INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

INFORME ANUAL 2012

RED DE SENSORES DE INTECO

Red de Sensores de Inteco

Enero 2013

Instituto Nacional
de Tecnologías
de la Comunicación

Índice

Índice de figuras

1. INTRODUCCIÓN Y EQUIPO RED DE SENSORES DE INTECO

El objeto de este informe es ofrecer un resumen de la evolución experimentada de la Red de Sensores de INTECO durante el pasado año 2012, analizar la situación de la red de sensores al fin del año 2012 y resumir las incidencias destacadas en dicho periodo.

En primer lugar se muestra la situación de la red de sensores a la conclusión del año 2012, la actividad de los sensores, las incorporaciones y los convenios suscritos a lo largo del año.

En el apartado de Datos del Año aparecen diferentes estadísticas e incidencias ocurridas a lo largo del año. Se resumen datos sobre el volumen de correo analizado, virus, vulnerabilidades y se citan noticias o eventos que estimamos hayan podido resultar de interés para la comunidad que forma la Red de Sensores de INTECO durante el año 2012.

A continuación incluimos la información de contacto a la que deberéis dirigiros para resolver cuantas dudas puedan surgir.

Área técnica Análisis, diseño y desarrollo de scripts. Soporte a sensores. soporte.sensores@inteco.es	
Luis Fernández Prieto	luis.fernandez@inteco.es
Área Institucional y Coordinación Gestión de Sensores y colaboraciones. gestion.sensores@cert.inteco.es	
Jorge Chinea López	jorge.chinea@inteco.es
Coordinación Coordinación y lista de correo rsi@sensores.inteco.es	

2. EVOLUCIÓN RED DE SENSORES DE INTECO

Al finalizar el año 2012, la Red de Sensores de INTECO está formada por **103 entidades** que albergan al menos un sensor y que están ubicados en diferentes sectores con el porcentaje de distribución que aparece en la figura.

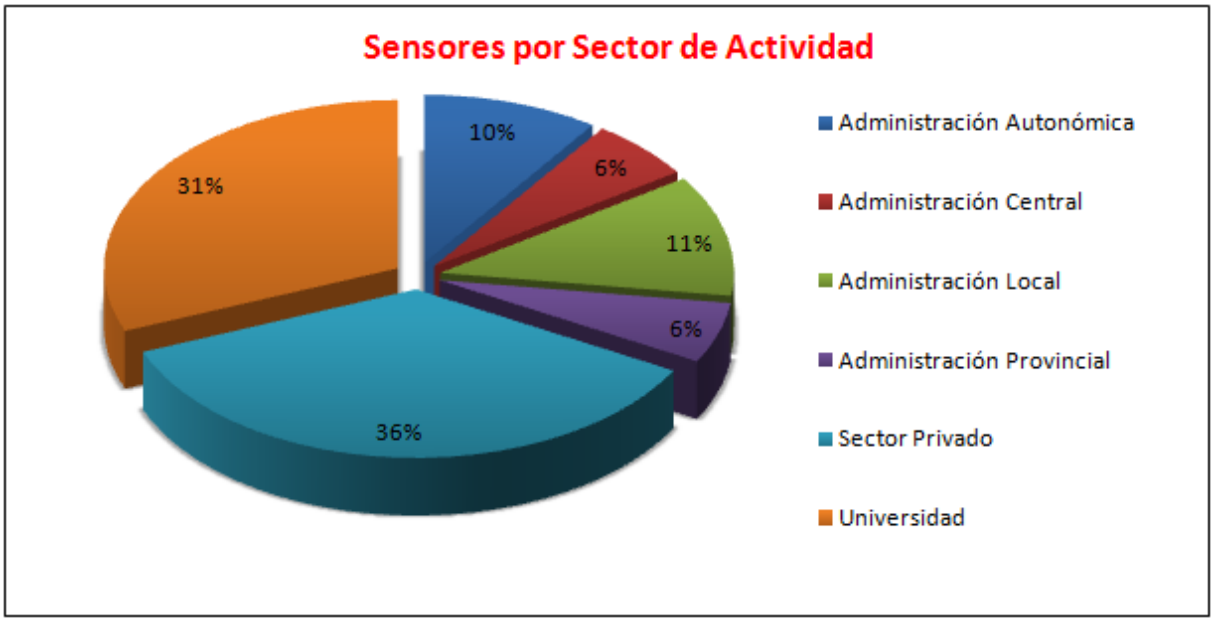

Figura 1: Distribución de los sensores por sector de actividad.

2.1. Actividad de los sensores

Los gráficos de actividad para el año 2012 revelan cómo el número de sensores con baja frecuencia de envío se ha reducido fuertemente a lo largo del año. La razón son los ajustes realizados, dando de baja entidades y sensores que llevaban mucho tiempo sin dar señales de vida.

También se han reducido los sensores con una frecuencia de envíos 'alta', en su mayoría por la irrupción del servició LAVADORA de Rediris en el sector universitario.

