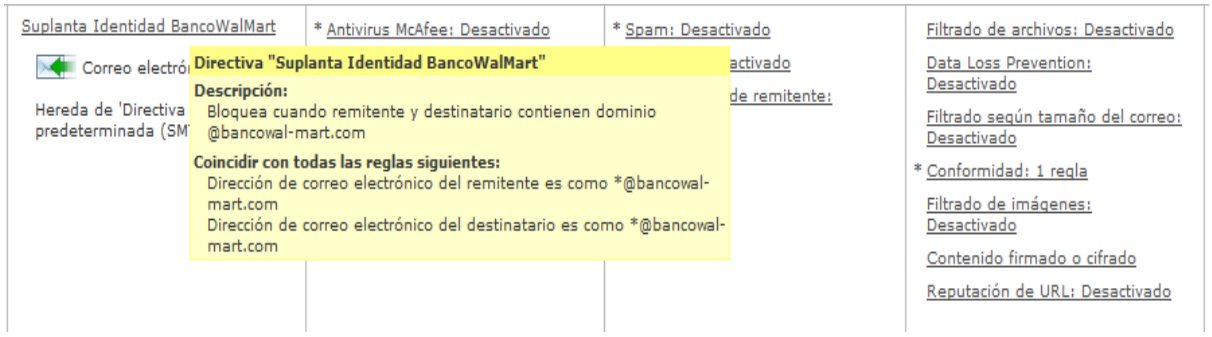


Ilustración III.14 Directiva 1 Suplanta Identidad

III.5.2 Directiva No. 2 Bloquea Correo Entrante

Objetivo: Identificar correos Entrantes de cuentas y dominios registrados en el sistema como potencialmente peligrosos o no deseados, contiene elementos del grupo “DominiosBloqueoEntF” y “UsuariosBloqueoEntF”. Los mensajes de estos usuarios o dominios deben ser bloqueados, en caso contrario será examinada por otra directiva (véase Ilustración III.15).

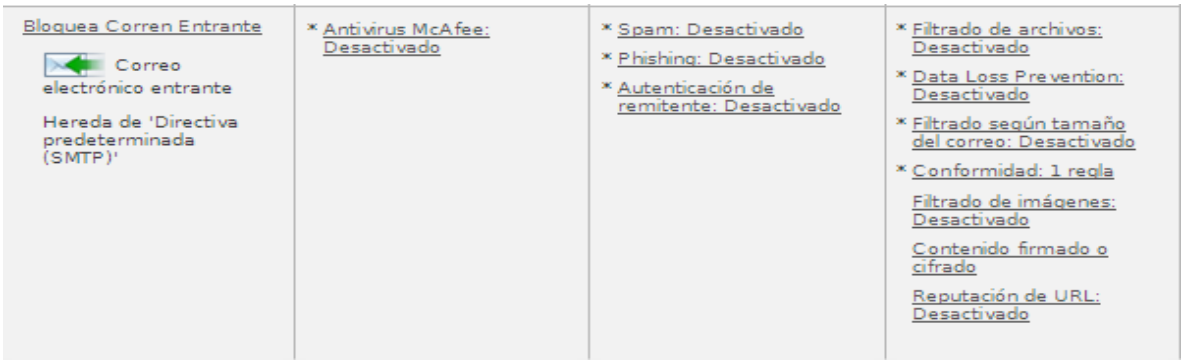


Ilustración III.15 Directiva 2 Bloquea Correo Entrante

No aplica política antivirus, antispam, ni opciones de directiva, debido a que se basa en dos grupos, si el remitente o el dominio del remitente pertenecen a cualquiera de estos grupos se niega la conexión, como podemos observar en la Ilustración III.16.

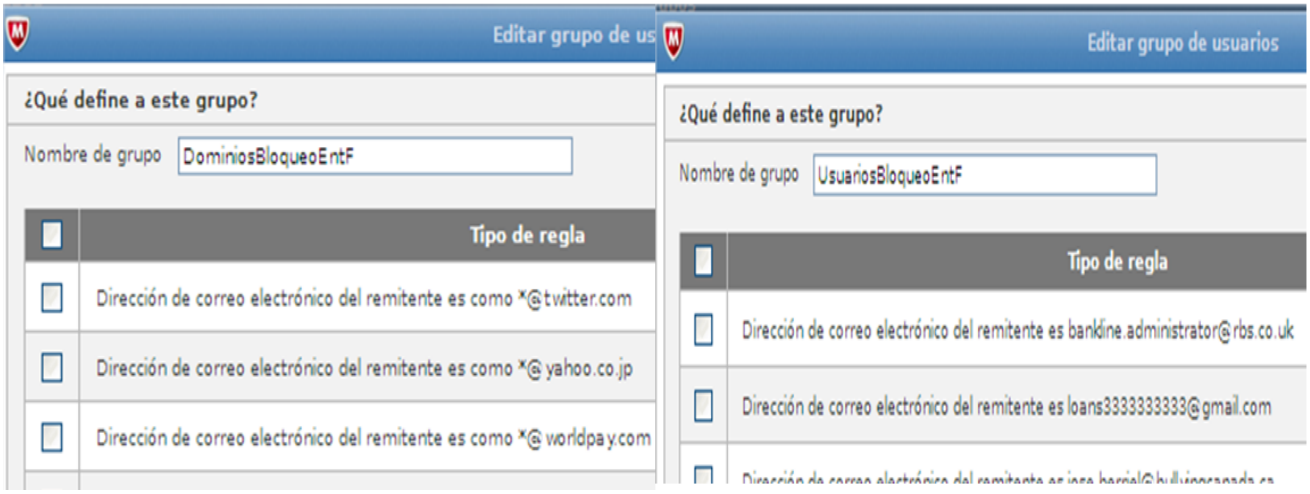


Ilustración III.16 Grupos de bloqueo usuarios y dominios entrantes

III.5.3 Directiva No. 3 Bloquea Usuarios sin Email

Objetivo: Identificar correos entrantes y salientes de usuarios del dominio **bancowal-mart.com** que solo pueden enviar y recibir correos internos, este grupo contiene elementos del grupo "Usuarios Sin Email" registrado en el Directorio Activo de Windows, (véase ilustración III.17).

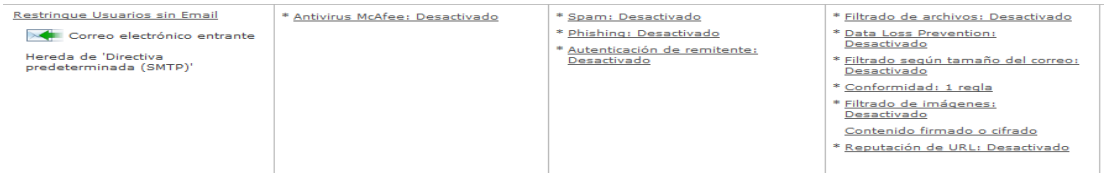


Ilustración III.17 Directiva 3 Bloquea Usuarios sin Email

Si aplica política de Conformidad para bloquear envío y recepción de dominios externos.

Esta directiva aplica a los grupos previamente establecidos en el directorio activo de Microsoft toda persona que se encuentre dentro de dicho grupo solo podrá enviar y recibir correos internos:

Los usuarios del grupo se validan contra el directorio activo de Windows mediante consultas LDAP, como podemos ver en la ilustración III.18, de manera que los integrantes se dan de alta en el directorio activo y no en el Email Gateway.

Esta regla aplicara para entrada y salida de correos ya que exige que ambos correos y destinatario pertenezcan a los dominios locales de Wal-Mart.

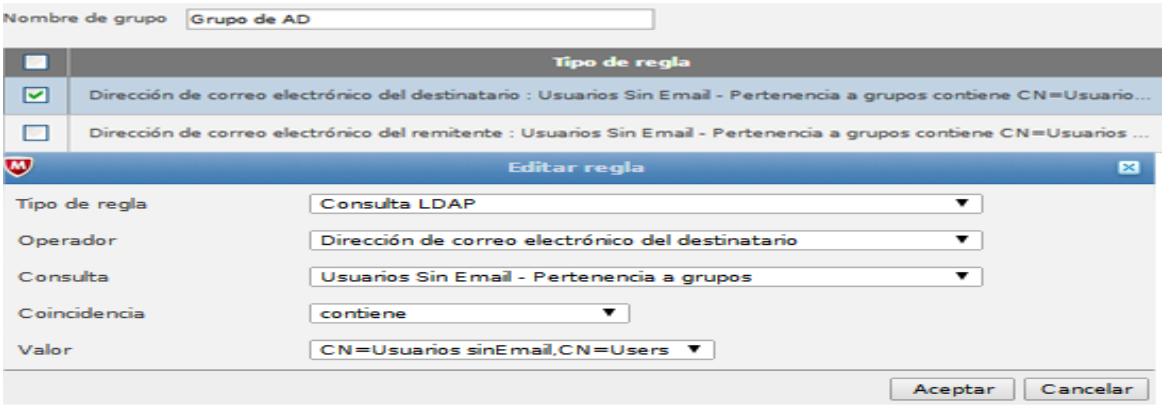


Ilustración III.18 Consulta LDAP

III.5.4 Directiva No. 4 Bloquea Correo Saliente

Objetivo: Identificar correos SALIENTES de cuentas y dominios registrados en el sistema como potencialmente peligrosos o no deseados, en la ilustración III.19 podemos observar la configuración de la directiva, este grupo contiene elementos del grupo “DominiosBloqueoSalT” y “UsuariosBloqueSalT”, como podemos observar en la ilustración III.20. Los mensajes de estos usuarios o dominios deben ser bloqueados.

Ilustración III.19 Directiva 5 Bloquea Correo Saliente

No aplica inspección de antivirus, antispam, ni opciones de directiva. Solo Conformidad que es un diccionario para todos los destinatarios.

Esta directiva aplica para los siguientes grupos de destinatarios no permitidos:

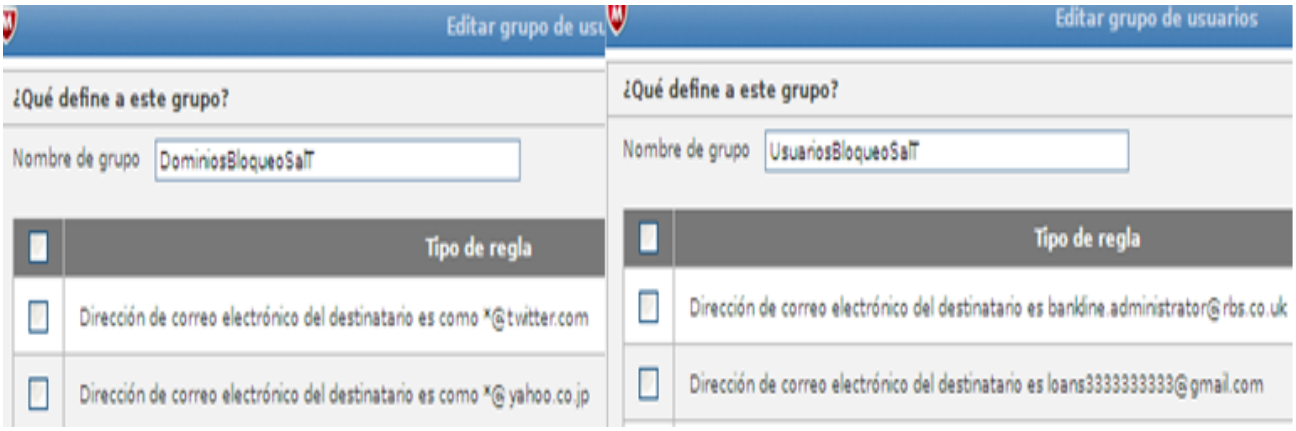


Ilustración III.20 Grupos de bloqueo usuarios/dominios salientes

III.5.5 Directiva No. 5 Confiables Entrantes

Objetivo: Identificar correos entrantes de dominios conocidos, en la ilustración III.21, podemos observar la configuración de la Directiva. Los mensajes de usuarios o dominios deben tener una revisión básica de seguridad, como podemos observar en la ilustración III.22, el caso de la revisión de antivirus, para que circulen más rápido. Se agrupan en el grupo ListaBlancaEntr_Remi.

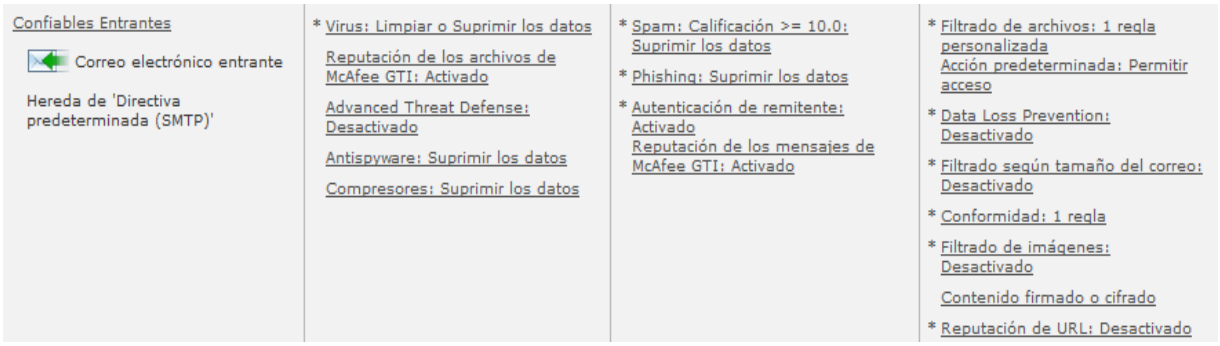


Ilustración III.21 Directiva Confiables Entrantes

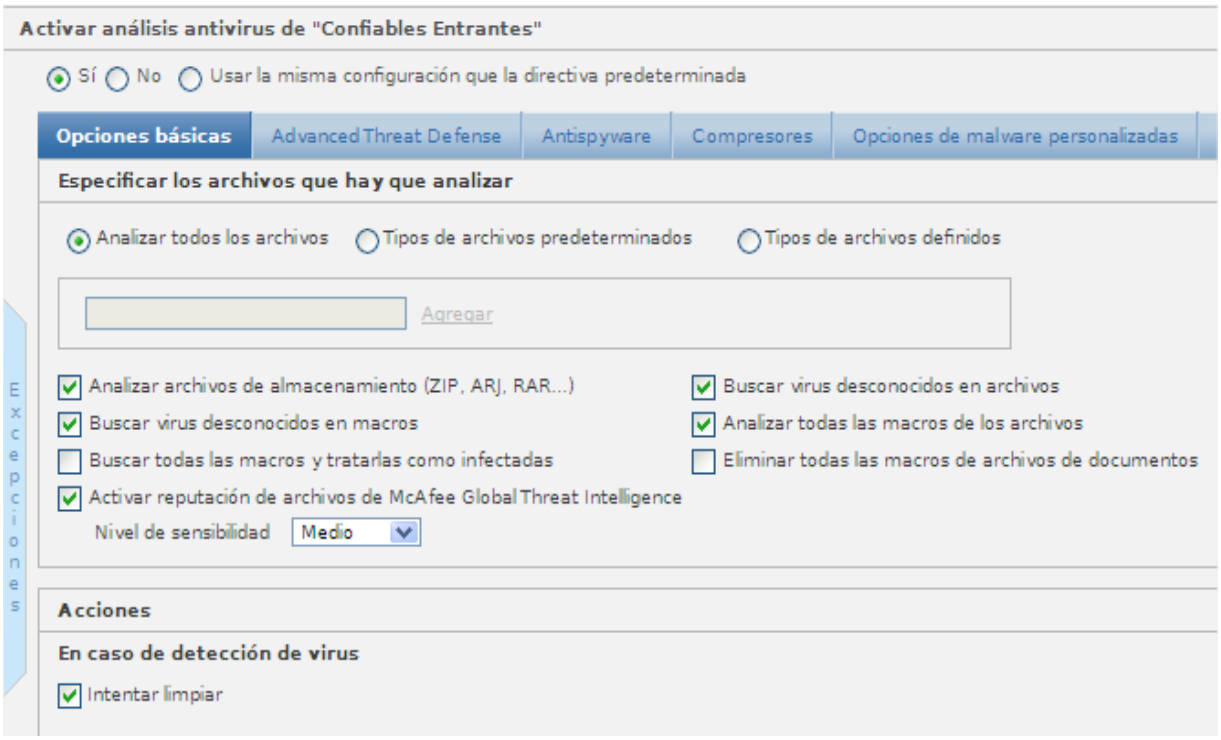


Ilustración III.22 Antivirus confiables entrantes

El análisis del antivirus tiene como acción en caso de detección “Intentar limpiar” y si se produce un fallo en la limpieza, no permitirá que el correo sea entregado y será colocado en cuarentena, como podemos ver en la siguiente ilustración III.23.

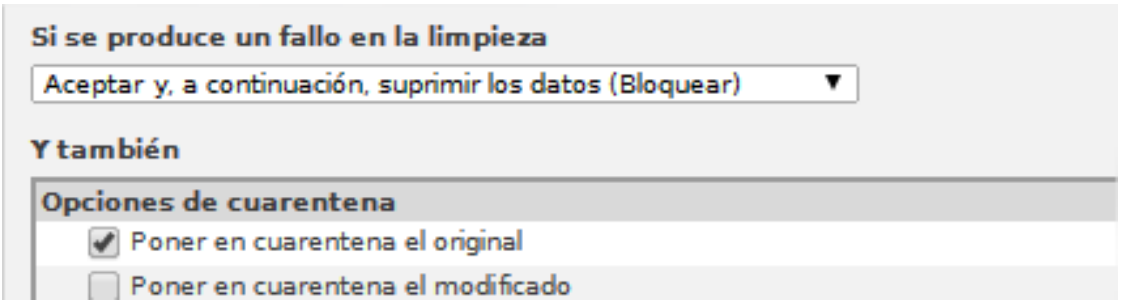


Ilustración III.23 Limpieza antivirus.

En la inspección de conformidad de esta política se filtran los archivos conforme a la regla “Sin ejecutable”, la cual bloqueara todo correo que contenga adjunto un ejecutable de Windows.

III.5.6 Directiva No. 6 Entrantes

Objetivo: Identificar correos Entrantes no pertenecientes a los dominios locales del grupo Wal-Mart, los cuales deben pasar por políticas diferentes a las generales para su revisión, (véase ilustración III.24 Directiva Entrantes), se valida el origen y destino del correo por medio de listas blancas, en caso de no pasar los filtros se envían a cuarentena.

