INFORME TRIMESTRAL

RED DE SENSORES DE INTECO

CUARTO TRIMESTRE 2012

Red de Sensores de Inteco

Enero 2013

El presente documento cumple con las condiciones de accesibilidad del formato PDF (Portable Document Format).

Se trata de un documento estructurado y etiquetado, provisto de alternativas a todo elemento no textual, marcado de idioma y orden de lectura adecuado.

Para ampliar información sobre la construcción de documentos PDF accesibles puede consultar la guía disponible en la sección Accesibilidad > Formación > Manuales y Guías de la página http://www.inteco.es.

ÍNDICE

1. INTRODUCCIÓN Y EQUIPO RED DE SENSORES DE INTECO 6

2. EVOLUCIÓN RED DE SENSORES DE INTECO 7

2.1. Actividad de los sensores 7

3. DATOS DEL TRIMESTRE 8

3.1. Correos electrónicos procesados 8

4. VIRUS 10

4.1.1. Top Virus 10

4.1.2. Dispersión de antivirus en la Red de Sensores de INTECO 11

4.1.3. Virus por sectores de actividad 11

4.1.4. Virus por ámbito geográfico 13

4.2. SPAM 16

4.2.1. Nivel de SPAM 16

4.2.2. Evolución temporal de totales 17

4.2.3. Evolución trimestral del SPAM 17

4.2.4. Top 10 de dominios emisores de SPAM. 18

5. NO SOLO SENSORES 19

5.1. Vulnerabilidades 19

5.1.1. Productos más afectados 19

5.1.2. Fabricantes más afectados 19

5.1.3. Nivel de severidad de vulnerabilidades 20

5.1.4. Vulnerabilidades más comunes según su tipo 21

ÍNDICE DE FIGURAS

Figura 1: Distribución de los sensores por sector de actividad. 7

Figura 2: Distribución de sensores según frecuencia en el envío del informe. 7

Figura 3: Evolución trimestral de correos procesados y virus detectados. 8

Figura 4: Evolución trimestral del índice de infecciones por correo procesado. 8

Figura 5: Evolución mensual de correos procesados por sector de actividad. 9

Figura 6: Virus más activos en la red de sensores durante el pasado trimestre. 10

Figura 7: Antivirus utilizados en los sensores 11

Figura 8: Relación correos sin virus / correos con virus detectados por antivirus. **¡Error! Marcador no definido.**

Figura 9: Porcentaje de correos sin y con virus, por sectores de actividad. 12

Figura 10: Top virus por sector de actividad 12

Figura 11: Tabla de virus más detectados por sectores 13

Figura 12: Mapa autonómico de detecciones de virus. 14

Figura 13: Sensores, correo y porcentaje de infección detectada por autonomía. 15

Figura 14: Nivel de SPAM detectado por la red de sensores. 16

Figura 15: Evolución temporal del SPAM detectado por la red de sensores. 17

Figura 16: Evolución mensual del SPAM a lo largo del último año. 18

Figura 17: Top 10 países emisores de SPAM. 18

Figura 18: Productos más afectados por las últimas vulnerabilidades. 19

Figura 19: Fabricantes más afectados por las últimas vulnerabilidades. 20

Figura 20: Vulnerabilidades emitidas por nivel de riesgo. 20

Figura 21: Vulnerabilidades más comunes por tipo. 21

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 trimestre, analizar la situación actual de la red de sensores y resumir las incidencias destacadas en dicho periodo.

En primer lugar se muestra la situación actual de la red de sensores, la actividad de los sensores, las nuevas incorporaciones y los nuevos convenios suscritos a lo largo del trimestre.

En el apartado de datos del trimestre aparecen diferentes estadísticas e incidencias ocurridas a lo largo del trimestre. Se resumen datos sobre el volumen de correo analizado, virus y spam.

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	987 877 189 Ext. 5090
Área Institucional y Coordinación Gestión de Sensores y colaboraciones. gestion.sensores@cert.inteco.es		
Jorge Chinea López	jorge.chinea@inteco.es	987 877 189 Ext. 5059
Coordinación Coordinación y lista de correo rsi@sensores.inteco.es		

2. EVOLUCIÓN RED DE SENSORES DE INTECO

En la actualidad la "Red de Sensores de INTECO" (RSI) 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 siguiente figura.