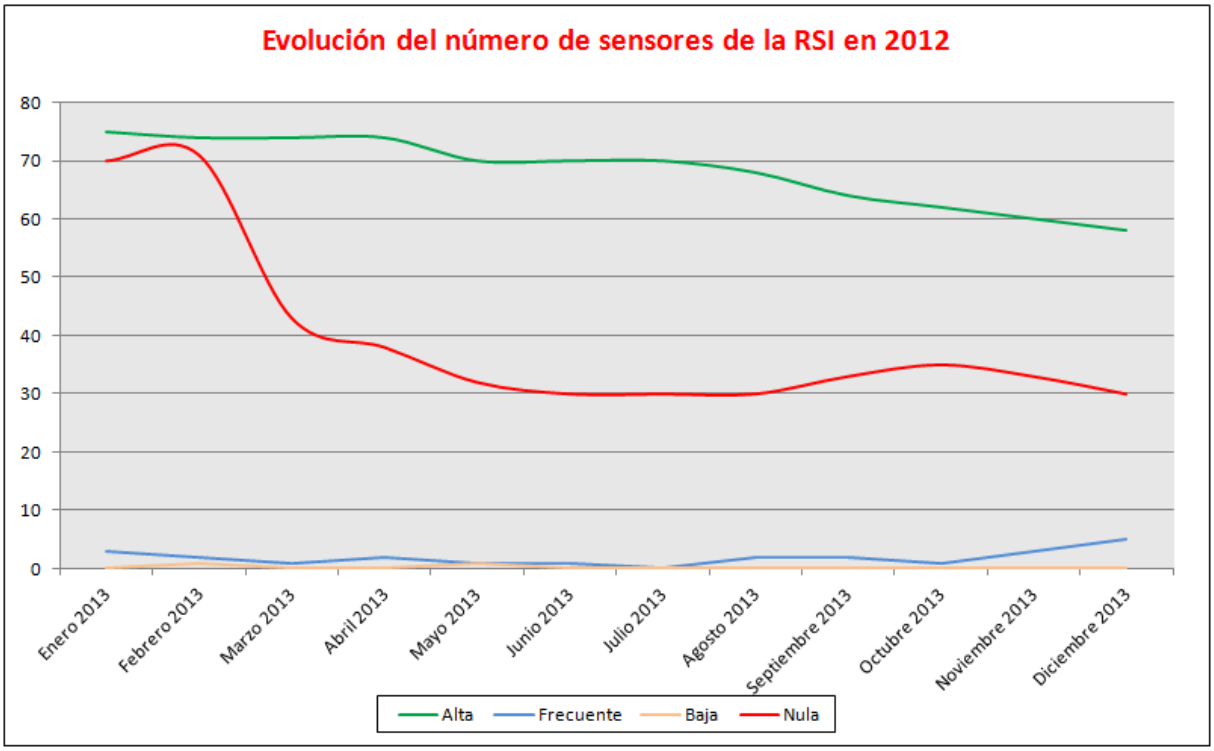

Figura 2: Evolución de la Actividad de los Sensores según la frecuencia en el envío del informe.

2.2. Nuevos sensores

En la siguiente tabla aparecen aquellas entidades que han formalizado el convenio de colaboración con INTECO durante el año 2012 o bien han enviado el primer informe durante este año.

Entidad	Fecha de envío primer informe	Fecha de publicación de la nota de portada
MasBytes	26/11/2012	-

3. DATOS DEL AÑO

3.1. Correos electrónicos procesados

La Figura 3 muestra el volumen de correo procesado mensualmente y el número de detecciones registradas. Nótese el doble eje del gráfico que muestra a la izquierda y en azul los correos analizados y a la derecha en rojo el número de virus encontrados.

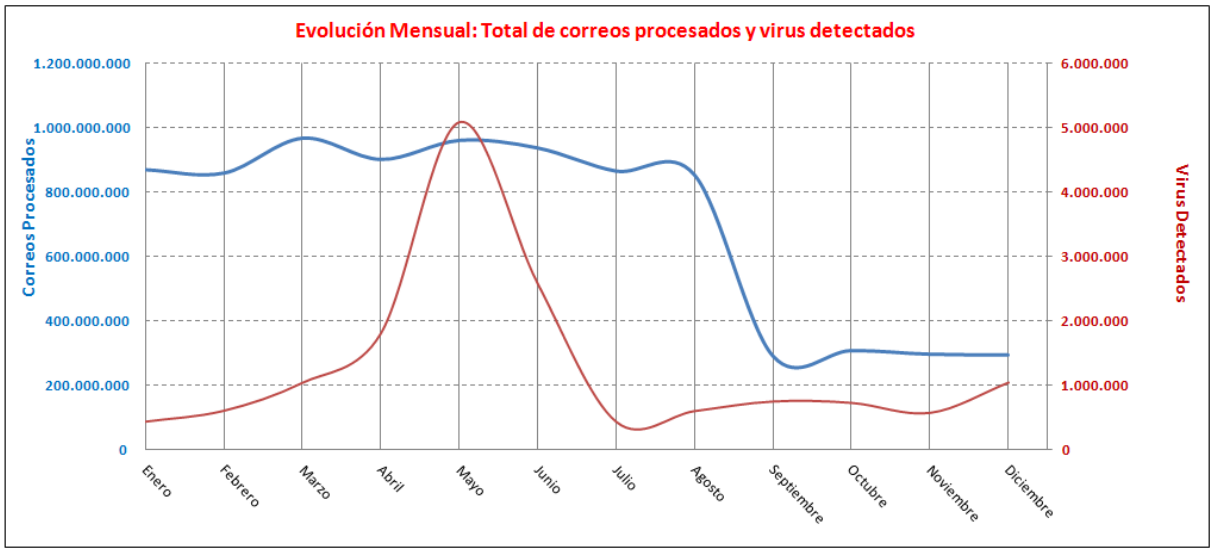

Figura 3: Evolución mensual de correos procesados y virus detectados.

Se puede observar en el gráfico que el número de correos procesados se mantiene más o menos estable a lo largo del año. La reducción que se ve en el mes de Septiembre se debe a la parada de envíos de uno de nuestros sensores más importantes: Mundivía. El volumen de virus detectados en correo, sufre una fuerte subida en los meses de Abril, Mayo y Junio. La razón fue una campaña de malware que afectó a varios de los sensores del sector privado.

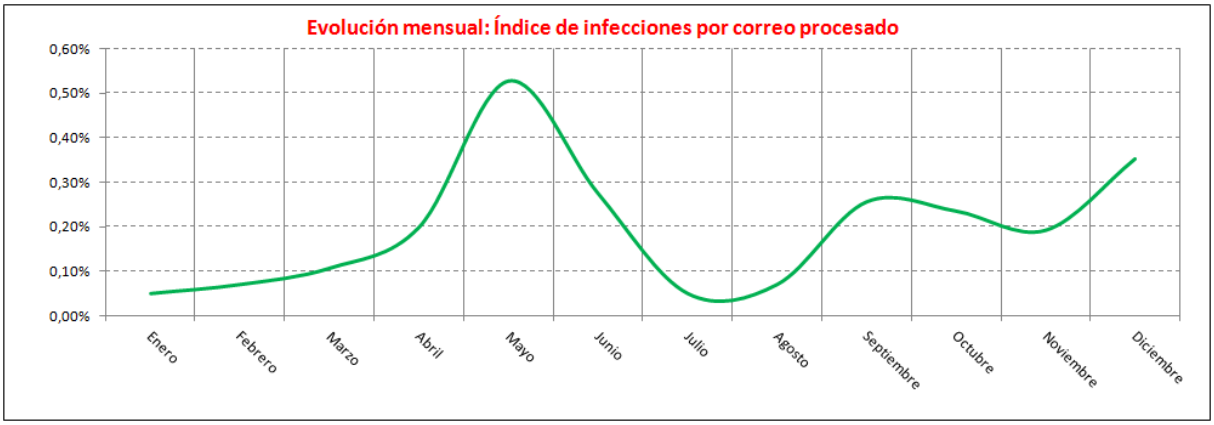

Figura 4: Evolución mensual del índice de virus detectados / correos procesados.