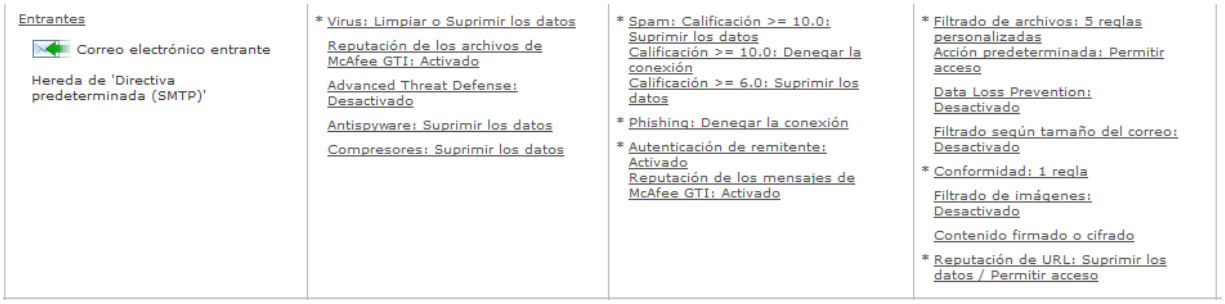


Ilustración III.24 Directiva Entrantes

Al igual que la política “Confiables Entrantes” los motores de antivirus, antispam y antipishing, hacen un análisis en busca de cualquier elemento que sea catalogado

como potencialmente peligroso y lo intenta limpiar en caso de que no se logre, el correo quedara bloqueado y en cuarentena.

Para el tema del antispam se basa en la condición de que el correo entrante sea sospechoso o no, para ello, existen reglas las cuales cuentan con una puntuación definida por McAfee y que la sumatoria de dichas puntuaciones se encuentre dentro de los rangos definidos.

Marcar cuando calificación sea del rango de >= 6.0 a (sospechoso) y cuando sea <= 10 (muy sospechoso). Si la calificación final del correo en base a todas la reglas que sean encontradas en él, se encuentra dentro de dicho rango será catalogado según su nivel que va de sospechoso a muy sospechoso, siendo los sospechosos atrapados por el MEG y colocando una copia en cuarentena y los muy sospechosos rechazados para que ni siquiera ingresen al dispositivo.

Ilustración III.25 Calificación de reglas de SPAM

Obsérvese en la ilustración III.25 que son 24,497 reglas para validar si es spam (validadas 10/agosto/15) cada una con su respectiva calificación.

Si la revisión de antiphishing encuentra algo malo y se activa, la conexión es bloqueada, el correo no debe ingresar al equipo, (véase ilustración III.26).

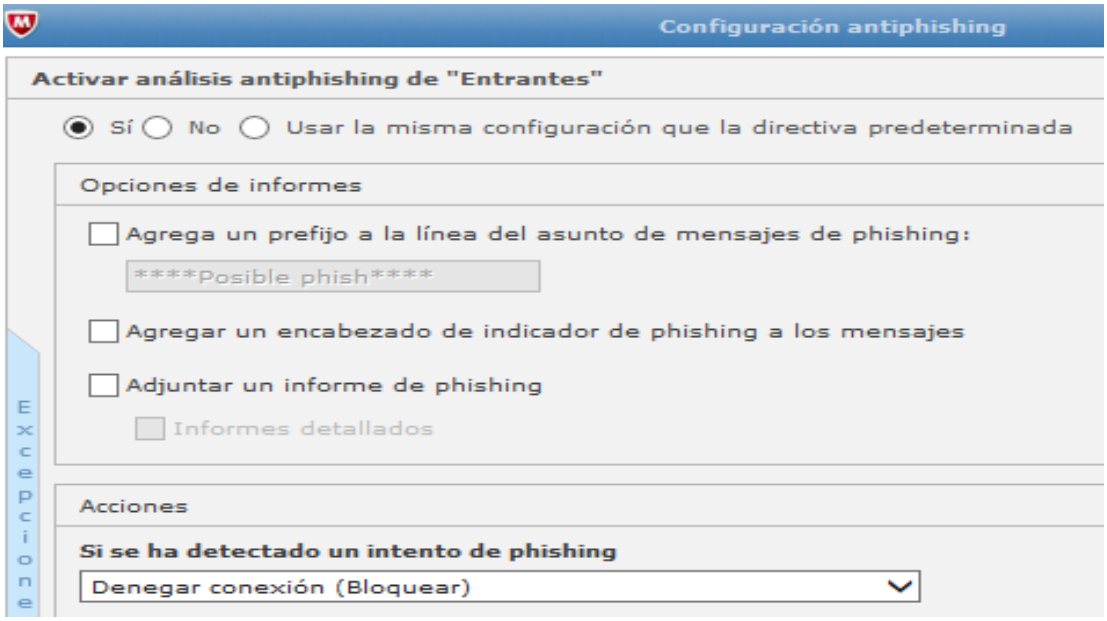


Ilustración III.26 Antipishing Entrantes

En la inspección por filtrado de archivos de esta directiva de basa en las reglas "Multimedia", "Comprimidos2", "Bloquearcab", "Comprimidos" y "No Ejecutables", (véase Ilustración III.27), para poder deliberar si la conexión es negada o aceptada en cualquier caso el original se guarda en cuarentena.

Ilustración III.27 Reglas de Filtrado de contenido.

El análisis de conformidad de esta política es muy similar al filtrado de archivos, se activan reglas, donde la acción si se cumple esta regla es “Aceptar y a continuación, Bloquear” y también “Poner el original en cuarentena”.

Este par de reglas indican que el campo Asunto en el correo Electrónico no debe tener expresiones como las listadas en el diccionario “Asunto Correos”, como se muestra en la ilustración III.28, y que la reputación de la URL no sea sospechosa, donde McAfee hace una comparación con sus bases de datos y verifica las estadísticas de envíos y recepciones de la dirección.

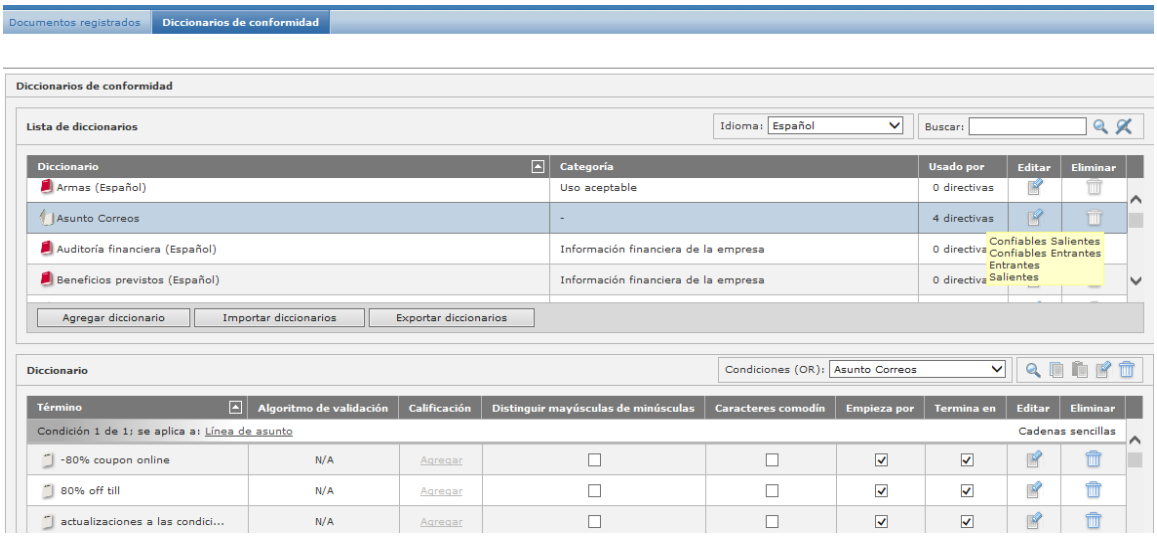


Ilustración III.28 Diccionario Asunto Correos

III.5.7 Directiva No. 7 Confiables Salientes

Objetivo: Identificar correos Salientes de dominios o usuarios conocidos, deben tener una revisión básica de seguridad, como se observa en las ilustraciones III.29 y III.30.

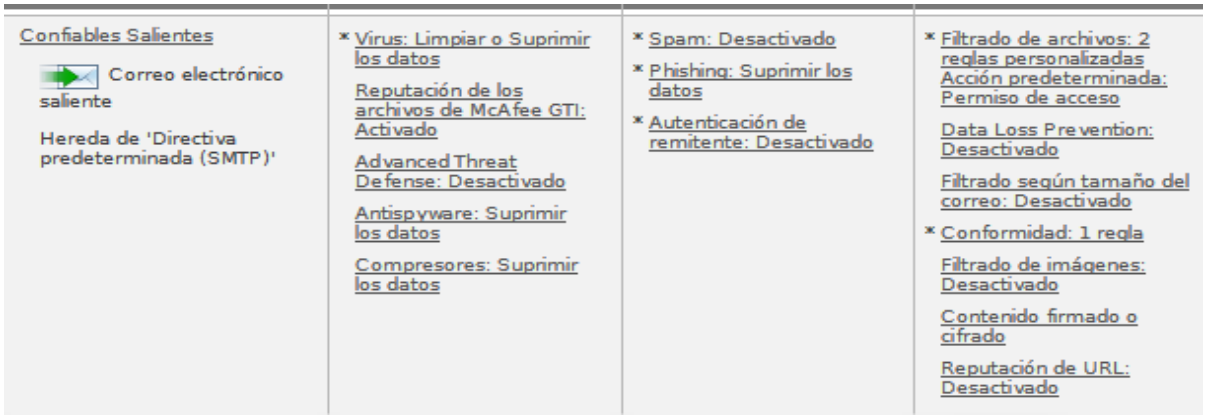


Ilustración III.29 Directiva 8 Confiables Salientes

Se agrupan en el grupo ListaBlancaSal_Dest

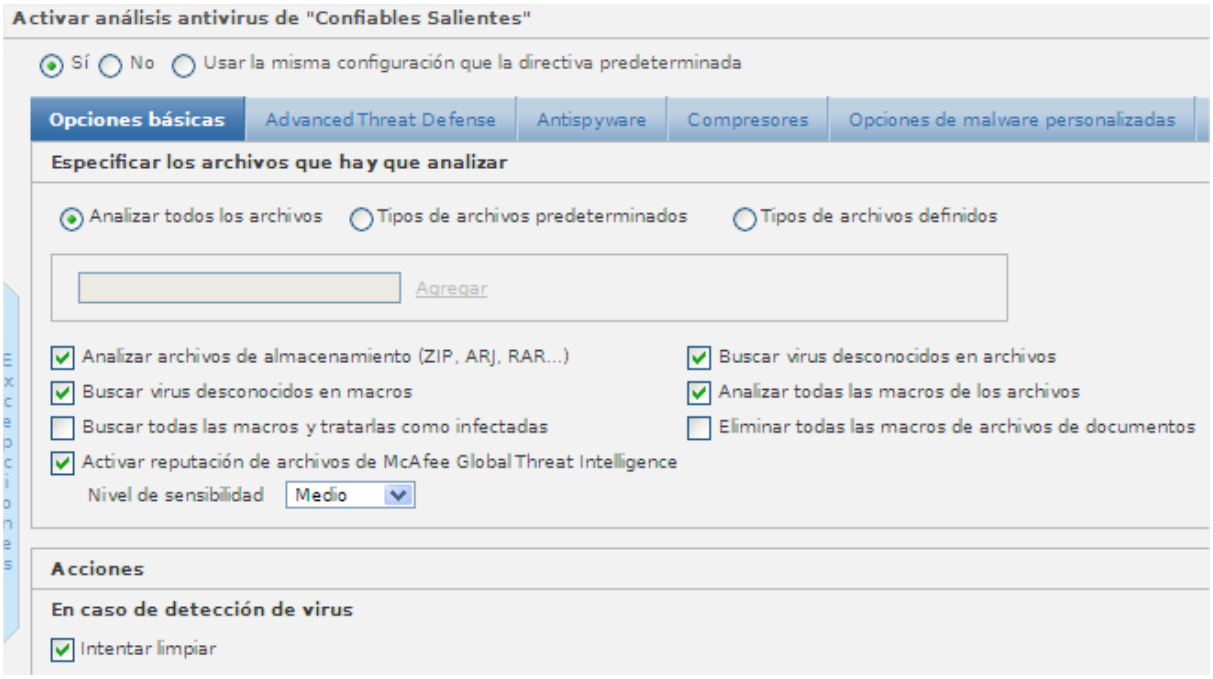


Ilustración III.30 Antivirus Confiables Salientes

En la sección del filtrado de archivos todo mensaje que contenga elementos comprimidos son validaos minuciosamente para asegurarnos de que no se está violando alguna política y todos los correos que contengan elementos ejecutables son bloqueados y puestos en cuarentena, para validación por personal de Seguridad de la Información, en base a reglas, como se muestra en la ilustraciones III.31.

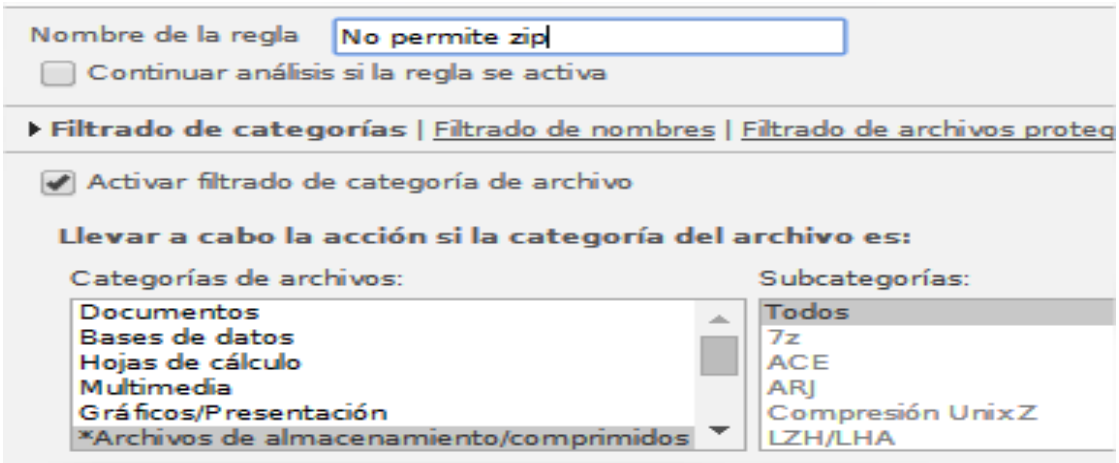


Ilustración III.31 Configuración de reglas No permita Comprimidos.

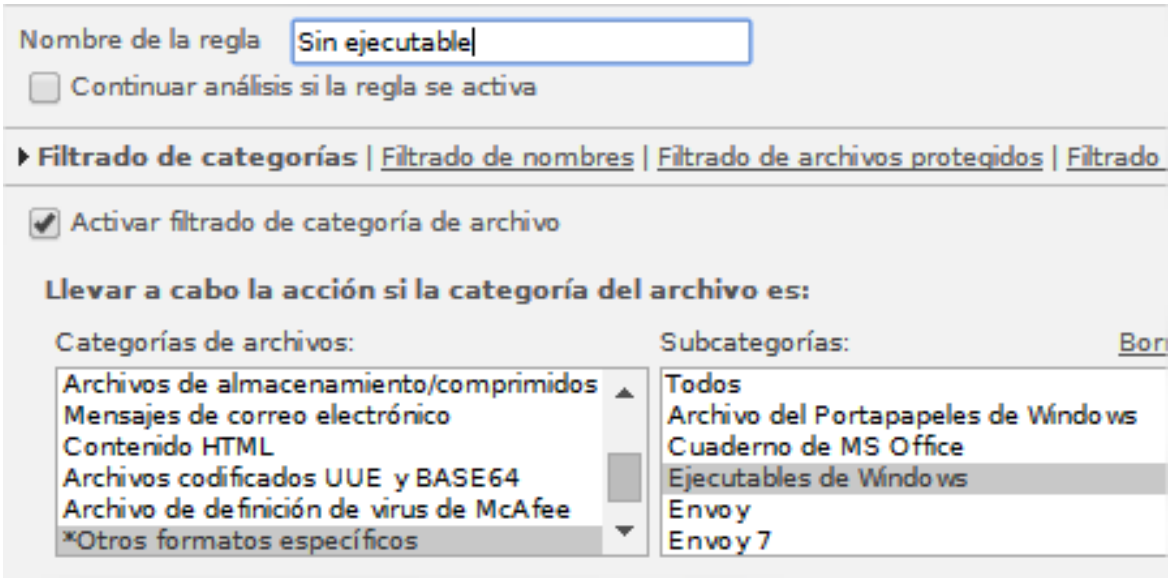


Ilustración III.32 Configuración de regla Sin Ejecutable

En la Ilustración III.32 la regla sin ejecutable aplica para todos los correos que contengan ejecutables de Windows y las acciones son que se bloquea la conexión, y guarda el original en cuarentena.

Aplica política de Conformidad – Conformidad

Diccionario Asunto correo/ permiso de acceso / confiables salientes

El diccionario “Asunto Correo” tiene las palabras o frases que permiten identificar correos peligrosos o no deseados.

III.5.8 Directiva No. 8 Salientes

Objetivo: Identificar correos Salientes dirigidos a dominios no pertenecientes a los locales del grupo Wal-Mart pero con origen en grupo de “Servidores Internos”, los cuales deben pasar por políticas diferentes a las generales para su revisión como se puede observar en l Ilustración III.33.

Se valida el origen y destino del correo, en caso de no pasar los filtros se envían a cuarentena, aplican políticas generales de seguridad para enviar correo limpio.

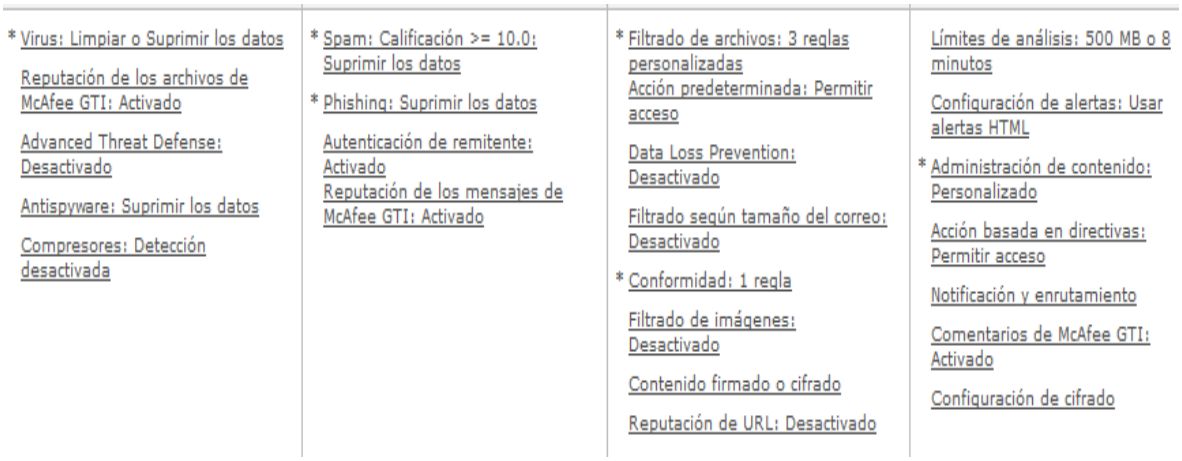


Ilustración III.33 Directivas 9 Salientes

Aplican políticas antivirus, antispam y conformidad y opciones de directiva, como se muestra en la Ilustración III.34.