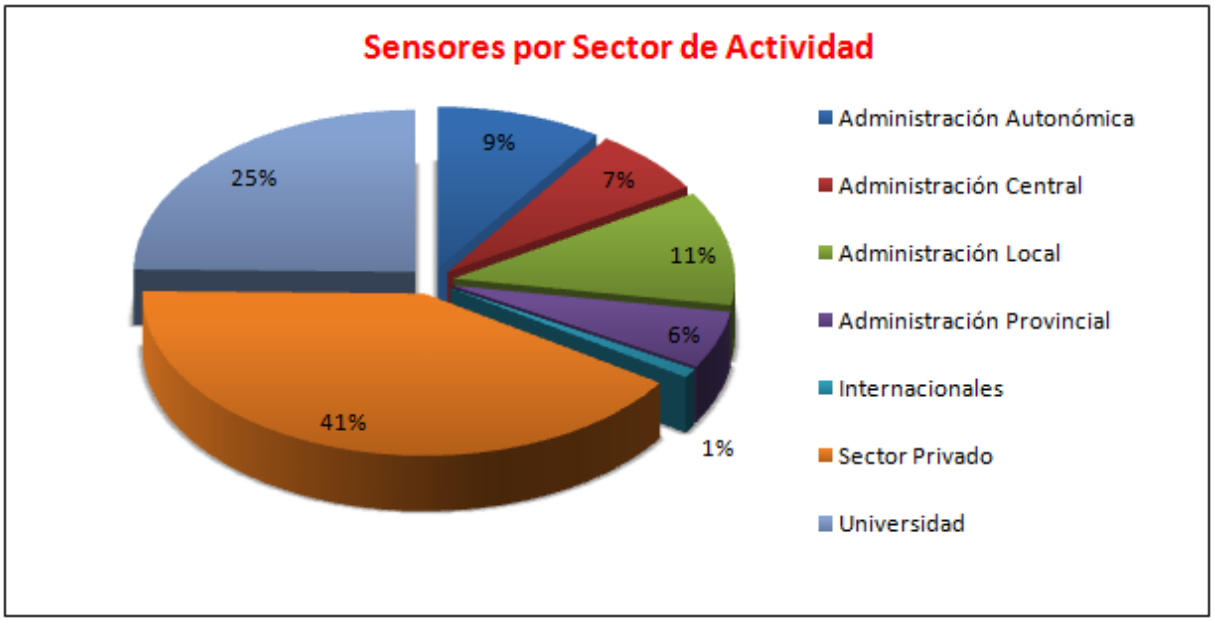

Figura 1: Distribución de los sensores por sector de actividad.

2.1. ACTIVIDAD DE LOS SENSORES

El gráfico de actividad para el último trimestre muestra que 5 sensores que enviaban de forma continua en el tercer trimestre envían ahora de forma intermitente:

Figura 2: Distribución de sensores según frecuencia en el envío del informe.

3. DATOS DEL TRIMESTRE

3.1. CORREOS ELECTRÓNICOS PROCESADOS

La Figura 3 muestra el volumen de correo procesado diariamente 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.