La figura 4 muestra de manera más precisa la evolución del índice de infecciones registradas por correo procesado.

A continuación se muestra la aportación al volumen de correos procesados de los diferentes sectores de actividad durante el año 2012.

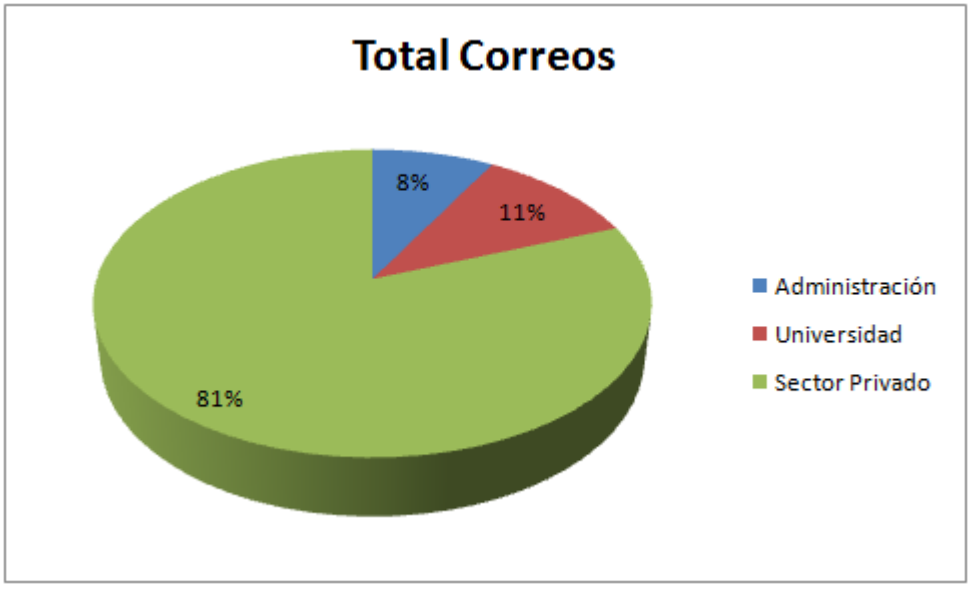

Figura 5: Aportación al volumen de correos procesados por cada sector de actividad.

Puede apreciarse que el sector de actividad "Sector privado" que constituye (tal y como se mostraba al principio de este informe) el 36% de los Sensores, es el sector que procesa más cantidad de mensajes, debido a que son sensores muy representativos del sector con un gran volumen de usuarios de correo electrónico. Dentro de este sector se encuentran las empresas proveedoras de servicios de correo electrónico.

Con respecto a 2012 este gráfico no cambia significativamente, el sector privado pasa del 83% al 81% y la administración aumenta ligeramente su "importancia" dentro de la red de sensores pasando del 6% al 8%.

3.2. Virus

La información que actualmente genera cada uno de los sensores de la red de INTECO y que diariamente se envía y procesa, hace referencia fundamentalmente al total de correos electrónicos procesados, virus detectados y su frecuencia de aparición.

Para analizar dicha información hay que tener en cuenta que los datos proporcionados por cada sensor dependen de la configuración y arquitectura de seguridad aplicada en cada uno de ellos. La utilización, cada vez más frecuente, de filtros anti-spam (listas negras, blancas y grises, eliminación por tipo de adjunto, etc.) que se anteponen a la labor del antivirus, debe tenerse en cuenta a la hora de analizar la información proporcionada.

3.2.1. Top Virus del año

La figura muestra la lista de los 10 virus *documentados* en INTECO-CERT que se consideran más activos en la Red de Sensores de INTECO, dado que han sido detectados por los antivirus de los sensores en mayor proporción durante el año.

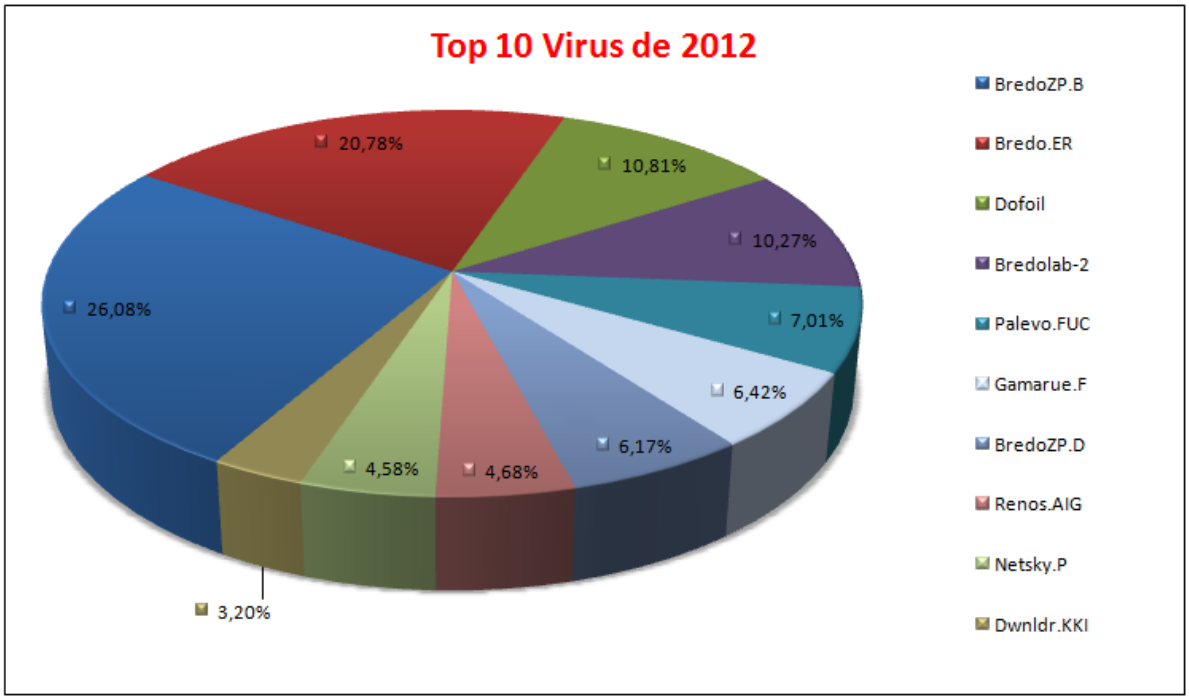

Figura 6: Virus más activos en la red de sensores durante el año 2011.