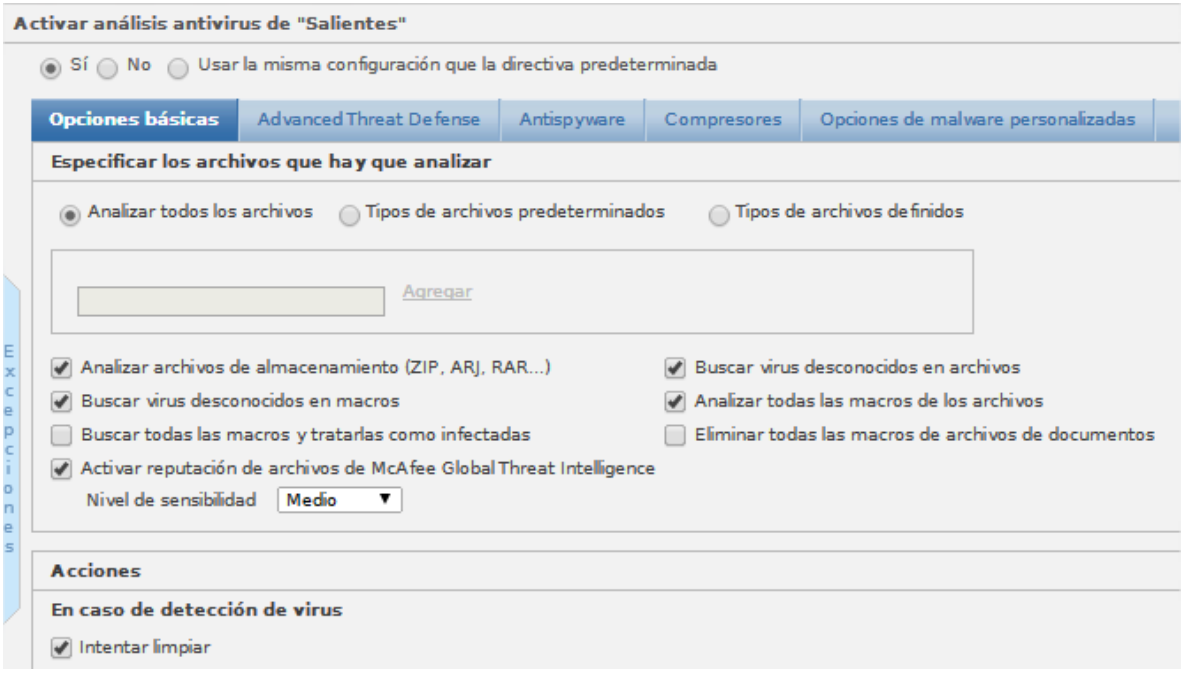


Ilustración III.34 Antivirus Salientes

Si se produce un fallo en la limpieza, bloquea el correo y pone el original en cuarentena.

En la directiva “Salientes” la validación de antispam es menos rigurosa ya que solo se valida y se activa siempre y cuando la calificación sea mayor o igual a 10 en este

caso el correo entra al dispositivo, pero es bloqueado y se coloca el original en cuarentena, la validación de antipishing tiene un tratamiento muy similar ya que solo si se activa la regla el correo es atrapado por el dispositivo y lo coloca en cuarentena.

En la sección de conformidad de esta directiva en realidad deja pasar los archivos adjuntos para su entrega al destinatario siempre y cuando no sea detectado por alguna regla como "Asunto Correos", "No ejecutables", "No comprimidos" y sobre todo no información confidencial como datos personales, cuentas bancarias, contraseñas.

En casos donde las directivas ya sea "salientes o confiables salientes" sean activadas se cuenta con una acción única en el área de "Administración de Contenido", que es la configuración de un aviso como se puede observar en la Ilustración III.35.

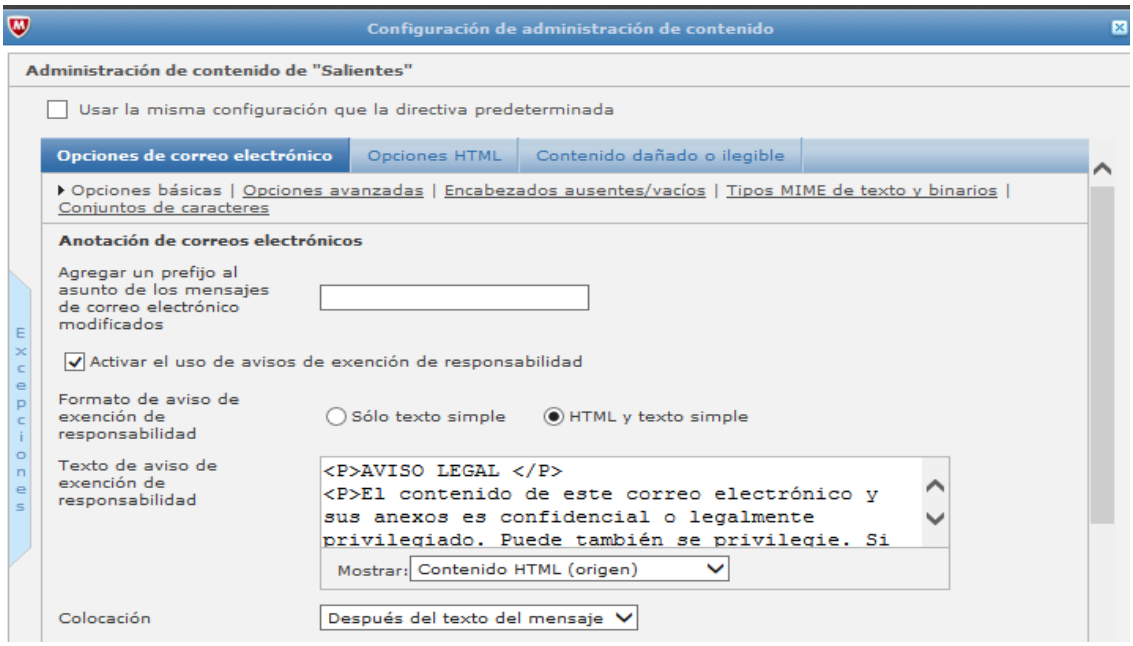


Ilustración III.35 Configuración de etiqueta empresarial

III.5.9 Directiva No. 9 General / Predeterminada

Objetivo: Esta directiva solo es la plantilla general del dispositivo una vez que se seleccionó se le cambia el nombre y podemos empezar a identificar sus acciones a

ejecutar, como se muestra en la Ilustración III.36, no viene configurado nada pero si realiza un análisis básico de antivirus, antispam.

Ilustración III.36 Resumen Directiva 10 General

III.6 Implementación MEG 4500 Septiembre 2014

Se ingresó el equipo MEG 4500 y se le configuraron los parámetros necesarios del sistema.

Una vez que se termina esta actividad, el equipo ya se encuentran dentro del centro de datos conectado a la energía eléctrica y a la red interna, ya se puede tener una administración remota y así se pudo realizar la configuración que estaba planeada para producción, en la cual el proceso fue el siguiente.

1. Configurar con la última versión el MEG 4500
2. Configuración de Políticas, acorde a la necesidad del negocio
3. Revisión de correo, acorde a las políticas configuradas. Y se detectó que los indicadores de correos bloqueados se estaban comportando de una manera muy anormal, por esta razón y dentro de la misma ventana de tiempo se inician los siguientes ajustes:
    a) Modificar Directiva predeterminada para que Permita pasar, quitando la anterior Denegar Conexión y se cambia a la forma de Aceptar y Bloquear
    b) Eliminar diccionario Blasfemia porque estaban entrando muchos correos en dicha política, se eliminó de directivas, Entrantes, Confiables Entrantes, Salientes, Confiables Salientes debido a que tiene variaciones por los idiomas y contextos de las oraciones

Se verificó que después de los ajustes realizados el comportamiento fue el esperado y se validó que la regla de Aceptar y Bloquear más la acción enviar a Cuarentena está generando 2 correos, uno por cada acción, como se muestra en la Ilustración III.37, estos correos después de un tiempo serán eliminados por el dispositivo.

inspecciones@empre...	jurquiza@bancowal-...	Como atender y resolver inspecciones de las autoridades en materia laboral	Entrantes	En cuarentena: Antispam
inspecciones@empre...	jurquiza@bancowal-...	Como atender y resolver inspecciones de las autoridades en materia laboral	Entrantes	Bloqueado: Antispam

Ilustración III.37 Correo bloqueado y en cuarentena

Se agregó Aviso legal en directivas Salientes y Confiables salientes, en la opción Administración de Contenido, para que cada correo que salga del dominio de Banco Wal-Mart contenga un aviso de privacidad, justo como lo podemos observar en la Ilustración III.38.

AVISO LEGAL

El contenido de este correo electrónico y sus anexos es confidencial o legalmente privilegiado. Puede también se privilegie. Si le fue enviado por error, sea tan amable de borrarlo sin revisarlo y por favor hágalo saber al remitente. Por este medio usted queda notificado de que está estrictamente prohibida cualquier divulgación, distribución, copia u otro uso del mensaje o sus anexos. El correo electrónico no es un medio de comunicación 100% seguro, por lo que no garantizamos que las comunicaciones de Internet sean oportunas, seguras,libres de error o virus.

DISCLAIMER

The contents and attachments of this e-mail are confidential or legally privileged. It may also be legally privileged. If it has been sent to you in error, kindly delete it and please notify the sender of the error. You are hereby notified that any dissemenation, distribution, copying, or other use of the message or its attachment is strictly prohibited . E-mail is not 100% secure communication medium, so we do not guarantee that the Internet communications to be timely, secure, error or virus-free.

Ilustración III.38 Aviso Legal para envió correos Banco Wal-Mart

Adicional se agregaron más dominios a Listas Blancas y Negras y se generó un respaldo de configuración.

III.7 Revisión y actualización de equipo MEG 4500B Febrero 2015

Se pretendía dejar actualizado con la versión 7.6.3.2, para permitir actualizar la versión en el MEG 5000.

Para ello se revisó que los parches de actualización que libera McAfee, junto con los DAT y motores de antivirus, spam entre otros estuviesen actualizados al día de hoy 24 de Febrero 2015 a las 3:00 am conforme a lo programado en la configuración del sistema.

Se importó una copia de respaldo de la configuración del MEG 4500 del día, para dejar al equipo nuevo 5000 con la misma configuración.

III.8 Ingreso MEG5000 Febrero 2015

Se cargó la copia de configuración del equipo productivo y se ingresó a producción.

Una vez que el equipo 5000 está en producción, el 4500 se turnó como equipo de desarrollo, pero se requiere que este dentro de la red, para poder realizar cambios y modificaciones, y ver el comportamiento, por ello se le asignó una IP con los privilegios de producción, para ello realice las siguientes actividades.

1. Intercambie las IP del MEG 5000 y del 4500 del ambiente de desarrollo al ambiente productivo respectivamente
2. Cambiar cable del servidor de producción MEG 4500 al MEG 5000, para que el nuevo dispositivo pueda empezar a recibir tráfico de la red y empiece a procesar los correos

El cambio se realizó con éxito, pero se perdió conexión al MEG desde la red 192.168.111.0/24 que es una de las interfaces para tener acceso de manera local, se sigue teniendo conectividad desde mi equipo personal, que se encuentra en la red interna de la empresa, por ello nos es fácil recuperar el control y volver a configurar los parámetros del dispositivo.

III.9 Actualización del Email Gateway a ver 7.6.4 Junio 2015

Producto: MEG 5000C y Email Gateway 7.6.3
MEG 4500B y Email Gateway 7.6.2

Actualmente el Meg5000C tiene la versión 7.6.3.x y el 4500B tiene la versión 7.6.2.2 se trata de actualizarlos a las versiones más reciente 7.6.4 para robustecer la seguridad, de esta manera se mantiene los dos equipos actualizados a la última versión y con la misma configuración, en caso de perder el dispositivo de producción por falla en el hardware o software, solo es cuestión de quitar el cable de red, cambiar la ip del equipo de desarrollo y asignarle la de producción,

Tiempo estimado 160 minutos, acciones a realizar:

1. Preparar equipo MEG 4500B que está como servidor Email Gateway de Desarrollo para actualizar primero
2. Una vez actualizado el MEG 4500B, sustituir al MEG 5000C de producción temporalmente en lo que se realiza el proceso de actualización de este último, también fuera de red, esto debido a que cada actualización implica un reinicio del sistema y los dispositivos MEG se llevan un tiempo aproximado de 15 minutos levantar todos sus servicios
3. Una vez concluida la actualización del MEG 5000C, regresarlo a operación en la red (producción) y mantener en red al MEG 4500B (IP desarrollo)

La finalidad que se hiciera la actualización de manera escalonada y fuera de red era de no interrumpir el servicio de correo, esto debido a que esta ventana de tiempo la programe en horario productivo del banco, y siempre se busca tener el menor impacto al negocio, por esa razón se actualiza un equipo, se ingresa a producción y actualizamos el segundo, una vez que estén listos ambos dispositivos se les asignara su IP correspondiente (producción y desarrollo).

Iniciamos 19:00

1. Aplicando actualizaciones a MEG 4500B

a. Conectarse a través de navegador web: https:// 10.228.X.X:10443
b. En Sistema - Gestión de Componentes – Instalador del paquete
    1. Cargar el archivo: MEG-7.6.3RTW1-3174.zip
    2. Cargar el archivo: MEG-7.6.3.1-3193.zip
    3. Cargar el archivo: MEG-7.6.3.2-3206.zip

Esta actualización no es por paquete .Zip, es desde CD, se tuvo que crear un CD a partir del .iso por eso la demora.

En el proceso se realizó configuración inicial por ser tipo completa y no actualización.

Al concluir la configuración inicial se importó la configuración de Respaldo para tenerla igual que el MEG 5000C, el cambio requirió otro reinicio.

Cargar el archivo: EG-7.6.4-3268-104.zip, concluyo reinicio con actualización 7.6.4 a las 22: 07 horas, por seguridad se reinició el equipo.

2. Procedimiento de intercambio de equipos
    a. Procedemos a intercambiar equipos, el MEG 4500B queda como producción temporalmente en lo que se actualiza el MEG5500C

Se verifica que los correos estén entrando y saliendo a través del Email Gateway.

b. Inicia procedimiento de actualización de MEG 5000C
c. Conexión mediante laptop al MEG 5000C vía interface de administración: https://10.254.10.42
d. En Sistema - Gestión de Componentes – Instalador del paquete

Cargar el archivo: MEG-7.6.4-3268-104.zip y reiniciar equipo.

3. Intercambiar equipos nuevamente quedando:

    MEG 5000C IP: 10.254.10.42 (en producción)

    MEG 4500B IP: 10.254.10.5 (en desarrollo)

Ambos equipos quedan con versión Email Gateway 7.6.4, se realiza una última revisión de flujo de correos entrantes y salientes a través del Email Gateway, para ver el tráfico y los indicadores, y vemos que todo opera con normalidad, fin de cambios 00:51 horas.

IV. PRUEBAS Y APORTACIONES

En este capítulo se presentan, las pruebas realizadas, durante este proyecto, los inconvenientes que se presentaron durante la implementación, el cómo se fue dando solución a cada uno y para finalizarlo se presentan las acciones a manera de recomendación que se pueden realizar a futuro con la herramienta McAfee.

IV.1 Pruebas del Sistema

Las primeras pruebas que se realizaron, fueron directamente en la consola para verificar que el dispositivo físicamente estaba operando de manera correcta, en la Ilustración IV.1 podemos ver un ejemplo de las pruebas que se ejecutaron.

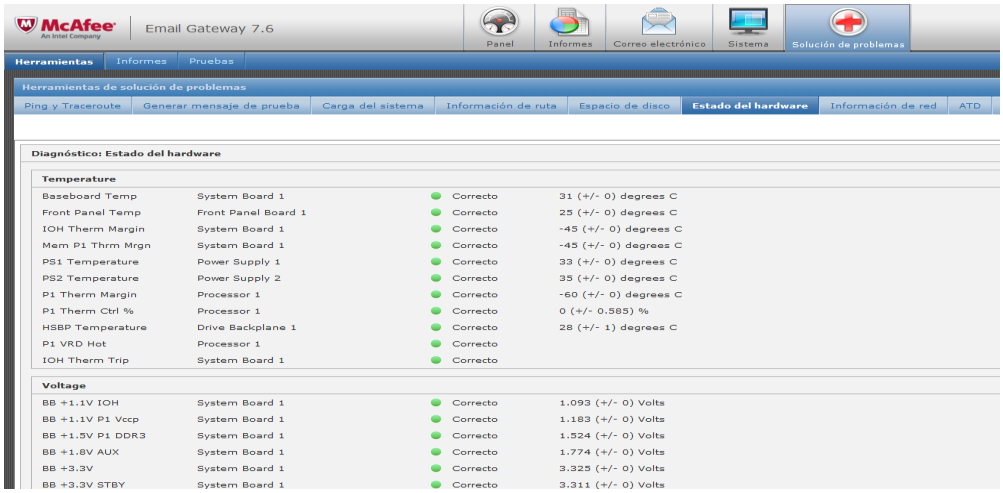


Ilustración IV.1 Estado Físico del Equipo.

También se validó que la configuración de red era la correcta, para ello desde la consola se mandó un trazado de ruta hacia un servidor conocido para validar que la configuración de red es correcta, el resultado de esta prueba lo podemos observar en la Ilustración IV.2.

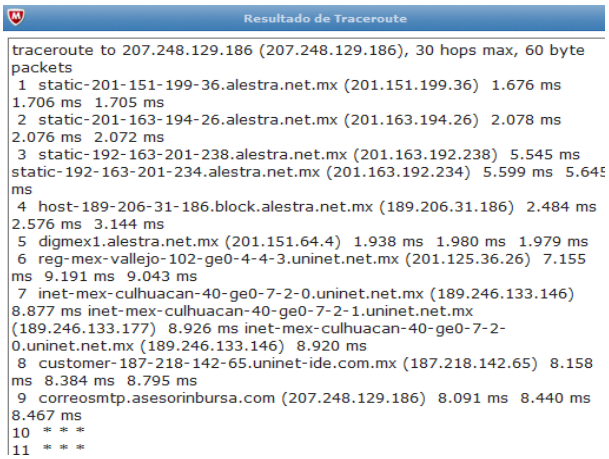


Ilustración IV.2 Traceroute desde consola

Adicional en el apartado de solución de problemas existe un campo que se llama pruebas, y en esta sección se puede obtener de una manera más simplificada un reporte en el cual se indica que es lo que está funcionando de manera correcta o si hay algún aviso, en caso de que la prueba sea exitosa, se colocara una palomita verde al final de ella, si la prueba falla arrojara un círculo rojo con una cruz y si presenta alguna complicación se muestra un triángulo amarillo con un signo de exclamación, el cual indica que está operando, pero no siempre de la mejor manera, puesto que recordaremos que cada administrador va a configurar acorde a las necesidades de la empresa, como lo podemos observar en la Ilustración IV.3.