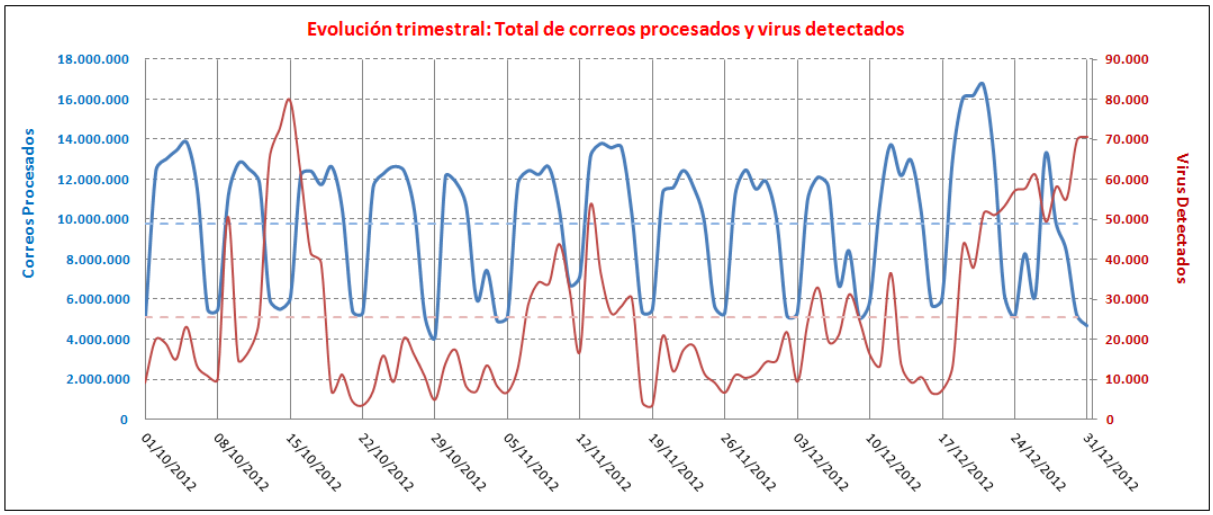

Figura 3: Evolución trimestral de correos procesados y virus detectados.

Cabe comentar la correspondencia de las caídas en el volumen de correos procesados coincidiendo con la disminución de actividad propia de los fines de semana y festivos.

La siguiente figura muestra de manera detallada la evolución del índice de infecciones por correo electrónico en los últimos tres meses.

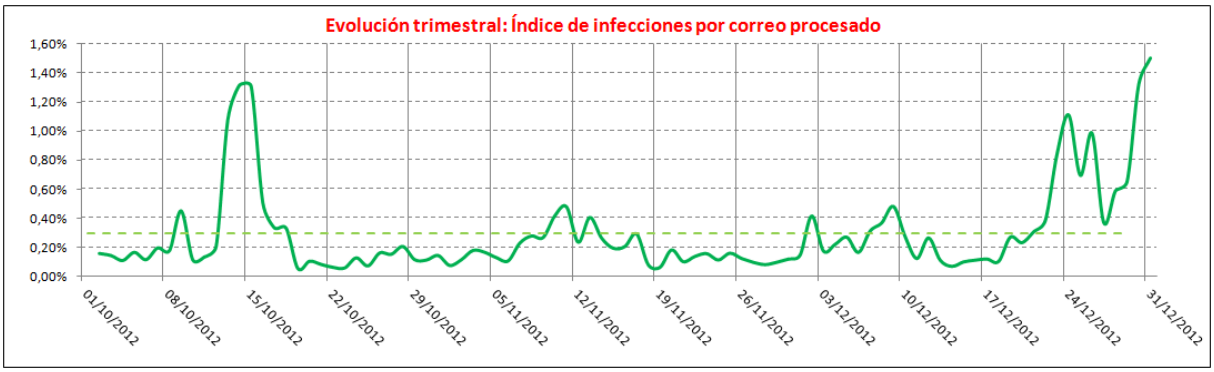

Figura 4: Evolución trimestral del índice de infecciones por correo procesado.

Se puede ver el fuerte incremento del nivel de peligrosidad del correo electrónico en las fechas navideñas.