Analizando la evolución de las incidencias de Virus en la Red de Sensores, encontramos los 10 virus más activos a lo largo de 2012 han sido los que se muestran en la Figura 6. Destacan, por su grado de actividad el *BredoZP.B*, con el 26,08% del total de infecciones del año, el *Bredo.ER* con el 20,78% y el *Dofoil* con el 10,81%.

Esto puede comprenderse mejor a la vista de la siguiente figura, que muestra la evolución mes a mes del grado de actividad de los 8 virus con más incidencias con respecto al total de las detecciones documentadas.

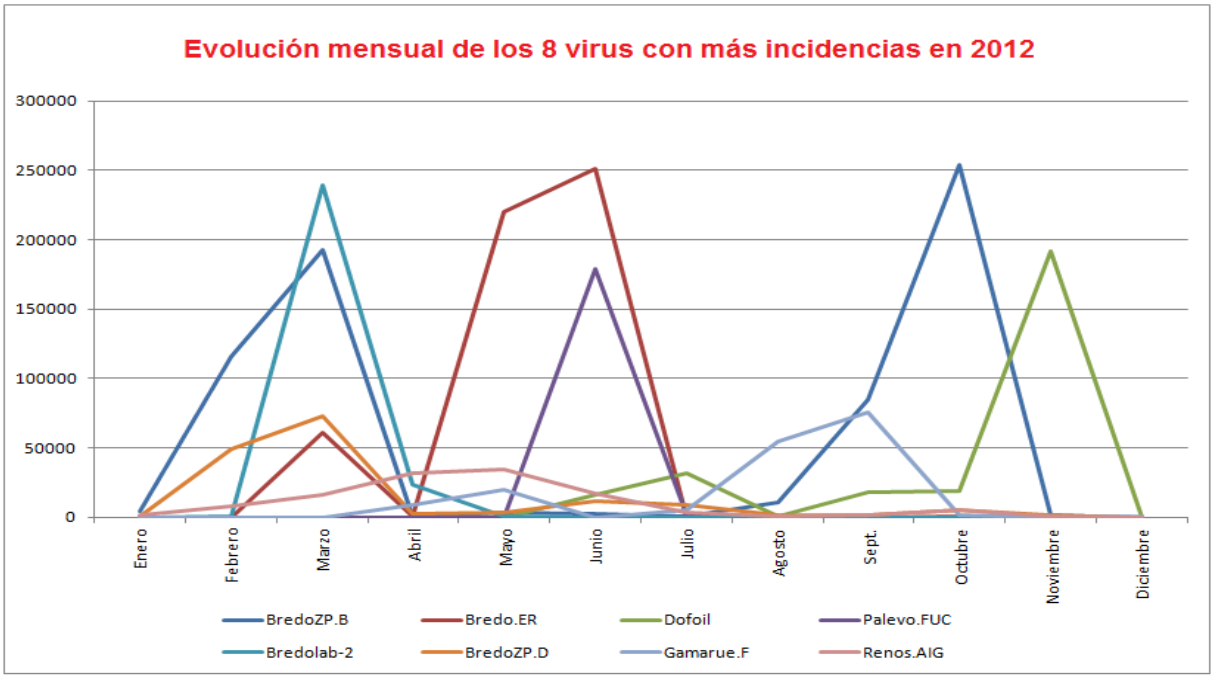

Figura 7: Virus más activos mes a mes en la red de sensores durante el año 2011.

En esta gráfica se ve claramente que las incidencias de virus responden a campañas temporales en las que un determinado virus se muestra muy activo para, posteriormente desaparecer del mapa. Por ejemplo el virus BredoZP.B tuvo picos de actividad los meses de Marzo y Octubre, Bredolab-2 afectó sobre todo en Marzo, Bredo.ER fue el más activo los meses de Mayo y Junio y a Dofoil lo encontramos sobre todo en Noviembre.

3.2.2. Virus por sectores de actividad

La presencia de virus en los diferentes sectores de actividad de los sensores de la Red de Sensores de INTECO sobre el volumen de correo procesado en cada uno de ellos aparece en la siguiente figura.

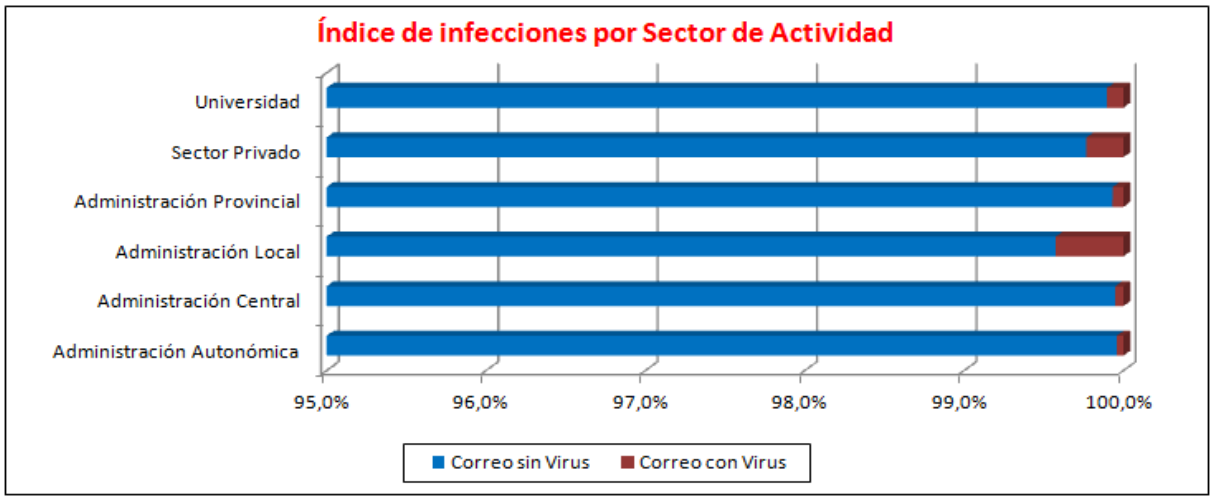

Figura 8: Porcentaje de correos analizados sin virus frente a correos con virus por sector de actividad.