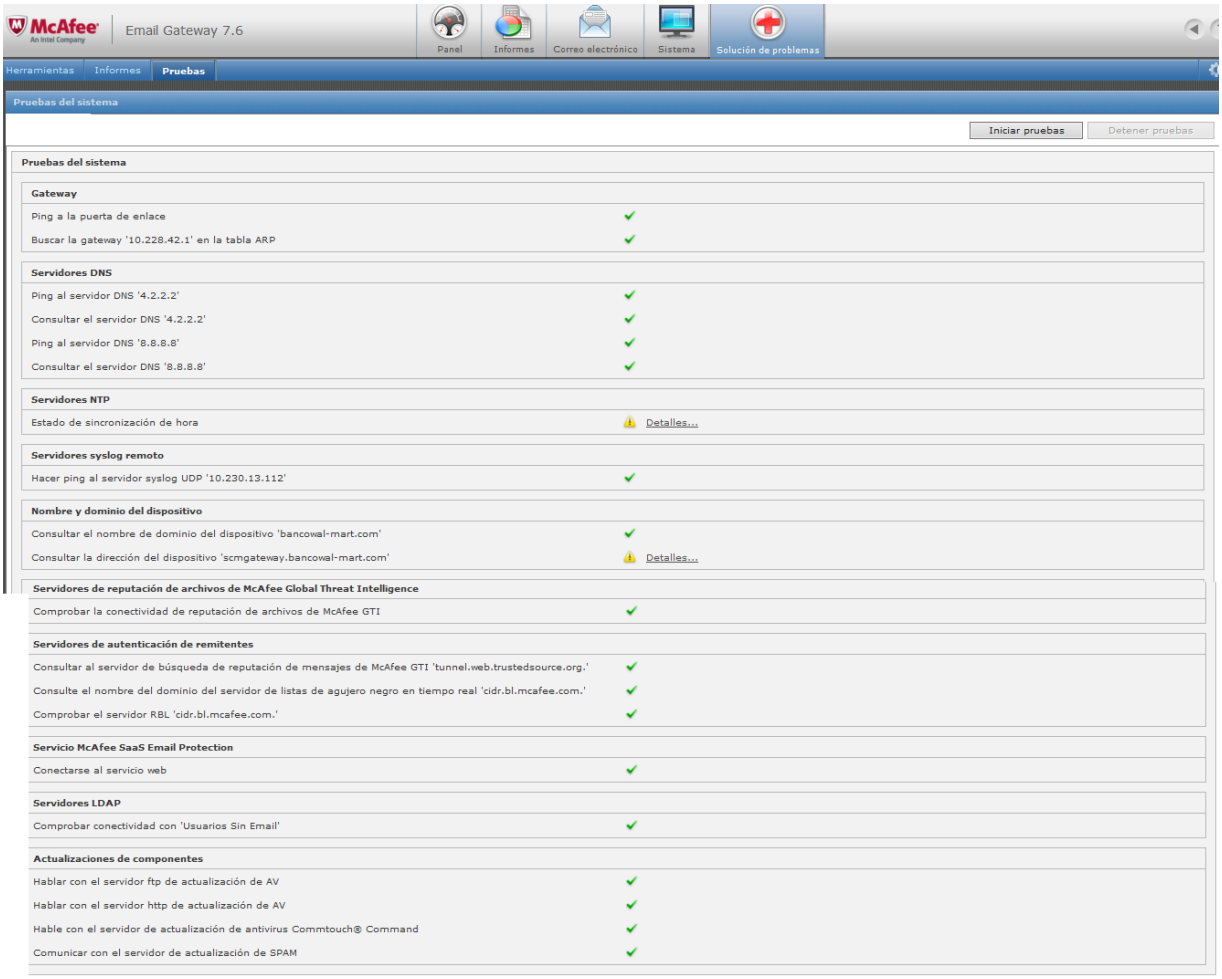


Ilustración IV.3 Pruebas del sistema.

IV.2 Problemas con bloqueo de "Usuarios sinEmail"

Al parecer no se está ejecutando bien la sincronización con Directorio Activo y/o la política no está correctamente definida, se reportan problemas para bloquear correo a grupo "Usuarios sin Email".

Marque al 01800 1233264 donde me canalizaron con un Ing. especialista en Email Gateway, se creó ticket de soporte en McAfee **SR # 4-5959949711**

Realice diferentes intentos para generar una consulta que primero permitiera identificar el grupo "UsuariossinEmail" y después una política que bloqueara Entrada de correos desde el exterior y la Salida al exterior, permitiendo el envío y recepción de correos al grupo solo en el dominio @bancowal-mart.com, después de varios intentos mi consulta no encontraba el grupo hasta que se escribiera "Usuarios%20sinEmail", por cuestiones del espacio.

El Directorio Activo no tiene a todos los usuarios bajo el grupo "Usuarios", existen grupos como "Office" y usuarios personales en el mismo nivel, lo que dificulta ubicar a todos los usuarios del grupo "Usuarios sinEmail".

Se presentaron algunas complicaciones y no encontré la forma de generar la consulta ya que mi consulta era de manera estática, por lo que el Ing. de soporte, me enseñó cómo generar una lista o diccionario basado en una consulta LDAP dinámica, y así poder actualizar con los cambios de usuarios en el Directorio Activo.

El ingeniero de soporte me sugirió actualizar la versión 7.0.2 a 7.6.2 que es la más reciente antes de replicar la configuración en el equipo 5000.

Con esto se concluyó el SR # 4-5959949711

IV.3 Generación de correos de alerta a usuarios con correos en cuarentena

Se detectó que a todo usuario que mandase algún correo y este fuese puesto en cuarentena se le mandaba un mensaje de alerta, que le indicaba que su correo fue atrapado y que se comunicara con el administrador, esta acción es no deseada por generar tráfico extra y molestia entre los usuarios, por tal motivo se debe desactivar la opción de Resúmenes, misma que encontraremos como la Ilustración IV.4

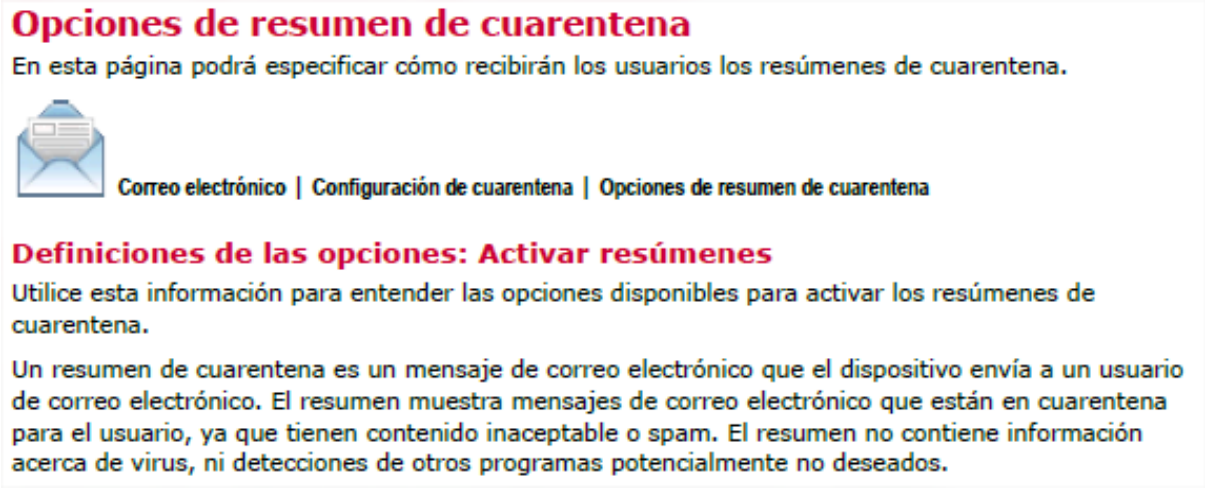


Ilustración IV.4 Alerta Cuarentena predeterminada

En la configuración inicial del MEG se deseaba que el equipo generará reportes automáticos para los Administradores del sistema, pero dichos reportes no eran para los administradores, eran para los remitentes de cualquier correo atrapado en la cola de cuarentena, cuando los usuarios reciben alguna notificación se alarman y empiezan a saturar de llamadas a Seguridad de la Información, se decide desactivar dicha acción.

IV.4 PDF adjunto, sin virus pero bloqueado como “archivo dañado” Octubre 2014

Fue difícil detectar que política estaba aplicando la acción de bloquear, finalmente se ubicó en la directiva: Entrantes

Opciones de directiva – Administración de Contenido – Contenido dañado o Ilegible

La directiva estaba configurada como se muestra en la Ilustración IV.5, para CONTENIDO DAÑADO y ARCHIVOS PROTEGIDOS (Contraseñas)

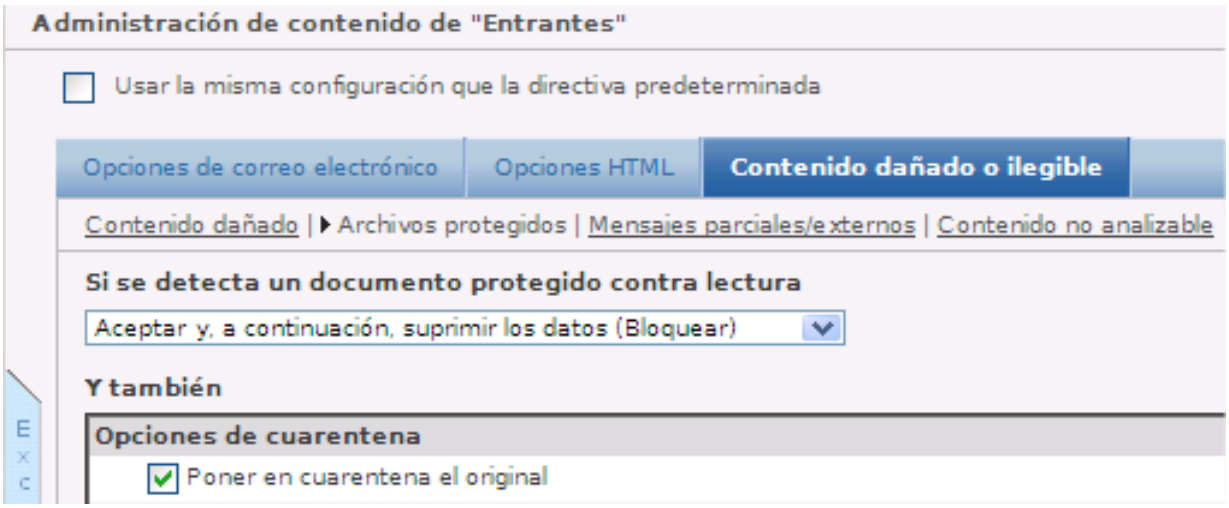


Ilustración IV.5 Acción contenido dañado o ilegible "Entrantes"

Se modificaron para simplemente dejar pasar (SUPERVISAR), quedando como la Ilustración IV.6.

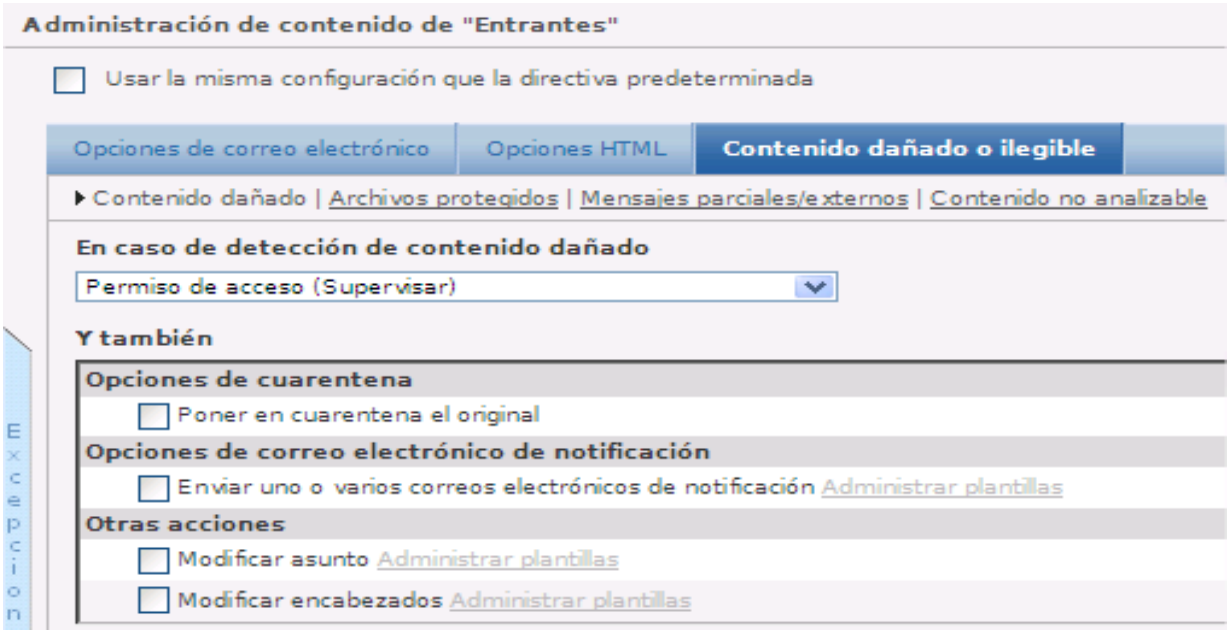


Ilustración IV.6 Permiso de acceso contenido dañado "ENTRANTES"

IV.5 Correos del área de fraudes, no están saliendo Noviembre 2014

El área a donde se envían estos correos recientemente aplico ajustes para evitar la vulnerabilidad de TLS [21] 3.0

Se revisaron las conversaciones de los mensajes encontrando que el MEG procesa el correo y lo analiza correctamente pero cuando inicia la entrega, en la parte de abrir conexión TLS [21], esta se inicia pero a continuación indica el error: **"451 System problem: retry later (critical disk space error)**", véase Ilustración IV.7

Mar Nov 04 2014 11:18:47	RESET	<	**RSET**
Mar Nov 04 2014 11:18:51	ENTREGA		Intento de entrega en Tue Nov 4 11:18:50 CST 2014
Mar Nov 04 2014 11:18:51	ENTREGA		Realizando búsqueda de entrega para Fraudalerts@tsys.com
Mar Nov 04 2014 11:18:51	ENTREGA		La búsqueda de entrega Fraudalerts@tsys.com ha resultado en 65.240.184.225:25
Mar Nov 04 2014 11:18:51	ENTREGA		Búsqueda de entrega llevada a cabo correctamente; iniciando entrega
Mar Nov 04 2014 11:18:51	ENTREGA		Realizando búsqueda de entrega para JDiaz@tsys.com
Mar Nov 04 2014 11:18:51	ENTREGA		La búsqueda de entrega JDiaz@tsys.com ha resultado en 65.240.184.225:25
Mar Nov 04 2014 11:18:51	ENTREGA		Búsqueda de entrega llevada a cabo correctamente; iniciando entrega
Mar Nov 04 2014 11:18:51	ENTREGA		Intentando conectarse a 65.240.184.225
Mar Nov 04 2014 11:18:51	ENTREGA		Conexión correcta
Mar Nov 04 2014 11:18:51	ENTREGA	>	**EHLO scmgateway.bancowal-mart.com**
Mar Nov 04 2014 11:18:51	ENTREGA	<	**250 Requested mail action okay, completed.|STARTTLS**
Mar Nov 04 2014 11:18:51	ENTREGA	>	**STARTTLS**
Mar Nov 04 2014 11:18:52	ENTREGA	<	**220 Start TLS negotiation.**
Mar Nov 04 2014 11:18:52	ENTREGA		Conexión segura. Cifrado: TLS: TLSv1/SSLv3, 256bits, AES256-GCM-SHA384
Mar Nov 04 2014 11:18:52	ENTREGA	>	**EHLO scmgateway.bancowal-mart.com**
Mar Nov 04 2014 11:18:52	ENTREGA	<	**250 Requested mail action okay, completed.**
Mar Nov 04 2014 11:18:52	ENTREGA	>	**MAIL FROM:<marces@bancowal-mart.com>**
Mar Nov 04 2014 11:18:57	ENTREGA	<	**451 System problem: retry later. (Critical disk space error)**

Ilustración IV.7 Error al iniciar conexión TLS

Se realizaron pruebas de envío de correos sencillos a jjorozco@ipdsa.com por parte del remitente usuario@bancowal-mart, mismos que llegaron sin problemas. Con esto se descartó que el buzón del usuario tuviera problemas de espacio.

Se revisaron las estadísticas del disco duro en la consola.