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

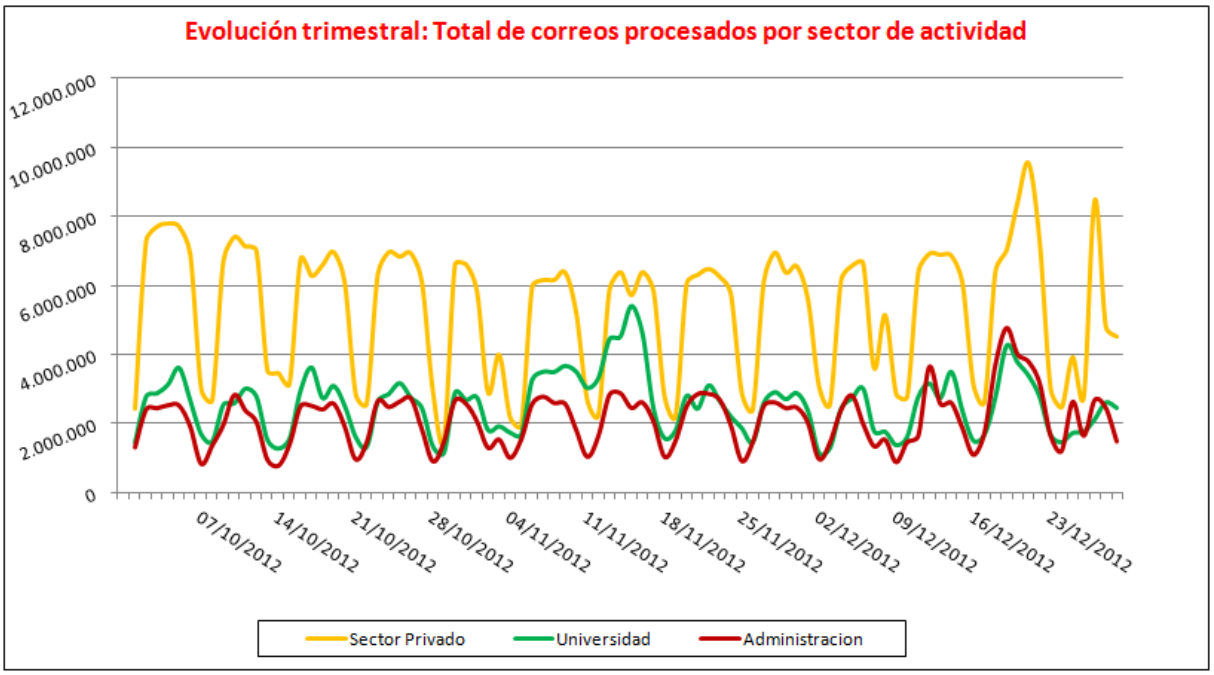

Figura 5: Evolución mensual de correos procesados por sector de actividad.

Puede apreciarse los fuertes altibajos ocasionados por los fines de semana. El SPAM no descansa en fin de semana, pero los trabajadores, sí. Esas diferencias de nivel son las ocasionadas por el trabajo diario y el correo remanente que siempre queda es, en su gran mayoría, SPAM.

4. 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.

4.1.1. Top Virus

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 cuarto trimestre de 2012.

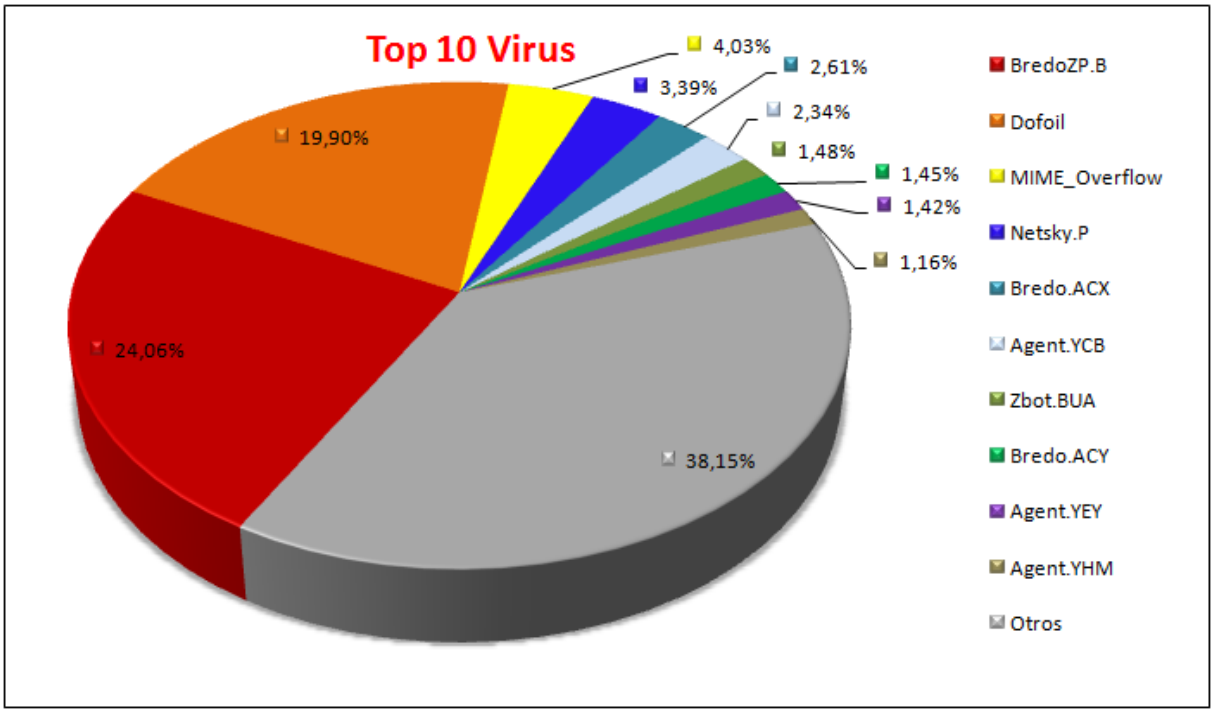

Figura 6: Virus más activos en la red de sensores durante el pasado trimestre.