3.3. Vulnerabilidades

3.3.1. Nivel de severidad de vulnerabilidades

La siguiente gráfica muestra el número de vulnerabilidades documentadas en http://cert.inteco.es y su nivel de severidad a lo largo del año 2012.

A lo largo de este año se emitieron un total de **5260** vulnerabilidades, un 26% más que durante 2012.

La evolución mensual del número de vulnerabilidades según su nivel de severidad publicada aparece en la siguiente figura.

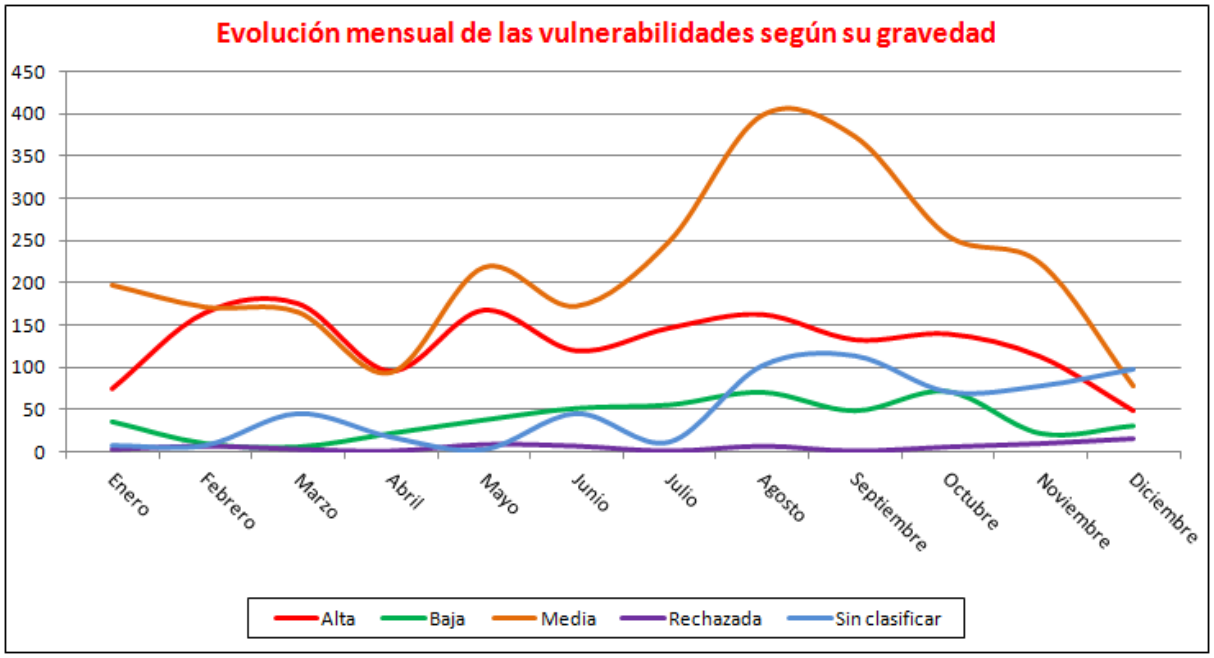

Figura 9: Evolución de las vulnerabilidades emitidas por nivel de riesgo.

En el gráfico se puede ver que la gran mayoría de las vulnerabilidades son de severidad media o alta y que el número de vulnerabilidades de estos tipos, dentro de ser variable, se mantiene más o menos igual y constante a lo largo del año.

3.3.2. Fabricantes y productos más afectados

La siguiente figura muestra los fabricantes más afectados por las vulnerabilidades registradas a lo largo del año 2012.

Este año es Mozilla el fabricante más afectado, aunque también es uno de los fabricantes que tienen más productos en el mercado. Con respecto al año pasado se ve un fuerte reducción del número de vulnerabilidades de Microsoft (un 50% de las vulnerabilidades que tuvo el año pasado), también una importante reducción de las vulnerabilidades en productos Oracle y por supuesto un fuerte crecimiento de las vulnerabilidades de Mozilla, que aumentan en un 250%.