El área de logs muestra una ocupación "baja", cuando se pensaba que pudiera estar cerca del nivel de saturación

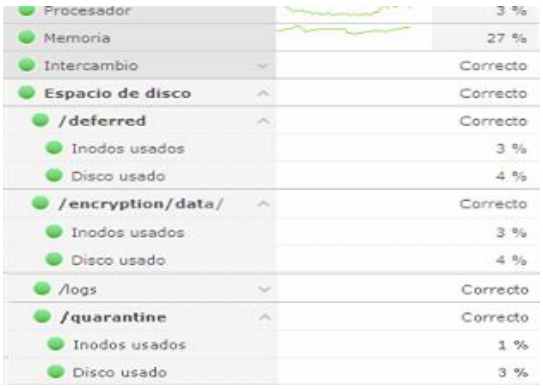


Ilustración IV.8 Estadísticas de MEG

El área de cuarentena donde se encolan los mensajes también muestra niveles bajos, como podemos observar en la Ilustración IV.9

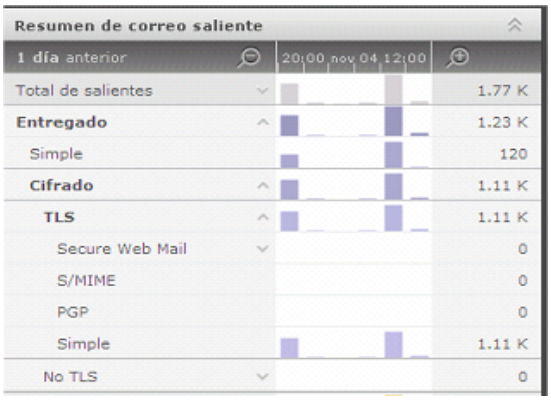
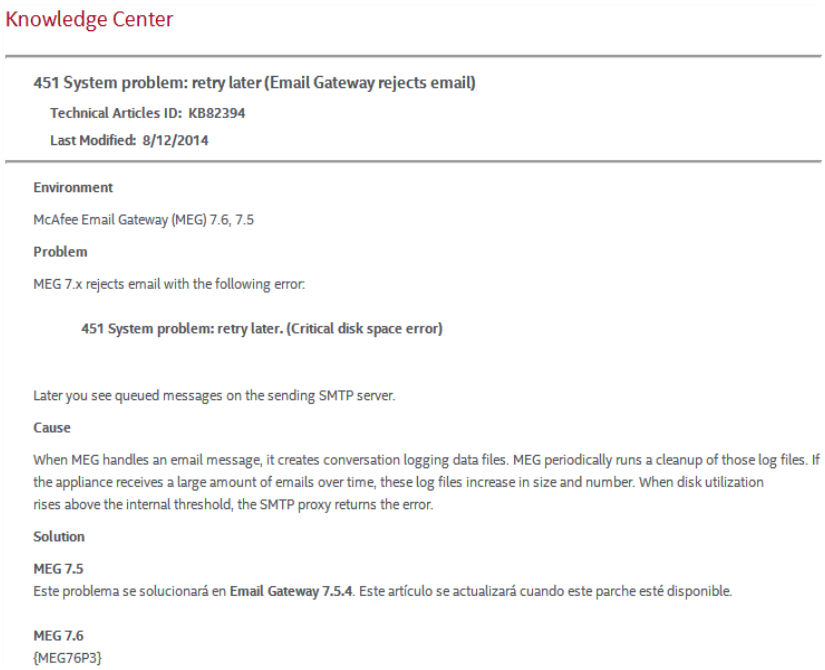


Ilustración IV.9 Estadísticas Correo Saliente

McAfee indica en su centro de apoyo y conocimientos de productos McAfee como se muestra en la Ilustración IV.10, que este problema es por la falta de los archivos logs y que se corrige actualizando a la versión 7.6.3.


Knowledge Center

451 System problem: retry later (Email Gateway rejects email)

Technical Articles ID: KB82394

Last Modified: 8/12/2014

Environment

McAfee Email Gateway (MEG) 7.6, 7.5

Problem

MEG 7.x rejects email with the following error:

451 System problem: retry later. (Critical disk space error)

Later you see queued messages on the sending SMTP server.

Cause

When MEG handles an email message, it creates conversation logging data files. MEG periodically runs a cleanup of those log files. If the appliance receives a large amount of emails over time, these log files increase in size and number. When disk utilization rises above the internal threshold, the SMTP proxy returns the error.

Solution

MEG 7.5

Este problema se solucionará en **Email Gateway 7.5.4**. Este artículo se actualizará cuando este parche esté disponible.

MEG 7.6

{MEG76P3}

Ilustración IV.10 Base de conocimiento McAfee error 451

Se realizó la aplicación del parche para la vulnerabilidad en el MEG 4500 para observar si corrige el problema y posterior al MEG 5000.

IV.6 Correos de HSBC y otras compañías con propaganda, deberían ser atrapados Enero 2015

Se detectaron correos falsos con propaganda de otras entidades financieras, como el ejemplo que se muestra en la Ilustración IV.11, mismos que por sus características deben ser considerados como spam.

Ilustración IV.11 Notificación de SPAM a usuarios

El problema es detectado en las directivas Entrantes y Confiables Entrantes.

Valide que las bases de datos de URL y motor spam estuvieran actualizadas, revise las directivas y realice ajustes para elevar un poco el nivel de filtrado de spam.

Directiva ENTRANTES:

SPAM: Se modificó el valor para clasificar un correo como SPAM, se tenía en mínimo 10, se ajustó a mínimo 6.

Directiva Confiable ENTRANTES:

SPAM: Se modificó el valor para clasificar un correo como SPAM, estaba inactivo, se ajustó a mínimo 10.

Se aplicó más rigor, puesto que se entiende que en la directiva Confiables Entrantes se supone que ya están validados los remitentes.

Se activó la Autenticación de Remitente que estaba deshabilitada pero la acción a aplicar se dejó en “Supervisar”.

IV.7 Alta incidencia de correos con archivos adjuntos Febrero2015

Comenzaron a llegar a la Directiva “Entrantes” correos para usuarios del dominio “@bancowal-mart.com” con mensajes extraños y archivos adjuntos del tipo:

- Nombre_usuario@bancowal-mart.com.zip
- .cab

Se revisaron las versiones de la Base de datos y el motor Antivirus encontrándolas actualizadas

De igual manera la regla Antivirus tiene un nivel de sensibilidad “MEDIO”, intentando limpiar y si falla la limpieza lo coloca en cuarentena.

Se crearon dos nuevas reglas llamadas “**Comprimidos2**” y “**bloquearcab**”, con **Filtrado de nombres** y **por categoría** respectivamente, en la cual se colocó el nombre de los adjuntos que se han detectado como peligrosos.

En la Ilustración IV.12 se encuentra la regla para detener los archivos adjuntos **.CAB**, con **filtrado por categoría**.

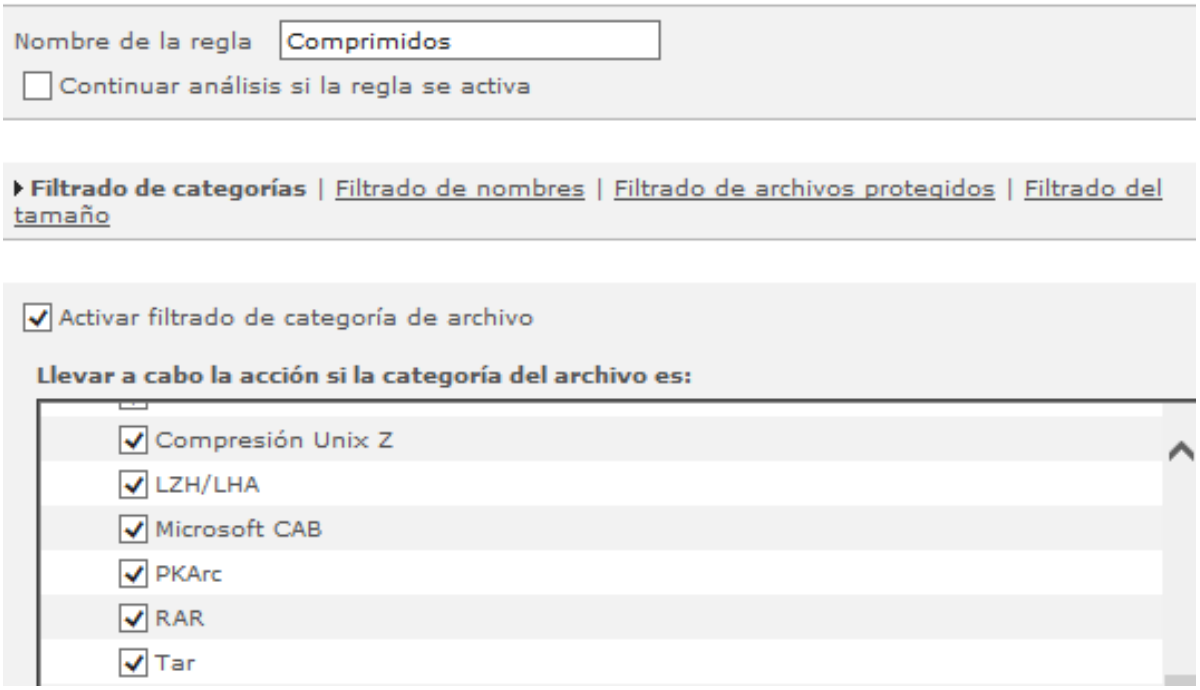


Ilustración IV.12 Filtrado por categoría de regla "Comprimidos"

Y en la ilustración IV.13 se encuentra la regla para detener los archivos comprimidos con un **filtrado por nombre**.

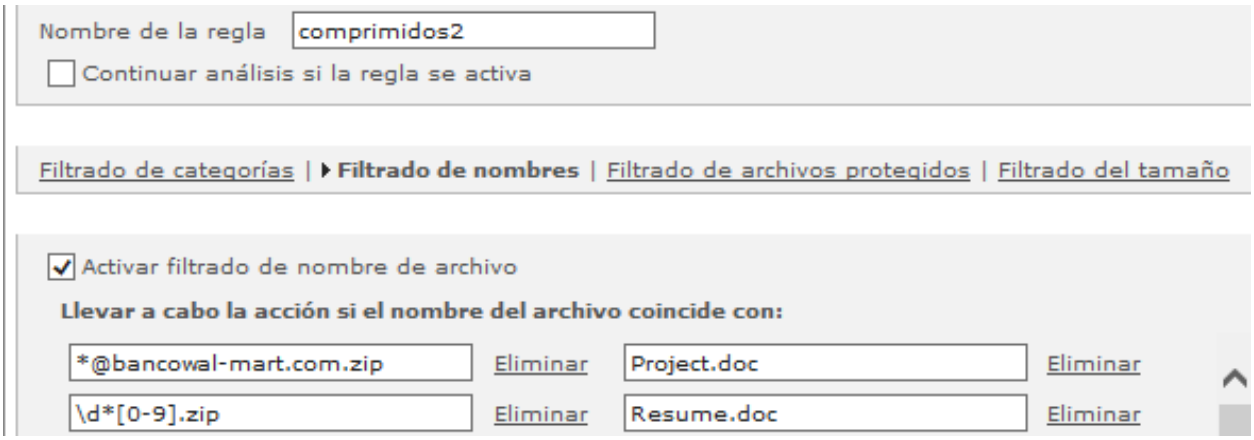


Ilustración IV.13 Filtrado por nombres regla "comprimidos2"

La Acción para las reglas nuevas es: "Denegar conexión" por ser ataque identificado.

Se realizó envío de correo de prueba desde una cuenta externa hacia jramirez@bancowal-mart.com, el correo no llego al buzón del usuario y se encontró el registro con status de Bloqueado. Esto comprueba que la regla aplico de manera efectiva, se guardó la configuración para grabar los cambios y se mantuvo en supervisión.

Por último las reglas "**bloquearcab**" y "**comprimidos2**", se colocaron antes de la política "**Comprimidos**", como se muestra en la Ilustración IV.14, ya que en los MEG la prioridad es importante.

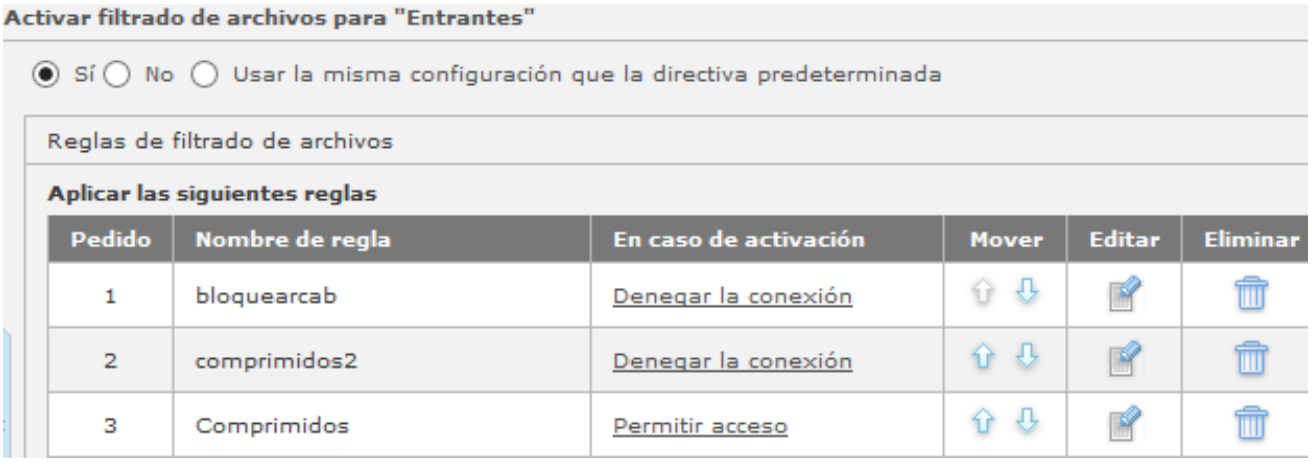


Ilustración IV.14 Orden prioridad reglas filtrado de archivos "Entrantes"

IV.8 Aportaciones Agregar un dominio al control del McAfee Email Gateway Agosto 2015

Aplica para: McAfee Email Gateway (MEG) ver 7.x.x (software de Administración)

MEG 5000C y MEG 4500B (Dispositivos)

Se quiere agregar al control del MEG los mensajes electrónicos de un nuevo dominio, es decir que puedan ser filtrados y revisados antes de entrar o salir a su destino.

Se cuenta actualmente con el filtrado de correos para el dominio **bancowal-mart.com.mx**

Se deberá agregar el dominio y la IP del nuevo servidor de correo para que:

- Los correos salientes del nuevo servidor sean enviados al MEG antes de entregarse al destinatario (modificar servidor Exchange)
- Los correos Entrantes para el nuevo dominio pasen primero por el MEG (modificar firewall).

Los cambios en la configuración del MEG se realizan en la sección:

Correo Electrónico – Configuración de correo electrónico – Recepción de correo electrónico - Configuración de Bloqueo de Retransmisión

Seleccionar la opción: **Retransmitir correo electrónico**

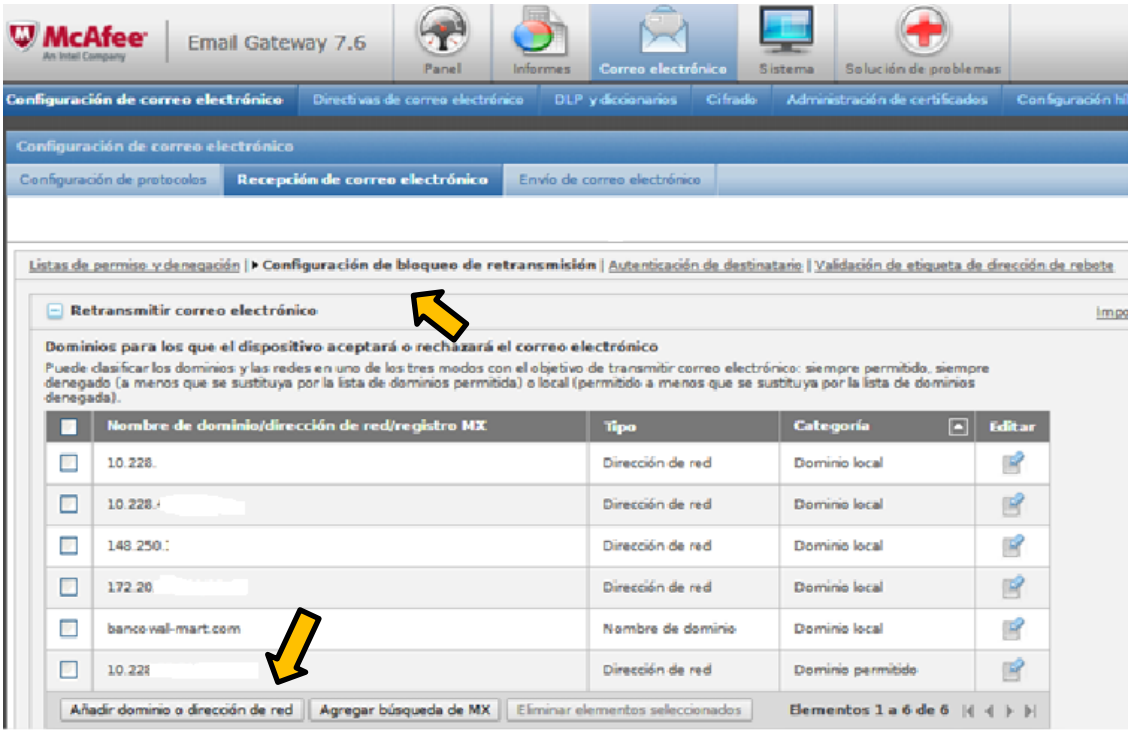


Ilustración IV.15 Nueva recepción de correo electrónico

Presionar botón "**Añadir dominio o dirección de red**", indicarle la dirección IP del servidor Exchange que maneja los correos del nuevo dominio, (véase Ilustración IV.15).

Se muestra una dirección ejemplo “192.68.38.230/24”, debemos capturar la dirección IP que corresponde al servidor Exchange que controla los correos de “nuevo_dominio.com.mx”

Presionar botón “**Aceptar**” para registrar la dirección IP, como se muestra en la Ilustración IV.16.

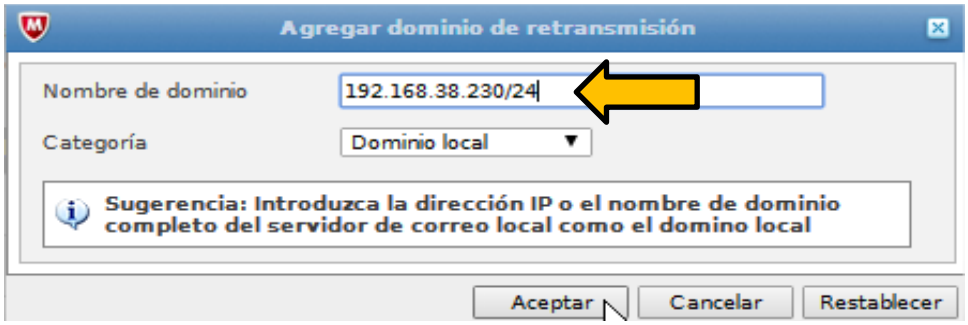


Ilustración IV.16 Añadir dominio dirección de red

La nueva dirección aparece en la lista de “Dominios para los que el MEG aceptará o rechazará mensajes de correo electrónico”, como se muestra a continuación en la Ilustración IV.17.