Este trimestre, fue el virus *BredoZP.B* el que registró un mayor número de incidencias, por lo que copa el ranking con un grado de actividad de un 24,06% del total de infecciones. A continuación se sitúan el *Dofoil* y el *MIME_Overflow*, con un grado de actividad del 19,90%, y 4,03% respectivamente. Este trimestre hay un gran número de virus que no entran en el Top 10 pero que en su conjunto suponen el 38,15% del total del virus detectados.

4.1.2. Dispersión de antivirus en la Red de Sensores de INTECO

La siguiente figura ofrece el número de sensores que utilizan cada una de las distintas soluciones antivirus. La solución mayoritariamente adoptada es ClamAV, seguida por Trendmicro:

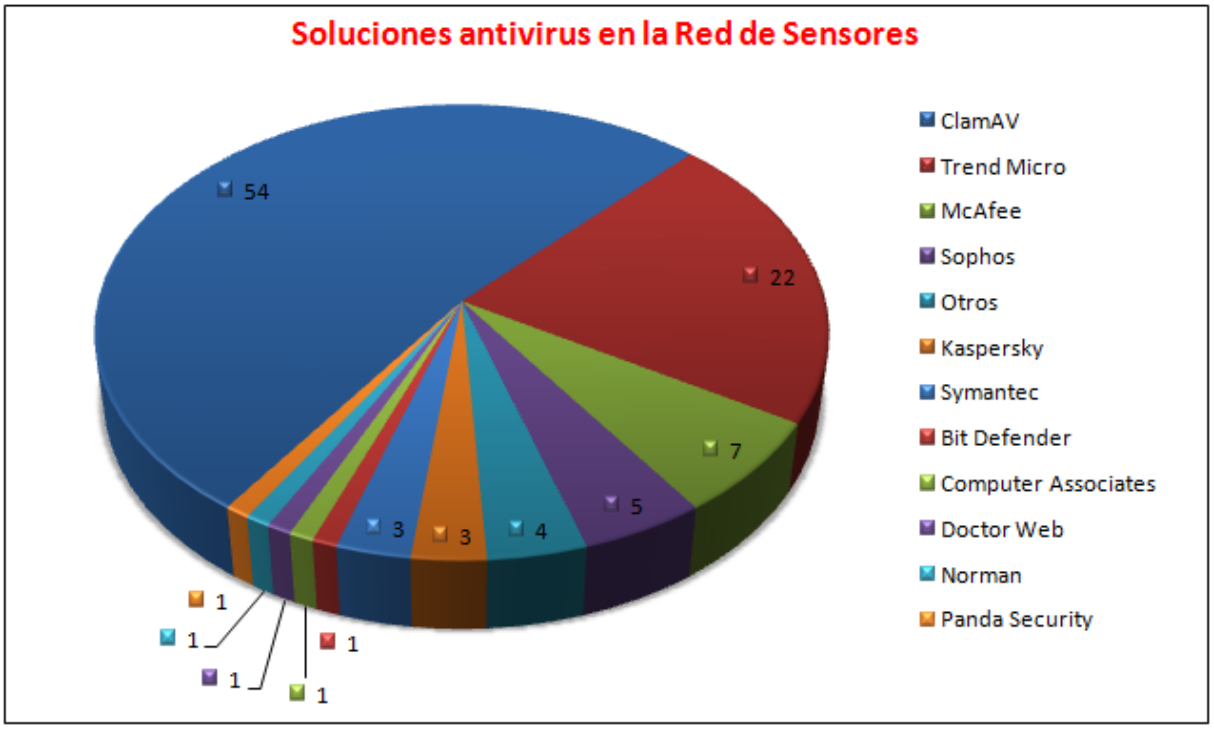

Figura 7: Antivirus utilizados en los sensores

4.1.3. 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.