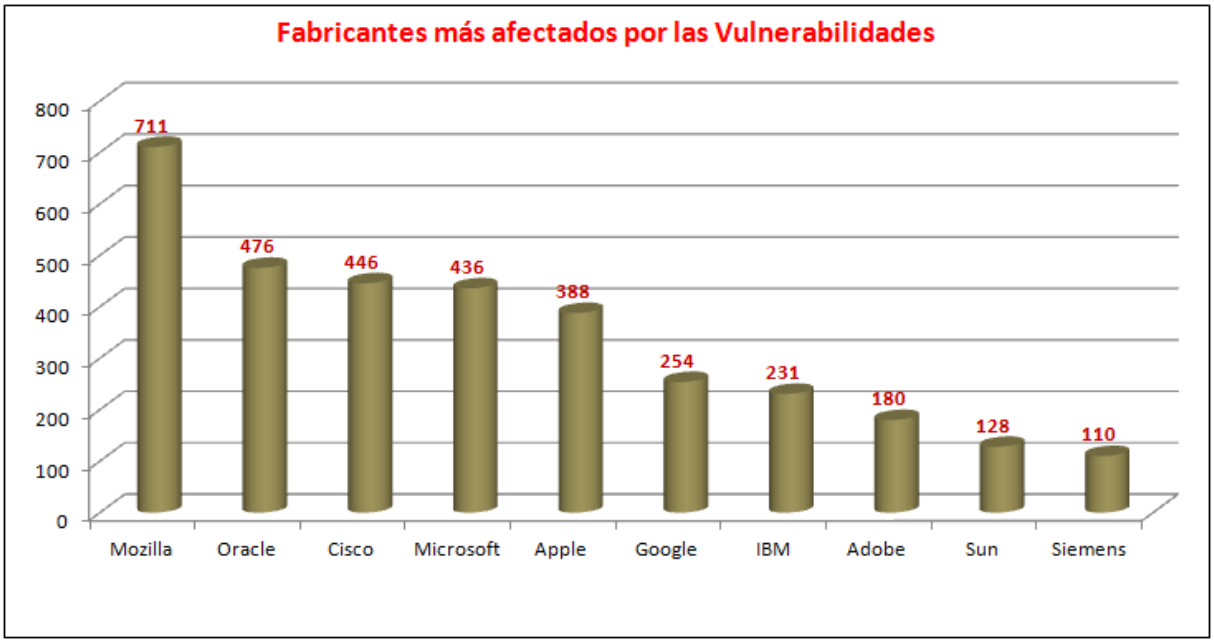

Figura 10: Fabricantes más afectados por las últimas vulnerabilidades.

3.3.3. Productos más afectados

La siguiente figura muestra los productos más afectados por las vulnerabilidades registradas a lo largo del año. Nótese que no aparecen aquellos productos afectados por menos de 60 vulnerabilidades.

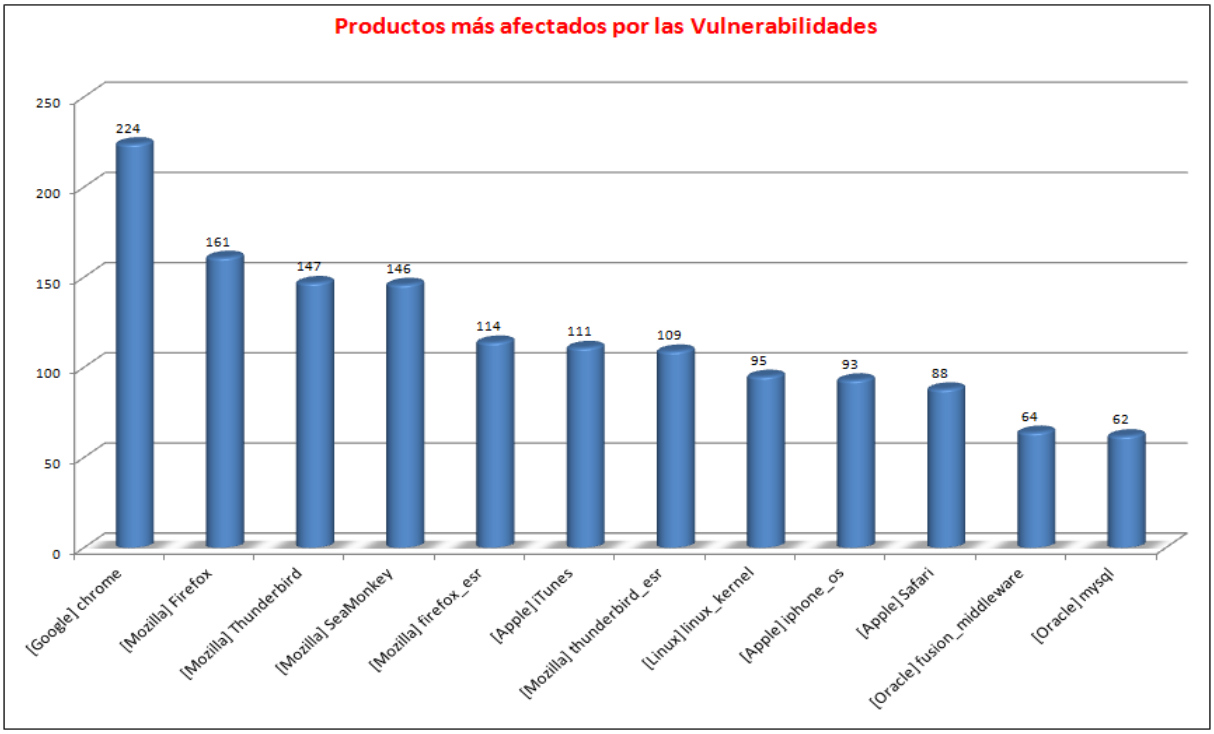

Figura 11: Productos más afectados por las últimas vulnerabilidades.

Uno productos más vulnerables continúa siendo *Google Chrome.* A éste le siguen hasta 6 diferentes productos de Mozilla.

3.3.4. Vulnerabilidades más comunes según su tipo

El siguiente gráfico muestra los tipos de vulnerabilidades más comunes sobre el total de las registradas durante el año 2012. Los dos tipos principales de vulnerabilidades se repiten con respecto a 2011 y los porcentajes son muy similares. La mayor diferencia se muestra en el incremento de vulnerabilidades de tipo "Error de configuración" que pasaron del 9% en 2011 al 11% actual. Esto implica un aumento creciente puesto que en 2010 suponían únicamente el 6% de las vulnerabilidades.