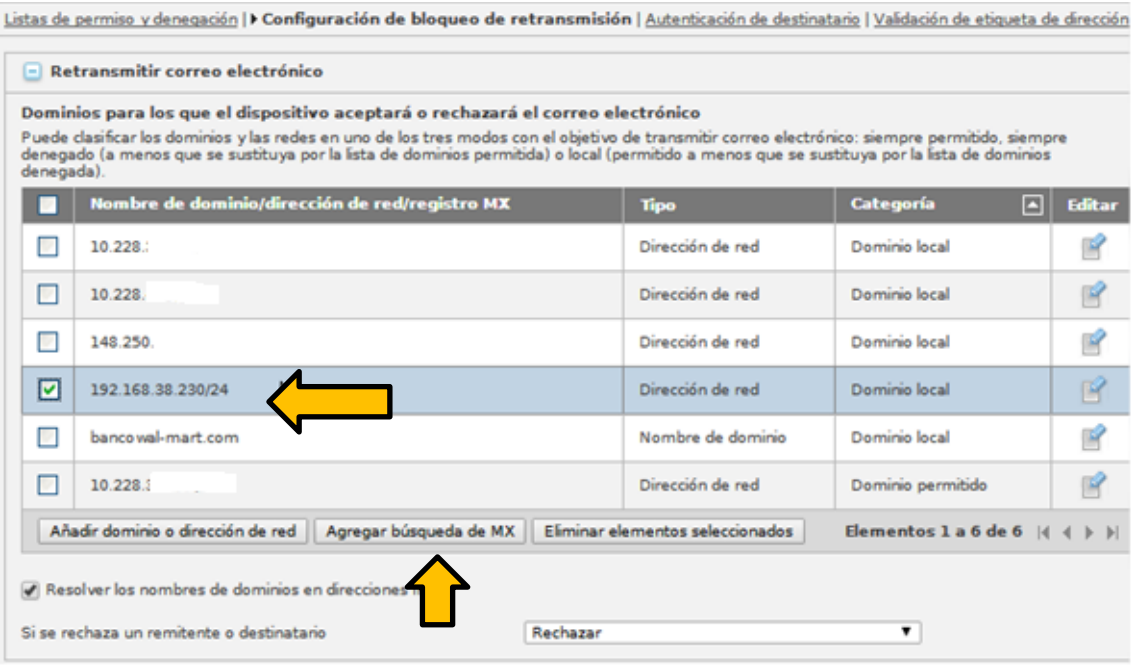


Ilustración IV.17 Nueva IP aceptada para correo electrónico

A continuación agregar el servidor MX para que el MEG pueda enviar los correos Entrantes después de procesarlos. Presionar botón "**Agregar búsqueda de MX**", (véase Ilustración IV.18).

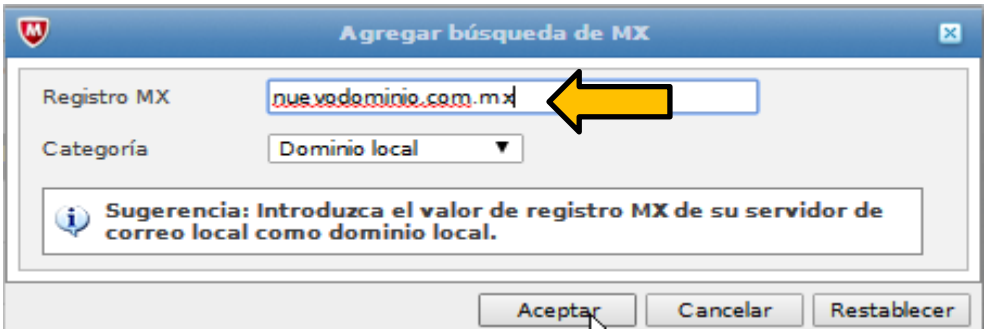


Ilustración IV.18 Agregar búsqueda MX

Se muestra dominio ejemplo, capturar el nombre del nuevo dominio real. Presionar "**Aceptar**".

Al terminar de agregar el dominio, la lista queda como la Ilustración IV.19.

Ilustración IV.19 Nuevo Dominio aceptado para correo electrónico

Esto permitirá al MEG procesar correos Entrantes y Salientes del dominio "nuevo_dominio.com.mx",

IMPORTANTE. Los siguientes pasos para aplicar son los cambios en el servidor Exchange, el Firewall y las Directivas de Correo.

El Nuevo dominio y las Directivas.-

Para controlar el nuevo dominio se deben modificar las Directivas existentes o crear nuevas para que apliquen los filtros deseados.

Opción A.- En el caso de No requerir nuevas directivas y simplemente agregar el nuevo dominio.

Debe ejecutar la siguiente acción.

- Agregar al grupo "**Servidores Internos**" el servidor que corresponde al nuevo dominio.

En el menú:

Correo Electrónico – Administración de grupos – Grupo de redes
Presionar el ícono "**EDITAR**" para agregar el Nuevo dominio al grupo (véase Ilustración IV.20).

Ilustración IV.20 Grupos de Redes

Se muestra la lista de direcciones IP correspondiente a los actuales servidores de correos.

Presionar el botón "**Agregar Regla**" para crear un nuevo registro, como se muestra en la Ilustración IV.21.

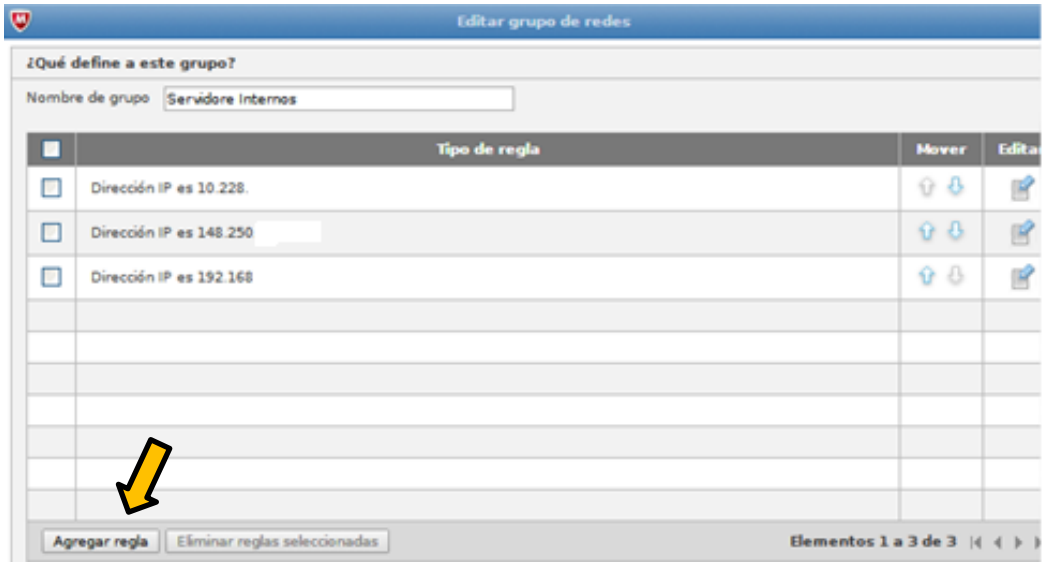


Ilustración IV.21 Agregar regla al grupo de redes

Capturar la dirección IP del nuevo servidor de correos y presionar el botón "**Aceptar**" para confirmar el cambio.

Como se muestra en la Ilustración IV.22 con la IP ejemplo 192.168.38.230

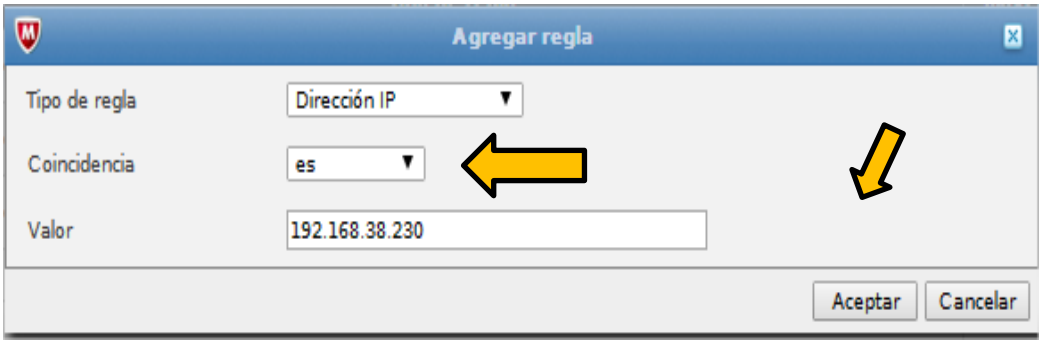


Ilustración IV.22 Datos del nuevo servidor de correo

Se muestra la dirección IP del nuevo servidor como miembro del grupo "**Servidores Internos**", como en la Ilustración IV.23.

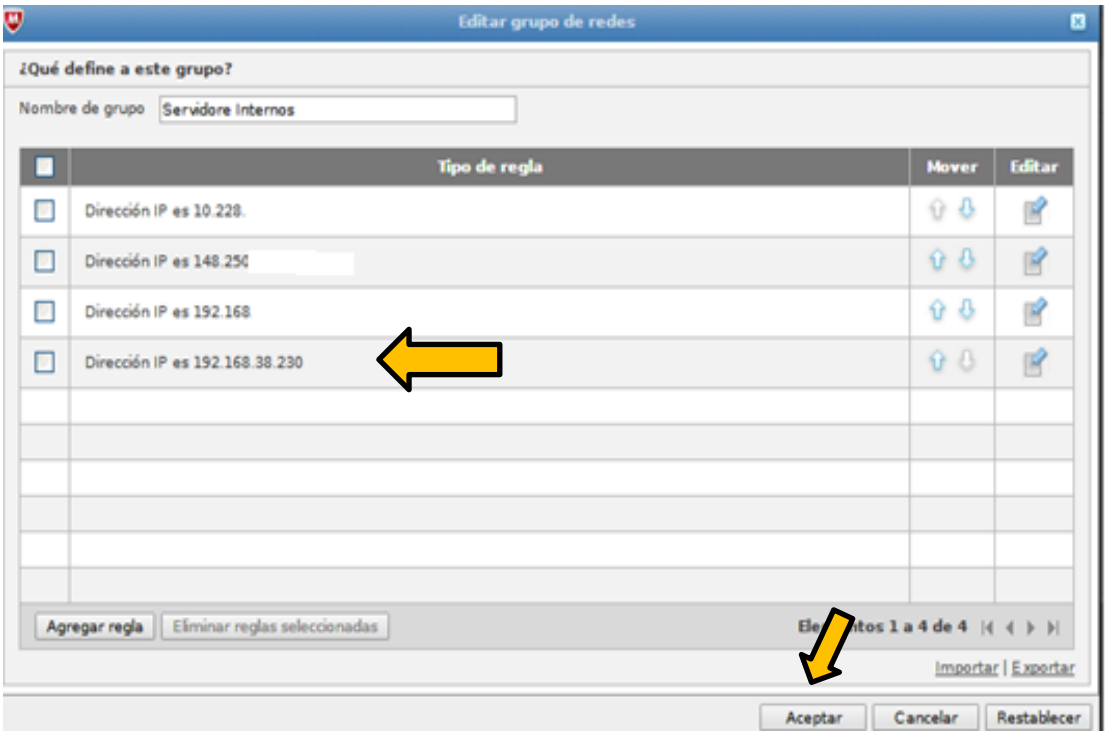


Ilustración IV.23 Nueva Ip en el grupo de servidores internos

Presionar botón "**ACEPTAR**" para finalizar la Alta en el grupo.

Por último en la parte superior derecha presionar el botón  para que aplique los cambios a la configuración del MEG.

(De NO hacerlo los cambios no aplicaran).

Opción B.- Se desea tener directivas propias que apliquen al nuevo dominio.

Para esto se tiene que definir un nuevo grupo para ubicar al servidor de correos del nuevo dominio.

En el Menú de **Administración de Grupos - Grupos de Redes**, elegir botón "**Agregar**", como se muestra en la Ilustración IV.24.

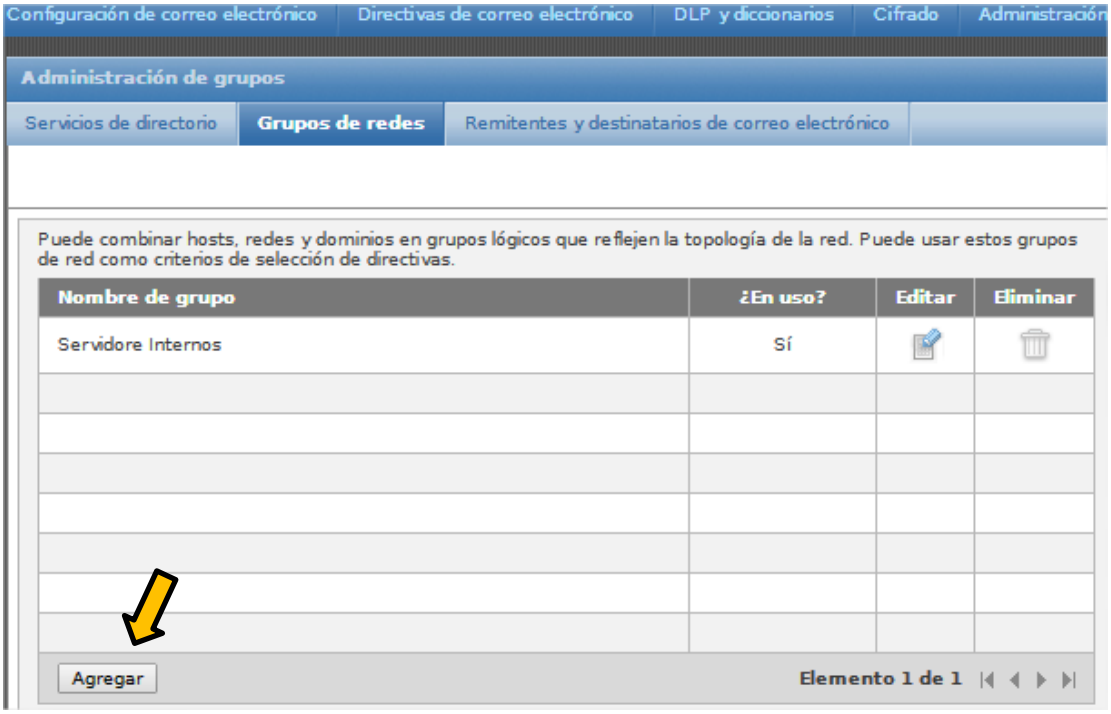


Ilustración IV.24 Agregar Grupo de Redes

En la ventana "**Agregar grupo de redes**" captura el nombre del grupo, en este ejemplo "***Grupo_Nuevo_dominio***".

Presionar el botón "**Agregar Regla**"

Se desplegara una pantalla que pedirá ingreses unos datos.

En los campos solicitados capturar:

Tipo de Regla: Dirección IP

Coincidencia: es

Valor: 192.168.38.230 (Dirección IP del servidor de correo, por ejemplo)

Presionar el botón "**Aceptar**" para concluir agregar nuevo grupo, (véase Ilustración IV.25).

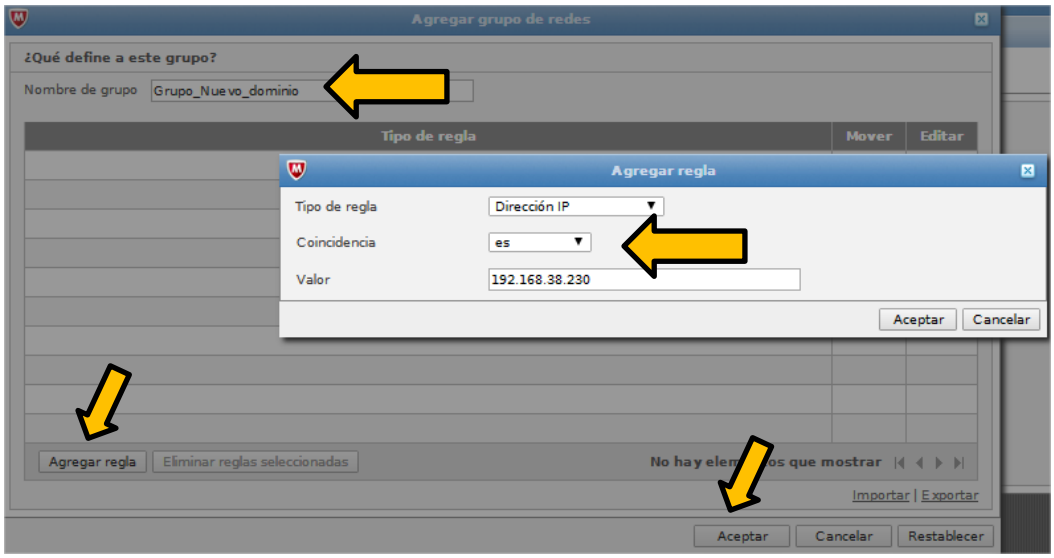


Ilustración IV.25 Nuevo Dominio directivas propias

La lista de grupo de redes queda actualizada, como se muestra en la Ilustración IV.26

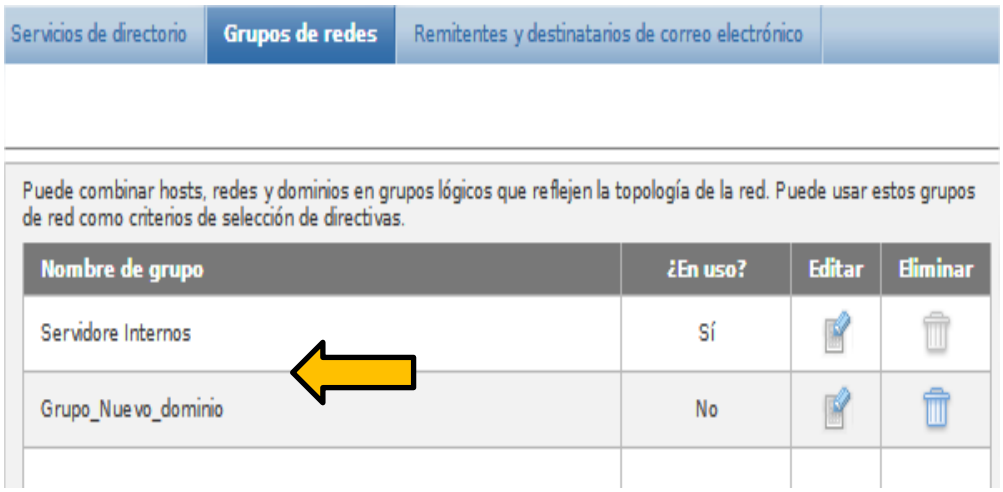


Ilustración IV.26 Grupo de nuevo dominio

Podemos presionar el botón  para que apliquen los cambios en la configuración o continuar creando las Directivas y aplicarlo al finalizarlas.

Para crear las directivas que se requieran, presionar botón "**Agregar Directiva**", como lo podemos observar en la Ilustración IV.27.