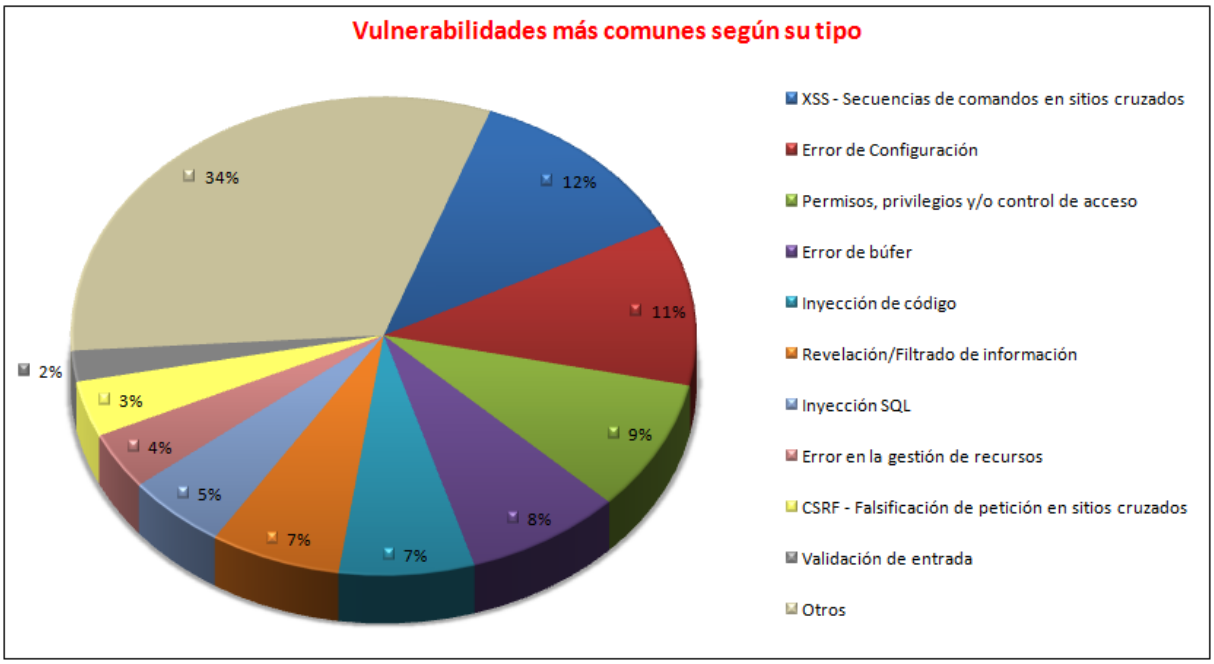

Figura 12: Tipos de vulnerabilidades más comunes.

3.4. SPAM

La información que actualmente genera cada uno de los Sensores de la red de INTECO y que diariamente se envía y procesa sobre el *spam*, reporta información sobre el *spam* recogida en los *logs* de su solución antispam.

Al igual que con los virus, para analizar dicha información hay que tener en cuenta que los datos proporcionados por cada sensor dependen de la política, configuración y arquitectura de seguridad aplicada en cada uno de ellos.

Para acceder a estos datos con información más actualizada y más específica visita: **https://ersi.inteco.es/**

3.4.1. Nivel de SPAM del año

La figura muestra el *spam* detectado a lo largo del año 2011, así como qué parte del mismo fue rechazado y cuál no.

El spam detectado corresponde al total de correos no deseados que llegaron al servidor de correo de las organizaciones participantes y el correo limpio se refiere a los correos que llegaron considerados como fiables o deseados.

La gráfica de la derecha corresponde al tratamiento que ha seguido el Spam Detectado, si se ha eliminado/descartado (*Spam* Rechazado), evitando que llegue al usuario, o no (*Spam* No Rechazado).

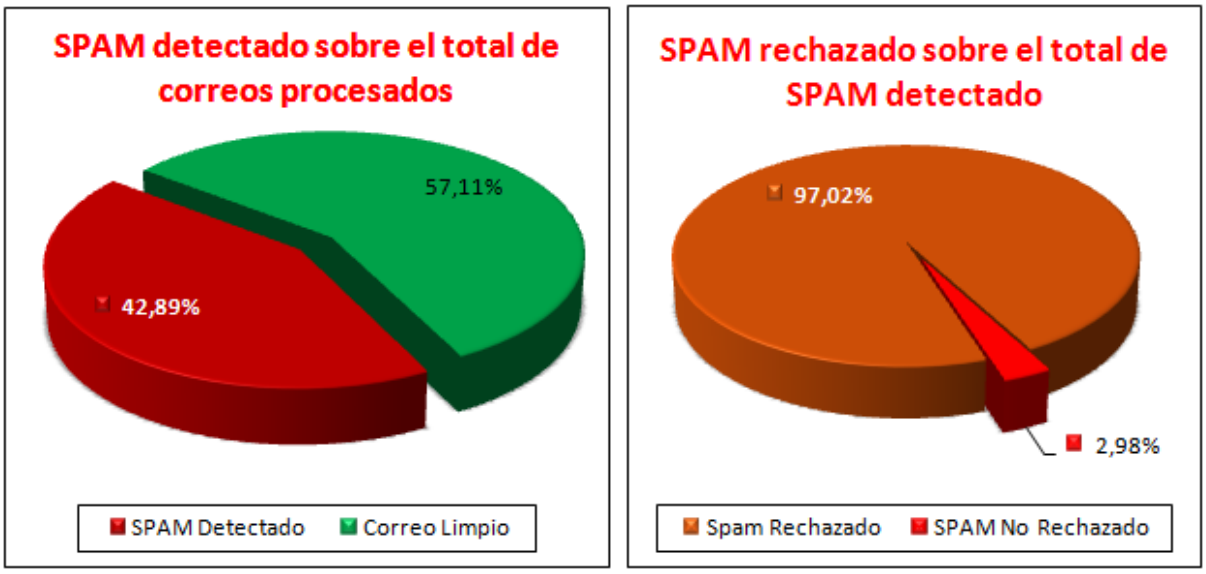

Figura 13: Nivel de SPAM detectado por la Red de Sensores.

El porcentaje de *spam* detectado en correo en 2012 ha sido muy similar al del año 2011, pasando de un 56,60% a un 57,11% del total de correos recibidos.

3.4.2. TOP 10 de los países origen de SPAM.

La figura de la página siguiente muestra el TOP 10 de los países origen del SPAM a lo largo del año 2012 y que afectaron a España. Hay que señalar que estos datos se obtienen en base a un muestreo estadístico sobre el total de los datos procesados.

En el gráfico se muestra que en el año 2012 Holanda fue el mayor emisor de SPAM hacia España. Realmente es un dato engañoso, ya que como se puede ver Estados Unidos es el tercer mayor emisor. La razón es que son países con gran concentración de servicios web que son también utilizados por los emisores de SPAM. Más claro es el caso de la India, que habiendo mandado 36 millones de correos este año, la gran mayoría son de SPAM..

Cabe mencionar que la pertenencia de un dominio a un país no se basa en la comprobación de la extensión del dominio sino usando técnicas de geolocalización de la IP de envío del SPAM.