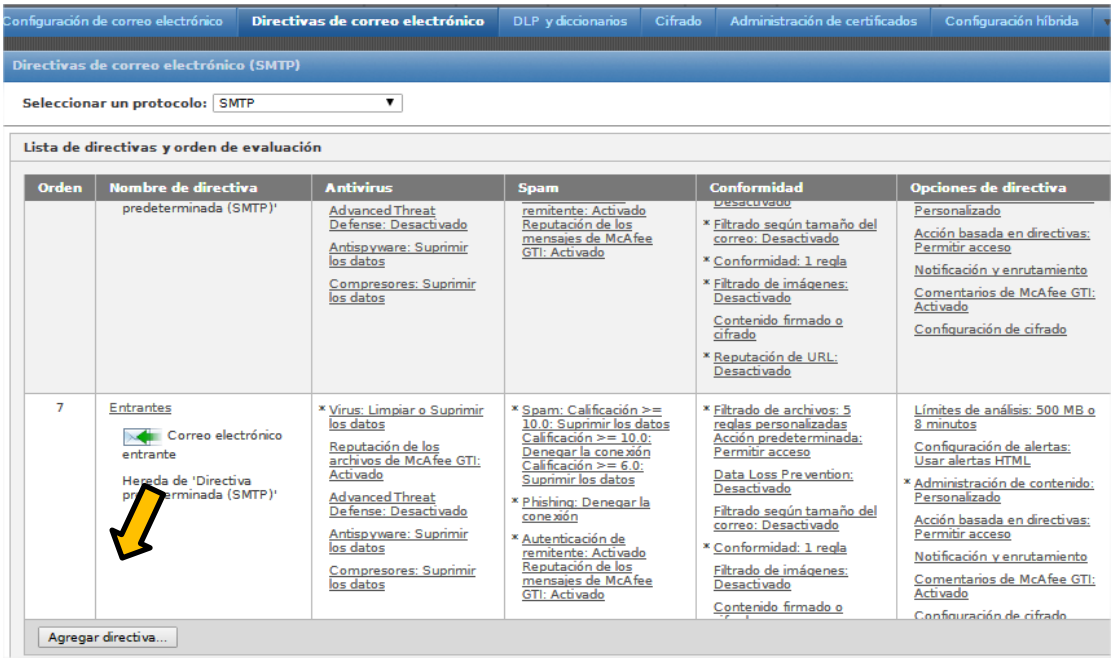


Ilustración IV.27 Agregar Directiva

Capturar los datos necesarios como, en la Ilustración IV.28.

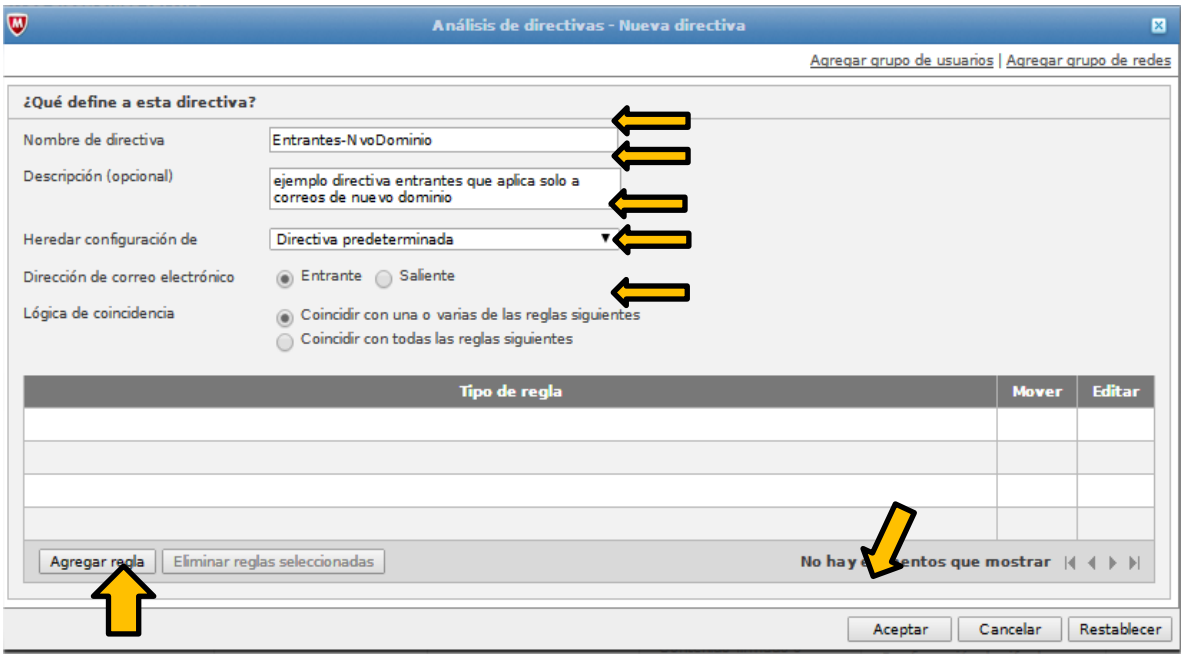


Ilustración IV.28 Configuración de Directiva

Los datos solicitados son Nombre de la Nueva Directiva, para este ejemplo fue **"Entrantes-NvoDominio"**, y una breve descripción de lo que realizara la Directiva

En el campo Heredar configuración dejar el valor "**Directiva predeterminada**"

Dirección de Correo electrónico, seleccionar "**Entrante**" porque es la directiva que requerimos.

Se configuran las reglas para que la directiva tenga sus primeros parámetros completos, presionar botón "**Aceptar**"

A continuación personalizar los Filtros Antivirus, Spam, Conformidad y Opciones de Directiva de acuerdo al objetivo de filtrado de esta Directiva.

CONCLUSIONES

Con base en nuestro objetivo principal, puedo decir que al implementar la tecnología de McAfee se tiene la certeza, de que, la interfaz de correo electrónico se encuentra protegida y mientras sea así, será más difícil que los ataques puedan llegar hasta los servidores de correo interno. La herramienta de McAfee agregó a la empresa seguridad mediante el fortalecimiento de la interfaz de acceso y el análisis detallado de los posibles ataques, proporcionando una serie de ventajas como:

- Protección total entrante y saliente
- Integración con los protocolos de Directorio Activo de Microsoft
- Agrupación y equilibrio de cargas para ofrecer alta disponibilidad
- Seguridad frente a la mayoría de las amenazas que llegan por el correo electrónico
- Cifrado de correo electrónico y protección de datos
- Administración centralizada del correo y su seguridad con implementación de directivas específicas, búsqueda de mensajes y registro de conversaciones
- Generación de reportes detallados en tiempo real, con paneles interactivos
- Cumplimiento de normativas y prevención de pérdida de datos confidenciales o sensibles

La manera de trabajar de los MEG es con base en Directivas las cuales nos ayudan a englobar requerimientos y no duplicar solicitudes, por tal motivo una vez instalado el dispositivo, se procedió con la creación de Políticas esto generando una administración más simplificada.

A la hora de crear un Directiva nueva se debe tener siempre presente el orden, ya que el método de análisis es a través de la prioridad, con esto se entiende que si colocamos una directiva permisiva dentro de las primeras a clasificar, el correo saldrá sin ser verificado por las directivas siguientes, por ello para este caso en particular decidí dar mayor rango las directivas de bloqueo, ya que si por alguna razón el

mensaje está catalogado como malicioso, será atrapado por el dispositivo sin permitir el acceso a la red.

Otro punto importante y que nos favoreció mucho fue la creación de listas blancas (de confianza) o negras (de bloqueo), ya que con esto se ayudó a detectar correos que por su método de envío, se pueden considerar SPAM y no lo son, o correos con malas intenciones que logren burlar nuestro dispositivo, sin que alguna alerta lo notifique, esto dejando huecos en la seguridad que NO podemos erradicar del todo, gracias a que los atacantes van cambiando su forma de operar.

Uno de las tareas que implica un gran logro a la hora de administrar una herramienta de filtrado de correo es la creación de grupos especializado en el Directorio Activo, los cuales desde el momento que el usuario es dado de alta en el dominio, se puede saber hasta qué punto le es permitido compartir información de la empresa a través del correo, esto facilitó la administración de los usuarios y sus permisos, ya que por cuestiones de operatividad al crear una política resulta mucho más sencillo administrar grupos o perfiles en lugar de usuarios, afectando a todas las personas contenidas en el mismo grupo o perfil, uno de los grupos que juega un papel importante se llama **"Usuarios sinEmail",** que es el que discrimina que usuarios NO pueden compartir información por medio del correo.

Todas aquellas personas contenidas en este grupo no podrán enviar, ni recibir correos a cualquier dominio externo a la empresa, esto por la sensibilidad de los datos que se manejan.

Los usuarios finales pueden solicitar que se agregue o se elimine cualquier objeto de la lista según sea el caso o la necesidad, pero estas acciones solo podrán ser realizadas por los administradores.

McAfee Email Gateway utiliza el servicio de reputación de la web, redes y mensajes para identificar los mensajes de correo electrónico con contenido malicioso, por tal motivo cada que se aplique un cambio, se tiene que actualizar la versión del manejador de correo y las bases de firmas de McAfee para poder estar a la vanguardia de las amenazas que hay en la red.

Los dispositivos McAfee tienen la opción de generar reportes, cuando se configuraron estos reportes se generó una serie de ventajas, ya que gracias a ellos se pudo simplificar la carga de trabajo, y fui definiendo algunos parámetros o comportamientos de los correos maliciosos para poder detectarlos oportunamente, todo en base a la relación de correos bloqueados, tráfico de correos entrantes y salientes.

Al momento de simplificar la administración obtuve ganancia en el tiempo y costos, ya que antes para operar y administrar tenían que contemplar a varias personas y las actividades de análisis llevaban el doble de tiempo, hoy en día puedo afirmar que con menos personas y en menos tiempo podemos tener un filtro seguro y confiable, además que se dio un paso muy grande en lo que es la concientización de los usuarios que usan las tecnologías de la información gracias a que se detectaron a tiempo correos maliciosos y se enviaron comunicados de seguridad para avisar oportunamente y que el riesgo que nos proporciona el compartir datos por la red sea cada vez menor, con esto pude definir como exitosa la actividad de Implementación de dispositivos de filtrado de correo electrónico.

Con la reciente compra de Banco Wal-Mart Adelante por Grupo Financiero Inbursa, se contemplan una serie de cambios para que la herramienta siga siendo aprovechada, pero ahora con un nuevo dominio y una reestructuración de las políticas, pues recordaremos que cada empresa tiene necesidades diferentes.

Con este proyecto se cubre una de las necesidades más preocupantes para cualquier empresa, la seguridad de la información y el cumplimiento de las legislaciones, pero en este caso particular, me ocupe en breve de los siguientes aspectos generales:

- Spam
- Virus
- Filtro de contenido
- Confidencialidad

Acorde a la experiencia de este proyecto puedo indicar que McAfee Email Gateway es una herramienta completa y fácil de administrar.

Todo gracias a la extensa documentación y apoyo a los usuarios a través del sitio Web de McAfee y de sus técnicos certificados y consultores de alto nivel.

Cada una de las actividades que desempeño en la empresa se debe gracias a los conocimientos adquiridos durante mi vida estudiantil, por eso también es merecido reconocer que la Facultad de Ingeniería y a la UNAM, porque gracias a ellas y a sus profesores obtuve las bases necesarias para poder defenderme en el mercado laboral y así sacar adelante los proyectos y tareas que se me encomiendan día a día.

El hecho de que los controles de seguridad se estén volviendo una parte integral de cualquier sistema y cuenten con una infraestructura muy bien preparada parece indicar que su uso se irá extendiendo a gran velocidad.

Para poder sacarle partido a las herramientas de McAfee es preciso usarlas de manera eficaz. Y eso a su vez, implica:

- Tomar conciencia de su poder y de la función que puede implicar
- Concientizar el buen uso

La clave está en usarlo como haría con cualquier otra herramienta de trabajo:
Con Precaución.

ÍNDICE DE IMÁGENES Y TABLAS

GLOSARIO

Activos Las instalaciones, teléfonos, computadoras, **correo electrónico**, fotocopiadora, papelería, solicitudes y formatos, etc.

Amenaza [11] Es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir daño (material o inmaterial) sobre los elementos (activos, recursos) de un sistema.

Antivirus [11]Bajo el nombre de antivirus se conoce a cualquier programa destinado a combatir los virus de una forma u otra, desde programas realizados para detectar y eliminar un único virus hasta aplicaciones completas que detectan y eliminan cientos e incluyen diferentes tipos de protección.

Ataque [11] Es una amenaza que se convirtió en realidad, es decir cuando un evento se realizó. No dice nada si o no el evento fue exitoso.

Autenticidad [7] La legitimidad y credibilidad de una persona, servicio o elemento debe ser comprobable.

Capa de Conexión Segura (SSL) [20] Sistema de protocolos de carácter general diseñado en 1994 por la empresa Netscape Comunications CO., está basado en la aplicación conjunta de criptografía, certificados y firmas digitales para conseguir un canal seguro a través del internet.

Certificado Digital [20] es un documento que atestigua la posesión de una entidad ya que es firmado digitalmente, evitando que cualquiera pueda generar una clave distinta y hacerse pasar por el dueño de la entidad, para poder conocer el contenido.

Cifrado Privacidad Bastante Buena (PGP) [20] En el proceso de cifrado, se comprime el documento o archivo y se genera una clave aleatoria. Al enviar el paquete de datos se adjunta una clave cifrada con la clave del receptor, que en el momento de descifrar el archivo o documento, realiza el proceso inverso, el depósito

oficial de los certificados PGP se encuentra en el sitio del Instituto de Tecnología de Massachusetts y se pueden adquirir gratuitamente.

Confidencialidad [7] Datos solo pueden ser legibles y modificados por personas autorizados, tanto en el acceso a datos almacenados como también durante la transferencia de ellos.

Denial of service (DoS) [7] Negación de Servicio tienen como objetivo saturar los recursos de la víctima de forma tal que se inhabilita los servicios brindados por la misma.

SISTEMAS DETECTORES DE INTRUSOS (IDS) [18] Este tipo de sistema detecta tráfico malicioso en la red. Monitorea los paquetes en la red y alerta si hay una actividad maliciosa. Además detectan gran cantidad de tipos de ataques.

Diccionarios son archivos con millones de palabras, las cuales pueden ser contraseñas posibles de los usuarios, o palabras las cuales tienen una relación entre sí.

Disponibilidad [7] Acceso a los datos debe ser garantizado en el momento necesario. Hay que evitar fallas del sistema y proveer el acceso adecuado a los datos.

Elementos de Información: También “Activos” o “Recursos” de una institución que requieren protección, para evitar su pérdida, modificación o el uso inadecuado de su contenido, para impedir daños para la institución y las personas que salen en la información. Se distingue y divide tres grupos, a) Datos e Información, b) Sistemas e Infraestructura y c) Personal.

Ethernet [18] También conocido como estándar IEEE802.3 es un método de transmisión de datos más popular en las LAN. Antes de que se enviara un paquete a través de la red, primero escucha y se da cuenta si algún otro nodo está transfiriendo. De no ser así el paquete es enviado.

Extensiones multipropósito de correo de internet (MIME) [18] y su versión segura cada vez más utilizada S-MIME permiten la transmisión de mensajes multimedia.

Gestión de Riesgo [7] Método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo. Está compuesta por cuatro fases: 1) Análisis, 2) Clasificación, 3) Reducción y 4) Control de Riesgo.

Integridad [7] Datos son completos, non-modificados y todos los cambios son reproducibles (se conoce el autor y el momento del cambio).

FIREWALL [18] colección de componentes colocados entre un red interna y una red externa para que solo el tráfico que es autorizado por la política de seguridad de la red interna esté permitido pasar.

Lenguaje de Marcado de Hipertexto (HTML) [10] protocolo utilizado para codificar las páginas Web, permite elaborar documentos con marcadores que cualquier navegador pueda interpretar. Desarrollado por el equipo de programadores de Centro Europeo de Investigación Nuclear de Ginebra (CEING).

Localizador de Recursos Uniforme (URL) [7] para identificar las páginas WEB dentro de la red, identificadores que están asociados a cada página, en ellos se indica el nombre de la página, localización y como se accede a la misma.

PHISHING [16] consiste en el envío de correos electrónicos que, aparentando provenir de fuentes fiables (por ejemplo, entidades bancarias), intentan obtener datos confidenciales del usuario, que posteriormente son utilizados para la realización de algún tipo de fraude.

POLÍTICAS [8] son una serie de normas, reglamentos y protocolos por seguir, donde se definen las distintas medidas que se van a tomar para proteger la seguridad del sistema, las funciones y responsabilidades de los distintos componentes de la organización y los mecanismos para controlar su funcionamiento.

Protocolo de transferencia de archivos (FTP) **[18]** es un protocolo de red que proporciona acceso a los archivos, transferencia de archivos y funcionalidades de administración de archivos.

FTP se basa en una arquitectura cliente-servidor y utiliza conexiones de control y de datos separadas entre el cliente y el servidor.

Protocolo simple de transferencia de correo (SMTP) **[18]** Una sesión SMTP consiste en comandos originados por un cliente SMTP (el agente de inicio, emisor o transmisor) y las respuestas correspondientes del SMTP del servidor (el agente de escucha, o receptor) para que la sesión se abra y se intercambian los parámetros de la sesión a través de TCP puerto 25 (SMTP) o el puerto 587 (Presentación), las especificaciones y muchos servidores soportan ambos. Aunque algunos servidores soportan el puerto 465 para el legado SMTP seguro.

Microsoft Exchange Server puede escuchar en los puertos 25, 587, 465, 475, y 2525.

Protocolo de oficina de correo (POP) [25] proporciona el acceso a los mensajes de los servidores SMTP por el puerto 110.

Protocolo de transferencia de Hipertexto (HTTP) **[10]** Protocolo que se encarga de la transferencia de Hipertexto, cada servicio de internet tiene su propia sintaxis y todas las direcciones correspondientes a WWW empiezan con http:// por el puerto 80 o en su modo seguro https:// por el puerto 443.

Protocolo de Acceso a Mensajes de Internet (IMAP) [25] aporta funciones de almacenamiento y envío. La última versión, la 4, permite que los usuarios accedan a su correo desde diversas terminales, los mensajes continúan siempre almacenados en el servidor, lo cual no ocurre con POP.

Red de Área Local (LAN) [24] Sistema de comunicaciones de alta velocidad que conecta ordenadores que se encuentran cercanos, por lo general dentro del mismo edificio. Una LAN da la posibilidad de que las PC compartan entre ellas información y recursos, como directorios e impresoras.

Redes internas (intranets) red informática que cuenta con todas las ventajas de la tecnología de internet, pero con el factor añadido de la seguridad. Utilizan la misma tecnología (navegadores, TCP/IP, HTML, etc.) pero son de uso limitado.

Red Privada Virtual (VPN) [5] es una red privada construida dentro de una infraestructura de red pública, como por ejemplo Internet. Las empresas pueden usar una red VPN para conectar de manera segura oficinas y usuarios remotos por medio de un acceso a Internet económico suministrado por un tercero.

Seguridad en la Capa de Transporte (TLS) **[21]** es un protocolo que garantiza la privacidad entre las aplicaciones de comunicación y sus usuarios en Internet. Cuando un servidor y el cliente comunican, TLS asegura que ningún tercero puede espiar o manipular cualquier mensaje.

SPAM **[17]** correo electrónico no solicitado que es enviado en cantidades masivas a un número muy amplio de usuarios generalmente con el fin de comercializar, ofertar o tratar de despertar el interés con respecto a algún producto o servicio.

Seguridad Informática **[11]**: Procesos, actividades, mecanismos que consideran las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad.

Servicios y Contenidos Todos los productos y servicios que preste Banco Wal-Mart y toda la información contenida en el Portal, incluyendo cualquier texto, programas, fotografías, imágenes y multimedia.

Sistema de Nombres de Dominio (DNS) [19] Conjunto de protocolos y servicios que permite a los usuarios utilizar nombres en vez de tener que recordar direcciones IP numéricas.

Sistema de Detección de Intrusos (IDS) Como su nombre lo indica detecta intrusiones al sistema, analizando paquetes para encontrar un patrón en común que se puede traducir en un ataque.

SUPLANTACIÓN [11] Ocupar el lugar de otra persona ilegalmente o hacerse pasar por ella contra su voluntad para obtener un beneficio.

Usuario Cualquier persona física o moral, está última a través de su representante o persona autorizada, que acceda al Portal de Banco Wal-Mart.

VIRUS [11] Es un programa que posee la capacidad de crear duplicados de sí mismo, en ocasiones introduciendo ligeras variaciones, y distribuirlos a través de un sistema, para causar un daño.

Vulnerabilidad [11] Son la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño.

REFERENCIAS

1. Andrade, A. (2002). Aprende redes. Recuperado el 8 de mayo de 2015, de Aprende redes: http://www.aprenderedes.com

2. Banco Walmart. (s.f.). Seguridad de la Información. Recuperado el Diciembre 2013, de Seguridad de la Información: http://pipeline.bwa.com/procesos/controlinterno/seguridaddelainformacion/Pages/default.aspx

3. Borghello, C. (2000). SEGU.INFO. Recuperado el Julio de 2015, de Amenazas Logicas Tipos de Ataquez Denial of Service: http://www.segu-info.com.ar/ataques/ataques_dos.htm

4. Cisco Systems. (s.f.). CISCO Latino America. Recuperado el Julio de 2015, de CISCO Latino America: http://www.cisco.com/web/LA/soluciones/la/information_security/index.html

5. Cisco Systems, Inc. (s.f.). VPN Cisco systems. Recuperado el Julio de 2015, de VPN Cisco systems: http://www.cisco.com/web/ES/solutions/es/vpn/index.html

6. Erb, M. (s.f.). Protejete.wordpress.com. Recuperado el Julio de 2015, de https://protejete.wordpress.com/gdr_principal/

7. García Tomás, J., Raya Cabrera, J., & Rodrigo Raya, V. (s.f.). Alta Velocidad y Calidad de Servicio en Redes IP. Alfa Omega Ra.

8. Gómez Vieites, Á. (2011). Enciclopedia de la Seguridad Informática. México D.F.: Alfaomega Grupo Editor, S.A. de C.V.

9. Haymarket Media, Inc. (22 de Abril de 2009). SC Magazine. Recuperado el Junio de 2013, de Best Email Security Solution: http://www.scmagazine.com/best-email-security-solution/article/130865/

10. Leduc, D., & Armond St., P. (2000). HTML creación y difusión de páginas WEB. México: Trillas.

11. Lopez Barrientos, M. J., & Quezada Reyes, C. (s.f.). Fundamentos de Seguridad Informática. México DF: Facultad de Ingeniería UNAM.

12. McAfee. (4 de Marzo de 2013). Como configurar LDAP en McAfee Email Gateway 7.x. Articulos técnicos ID: KB76232.

13. McAfee Inc. (2014). McAfee for Business. Recuperado el Mayo de 2015, de McAfee Email Gateway: http://www.mcafee.com/mx/products/email-gateway.aspx#vt=vtab-Recursos&nF=tab-Forums

14. Microsoft. (s.f.). Support.microsoft.com. Recuperado el Julio de 2015, de https://support.microsoft.com/es-es/kb/196464

15. Nombela, J. J. (s.f.). Seguridad Informática. Paraninfo.

16. Panda Security. (2015). Pishing. Recuperado el Julio de 2015, de Pishing: http://www.pandasecurity.com/mexico/homeusers/security-info/cybercrime/phishing/

17. Panda Security. (2015). SPAM. Recuperado el Julio de 2015, de SPAM: http://www.pandasecurity.com/mexico/homeusers/security-info/cybercrime/spam/

18. Siyan, K., Hare, C., & Gutierrez, J. (s.f.). Firewall y la Seguridad en Internet. Prentice Hall Hispanoamericana.

19. SomeBook & News. (s.f.). Somebooks.es. Recuperado el Julio de 2015, de http://somebooks.es/?p=3375

20. Stoltz, K., & Ruiz Faudon, S. (s.f.). Todo acerca de las redes de computadores. Prentice Hall Hispanoamericana.

21. Techtarget. (s.f.). What is Transport Layer Security?? Recuperado el Julio de 2015, de What is Transport Layer Security??: http://searchsecurity.techtarget.com/definition/Transport-Layer-Security-TLS

22. Virus Bulletin. (Septiembre de 2009). Virus Bulletin LTD. Recuperado el Julio de 2015, de email-gateway-review-virus-bulletin.pdf: http://www.mcafee.com/mx/resources/reviews/email-gateway-review-virus-bulletin.pdf

23. Walmart México y Centroamerica. (2012). Walmart México y Centroamerica. Recuperado el Julio de 2013, de Banco Walmart: http://www.walmartmexicoycam.com.mx/sala_de_prensa/operadoras/banco/2011/marzo/bn15032011.html#sthash.QUjHs8WB.dpuf

24. Wesley, A. (s.f.). Data Communications, computer networks and open systems. Fred HalSall Tercera Edición.

25. Whelan, J. (2000). E-mail en el trabajo evite los inconvenientes y explote el potencial. Prentice Hall.Banco Walmart. (s.f.). *Seguridad de la Información*. Recuperado el Diciembre 2013, de Seguridad de la Información

ANEXOS

Anexo 1Especificaciones Físicas y Técnicas del MEG

	EMG-4000-B	EMG-4500-B	EMG-5000-D	EMG-5500-D
Hardware Specifications				
Form Factor	Intel SR1530SH, 1U	Intel SR1630GPRX, 1U	Intel R1304SP4SHOC, 1U	Intel R1208GZ4GC, 1U
Supported Software Versions	MEG 7.x	MEG 7.x	MEG 7.x	MEG 7.x
Processor	Intel Celeron E3400, 2.6 GHz, 1 MB cache, 2 core	Intel Core I3-540, 3.06 GHz, 4 MB cache, 2 core	Intel Xeon E5-2430, 2.20 GHz, 15 MB cache, 6 core	2x CPU, Intel Xeon E5-2650V2, 2.60 GHz, 20 MB cache, 8 core
Memory	4 GB, 800 MHz, ECC	4 GB, 1333 MHz, ECC	3 x DIMM, 4 GB, 1600 MHz, DDR3, REG, ECC, SINGLE	4 x DIMM, 4 GB, 1600 MHz, DDR3, REG, ECC, SINGLE
Network Interfaces	2 copper, 10/100/1000	2 copper, 10/100/1000	4 x 10/100/1000 MB RJ45 Ethernet ports + 2 Port GBE Fiber Ethernet ports	4 x 10/100/1000 MB RJ45 Ethernet ports + 2 Port GBE Fiber Ethernet ports
USB Interfaces	3 USB 2.0 ports. 2 on the rear 1 on the front	3 USB 2.0 ports. 2 on the rear 1 on the front	Four USB 2.0 ports on rear	USB 2.0 connectors. 3 on back panel + 2 on front panel
Serial Interfaces	RJ-45 Serial-A Port	RJ-45 Serial-A Port	RJ-45 Serial-A Port	RJ-45 Serial-A Port
RAID	No	RAID-1	RAID-1	RAID-10
Hard Disk	1x 500 GB SATA 3.5 in., 7200 RPM	2x 300 GB SAS 3.5 in., 15 K RPM, hot swap	2 x HDD, 2.5 in., 600 GB, SAS 6 Gbps, 10K.6 RPM	6 x HDD, 2.5 in., 300 GB, SAS 6 Gbps, 10K.6 RPM
Optical	8x DVD-ROM drive	8x DVD-ROM drive	8x DVD-ROM drive, SLIMLINE	8x DVD-ROM drive, SLIMLINE
Voltage	Auto Switch 110/220 V	Auto Switch 110/220 V	Auto Switch 110/220 V	Auto Switch 110/220 V
Max Amps	6 A (RMS) @ 90 VAC, 3 A (RMS) @ 180 VAC	6 A (RMS) @ 90 VAC, 3 A (RMS) @ 180 VAC	6 A (RMS) @ 110 V, 3 A (RMS) @ 220 V	12 A (RMS) @ 90 VAC, 6 A (RMS) @ 180 VAC
Startup VAC	85 VAC +/– 4 VAC	85 VAC +/– 4 VAC	85 VAC +/– 4 VAC	85 VAC +/– 4 VAC
Input Voltage Range	110 V (90 Vrms – 140 Vrms) 220 V (180 Vrms – 264 Vrms)	110 V (90 Vrms – 140 Vrms) 220 V (180 Vrms – 264 Vrms)	110 V (90 Vrms – 140 Vrms) 220 V (180 Vrms – 264 Vrms)	110 V (90 Vrms – 140 Vrms) 220 V (180 Vrms – 264 Vrms)
Power Rating	350 W	350 W	2 X 650 W	2 X 750 W
Power Consumption	350 W	400 W	710 W	710 W
Dimensions	Height: 1.67 in. or 42.42 mm Width: 16.93 in. or 430.02 mm Depth: 20 in. or 508.00 mm	Height: 1.67 in. or 42.42 mm Width: 16.93 in. or 430.02 mm Depth: 25.51 in. or 647.95 mm	Height: 1.7 in. or 43.18 mm Width: 19.02 in. or 483.11 mm Depth: 22.28 in. or 565.91 mm	Height: 1.7 in. or 43.18 mm Width: 19.02 in. or 483.11 mm Depth: 28.94 in. or 735.08 mm
Max Weight	33 lbs or 14.97 kg	33 lbs or 14.97 kg	42 lbs or 19.05 kg	51 lbs or 23.13 kg
MTBF	58,000 hours	47,000 hours	75,000 hours	65,000 hours
Remote Access Card	No	No	RMM4	RMM4
Power Supply Unit	350 W Non-Redundant	350 W Non-Redundant	450 W Redundant PSU	750 W Redundant PSU
Motherboard	S3200	S3420GPRX	S1400SP4	R1000GZ
Environmental and Regulatory Specifications				
Operating Temperature	10°C to 30°C (50°F to 95°F) with the maximum rate of change not to exceed 10°C per hour	10°C to 30°C (50°F to 95°F) with the maximum rate of change not to exceed 10°C per hour	10°C to 35°C (50°F to 95°F) with the maximum rate of change not to exceed 10°C per hour	10°C to 35°C (50°F to 95°F) with the maximum rate of change not to exceed 10°C per hour
Non-Operating Temperature	-40°C to 70°C (-40°F to 158°F)	-40°C to 70°C (-40°F to 158°F)	-40°C to 70°C (-40°F to 158°F)	-40°C to 70°C (-40°F to 158°F)
Non-Operating Humidity	90%, non-condensing at 28°C	90% relative humidity, non-condensing at 35°C	50% to 90%, non-condensing with a maximum wet bulb of 28°C (at temperatures from 25°C to 35°C)	50% to 90%, non-condensing with a maximum wet bulb of 28°C (at temperatures from 25°C to 35°C)
Acoustic Noise	7.0 BA in an idle state at typical office ambient temperature. (23±2°C)	7.0 BA in an idle state at typical office ambient temperature. (23±2°C)	7.0 BA in an idle state at typical office ambient temperature. (23±2°C)	7.0 BA in an idle state at typical office ambient temperature. (23±2°C)
Shock, Operating	Half sine, 2 g peak, 11 Msec	Half sine, 2 g peak, 11 Msec	Half sine, 2 g peak, 11 Msec	Half sine, 2 g peak, 11 Msec
Shock, Unpackaged	Trapezoidal, 25 g, velocity change 136 inches/sec (≥ 40 lbs to < 80 lbs)	Trapezoidal, 25 g, velocity change 136 inches/sec (≥ 40 lbs to < 80 lbs)	Trapezoidal, 25 g, 170 inches/sec	Trapezoidal, 25 g, velocity change is based on packaged weight
Shock, Packaged	Non-palletized free fall in height 24 in. (≥ 40 lbs to < 80 lbs)	Non-palletized free fall in height 24 in. (≥ 40 lbs to < 80 lbs)	Product Weight: ≥ 40 to < 80 lbs Non-palletized Free Fall Height = 18 in. Palletized (single product) Free Fall Height = NA	Non-palletized Free Fall Height = 18 in.
Vibration, Unpackaged	5 Hz to 500 Hz, 2.20 g RMS random	5 Hz to 500 Hz, 2.20 g RMS random	5 Hz to 500 Hz, 3.13 g RMS random	5 Hz to 500 Hz, 2.20 g RMS random
ESD	±15 KV except I/O port ±8 KV per Intel environmental test specification	Air discharge 12 KV, Contact Discharge 8.0 KV	Air discharge 12 KV, Contact Discharge 8.0 KV	Air discharge 12 KV, Contact Discharge 8.0 KV
System Cooling Requirement	1660 BTU/hour	1660 BTU/hour	2550 BTU/hour	2550 BTU/hour
Safety				
EN 60950-1:2006/A11:2009/A1:2010/ A12:2011	Yes	Yes	Yes	Yes
UL60950-1/CSA C22.2 No. 60950-1, 2nd Edition + AMD 1:2011	Yes	Yes	Yes	Yes

	EMG-4000-B	EMG-4500-B	EMG-5000-D	EMG-5500-D
EMC				
Title 47 of the CFR, Part 15, Class A	Yes	Yes	Yes	Yes
ICES-003 Issue 4, February 7, 2004 Class A	Yes	Yes	Yes	Yes
EN 55022:2010 + AC:2011	Yes	Yes	Yes	Yes
EN 55024: 2010	Yes	Yes	Yes	Yes
VCCI V-1/07.09, V-2/08.04, V-3/08.04, V-4/07.04	Yes	Yes	Yes	Yes
BSMI CNS13438 Emissions (Taiwan)	Yes	Yes	Yes	Yes
AS/NZS CISPR 22 Emissions (Australia/NZ)	Yes	Yes	Yes	Yes
EN 61000-4-2 ESD	Yes	Yes	Yes	Yes
EN 61000-4-3 RF Immunity	Yes	Yes	Yes	Yes
EN 61000-4-6 Conducted Immunity	Yes	Yes	Yes	Yes
EN 61000-4-4 Electrical Fast Transients	Yes	Yes	Yes	Yes
Country Approvals				
USA	Yes	Yes	Yes	Yes
Canada	Yes	Yes	Yes	Yes
European Union (CE Mark)	Yes	Yes	Yes	Yes
China CCC	Yes	Yes	Yes	Yes
EAC (Euro-Asia Conformity) Russia, Kazakhstan, and Belarus	Yes	Yes	Yes	Yes
Argentina IRAM	Yes	Yes	Yes	Yes
South Africa LoA/SABS	Yes	Yes	Yes	Yes
Korea MISP	Yes	Yes	Yes	Yes
Australia/New Zealand	Yes	Yes	Yes	Yes
Israel	Yes	Yes	Yes	Yes
Croatia	Yes	Yes	Yes	Yes
Japan	Yes	Yes	Yes	Yes

Anexo 2 Mejores prácticas de Filtrado de contenido

Mejor práctica No. 1

Las normas de Filtrado de contenido se deben revisar manualmente durante 1-2 semanas antes de permitir que funcionen de manera autónoma sin el temor de que generen “detecciones falsas”. El método preferido para verificar la confiabilidad de la *norma* consiste en seleccionar “colocar en cuarentena” como la acción de la norma temporal donde los administradores pueden ver la información de encabezado del mensaje y el cuerpo (y los adjuntos) del correo electrónico. En casos en los que la norma genere una “detección falsa”, los administradores editarán la norma según corresponda.

Mejor práctica No. 2

Los diccionarios no deben contener palabras que, utilizadas en otros contextos, sean legítimas. Por ejemplo, la palabra “hot” (caliente) puede aparecer en un correo electrónico pornográfico, pero también aparece en el contexto del clima. Es más probable que las palabras individuales generen detecciones falsas que las cadenas de varias palabras.

Mejor práctica No. 3

Asegúrese de que alguna persona del departamento de Recursos Humanos le explique las normas de uso del correo electrónico en cuanto a lo que se considera aceptable e inaceptable.

Mejor práctica No. 4

En ambientes con gran volumen de correo (más de 50.000 mensajes por día), el Registro detallado (diario) de la Cola de espera alcanzará rápidamente un tamaño tan grande que quizás no sea práctico abrirlo en una ventana del explorador dentro de la interfaz gráfica. Se recomienda a los administradores iniciar una sesión en la Interfaz de línea de comandos a través del cliente SSH.

Mejor práctica No. 5

Aunque es una aplicación poderosa capaz de procesar decenas de miles de mensajes por hora, examina un mensaje para detectar coincidencias de diccionario, una vez por cada diccionario habilitado. Si están habilitados veinte diccionarios, examinará el mensaje veinte veces.

No existe diferencia en el rendimiento si se utilizan diez diccionarios de 1.000 palabras o cinco diccionarios de 2.000 palabras.

Anexo 3 Licencias Disponibles para McAfee Email Gateway

Estas son algunas de las licencias que están disponibles para McAfee Email Gateway:

• **Mail-Firewall** (proporciona configuración y cifrado para el envío de mensajes)

• **Mail-IDS** (ofrece protección las 24 horas del día, los 7 días de la semana, para bloquear los ataques contra la *red*)

• **Producto Base** (ofrece las funciones básicas de la versión reforzada de IronMail y la posibilidad de aplicar proxy al correo electrónico)

• **Mail-VPN** (proporciona configuración y cifrado para la recuperación de mensajes)

• **Administrador de Políticas** (permite la creación y aplicación de normas de correo electrónico)

• **McAfee Anti-Virus** (proporciona protección contra virus)

• **Anti-spam** (proporciona protección contra spam)

• **Secure Delivery** (proporciona una variedad de opciones para garantizar que los mensajes se entreguen de manera segura—por ej., *SSL*, S/*MIME*, PGP o HTTPS)
• **IronWebMail** (permite aplicar proxy y proteger el sistema de correo web)
• **Mantenimiento** (proporciona asistencia técnica las 24 horas del día, los 7 días de la semana, y actualizaciones para el software de IronMail)
• **Threat Response Updates (TRU)** (proporciona "normas" oportunas para la protección contra amenazas al correo electrónico para las cuales no existe otra solución actualmente)
• **Actualizaciones de firmas** (proporciona actualizaciones oportunas de las firmas de Mail-IDS que se utilizan para detectar los ataques de los hackers)
Los administradores pueden agregar licencias o extender la fecha de vencimiento de los productos o servicios en cualquier momento. (Las licencias se acumulan—es decir, se concatenan—en el dispositivo).