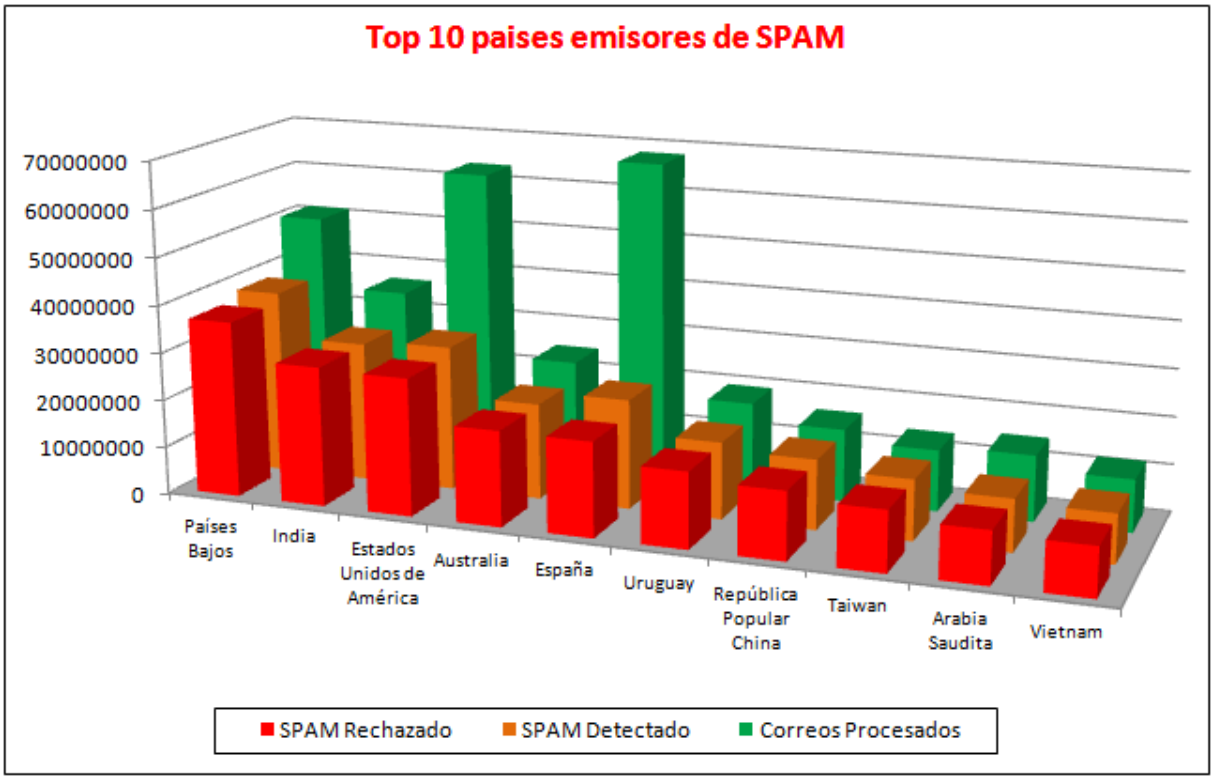

Figura 14: Top 10 de países origen de SPAM que afectan a España.

3.4.3. Evolución temporal de totales.

La siguiente figura muestra la evolución del *spam* a lo largo del año 2012. Son los datos de mensajes procesados, detectados y rechazados a lo largo del año dividido en intervalos mensuales.

Señalar que en esta ocasión, el número de correos procesados y detectados como *spam* prácticamente se solapan.

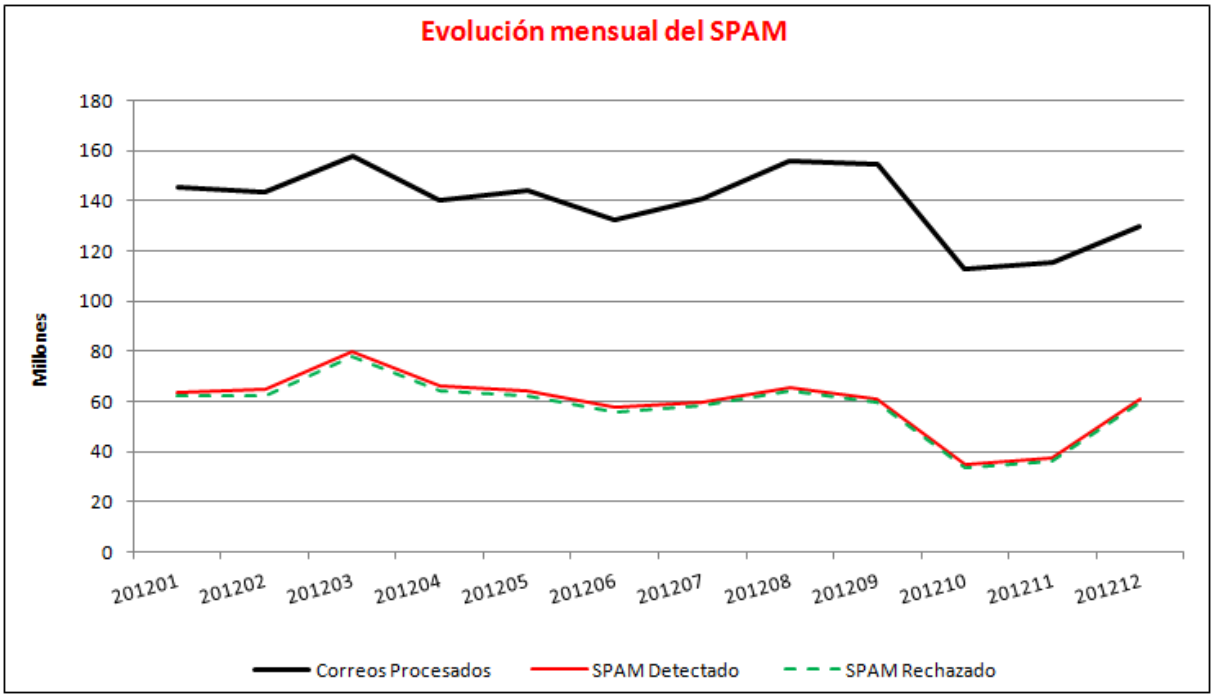

Figura 15: Evolución mensual del SPAM detectado por la red de sensores.

Puede apreciarse en la figura, por la proximidad de las líneas de correos procesados y *spam* detectado, cómo la cantidad de *spam* detectado se sitúa en torno al 60% de los correos procesados y cómo casi la totalidad de este *spam* es rechazado, de ahí que ambas líneas (la roja y la verde punteada) prácticamente se solapen.