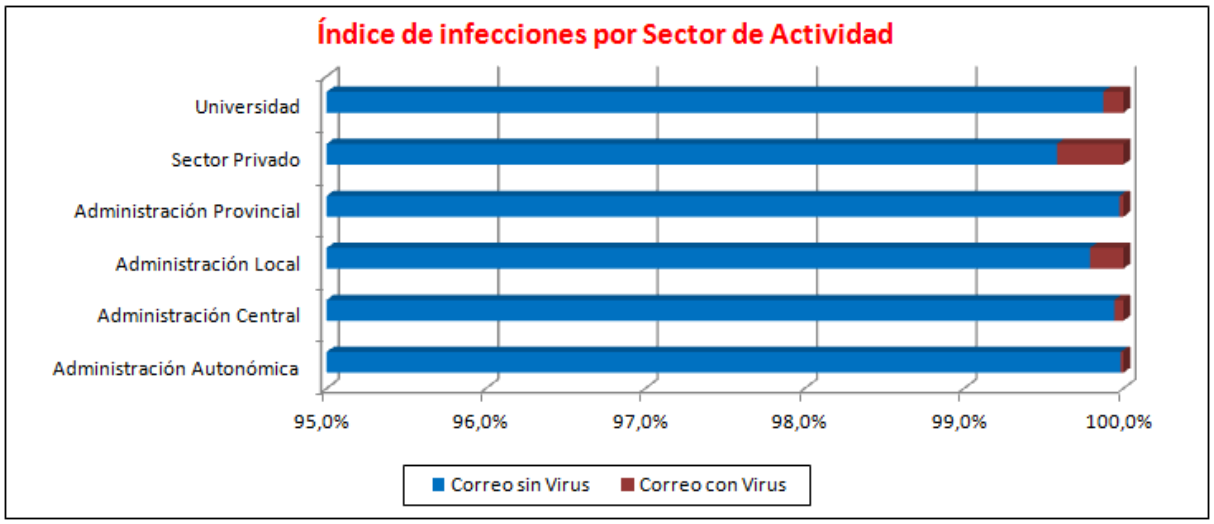

Figura 8: Porcentaje de correos sin y con virus, por sectores de actividad.

Como se ve, las soluciones antivirus van cumpliendo su trabajo y este trimestre, apenas un 0,14% (1,4 por cada 1.000) de los correos incluían algún tipo de malware.

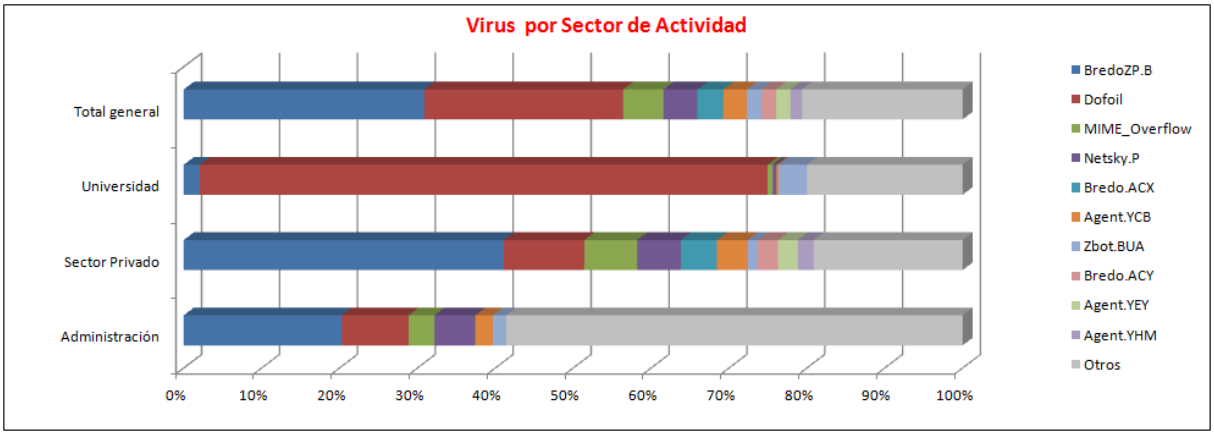

Figura 9: Top virus por sector de actividad

El gráfico anterior muestra la comparativa de virus más detectados por sectores de actividad, agrupando por un lado las administraciones, la universidad y el sector privado con los proveedores de servicios de correo electrónico.

Solo muestra información de los 10 virus más relevantes en su conjunto. Se puede comprobar que en la Administración más del 50% de los virus son “Otros”. La razón es que este trimestre dos virus atacaron bastante el correo de la Administración (*Netsky.R* y *Dwnldr.KKI*), con casi el 20% (cada una) de las infecciones en la administración y no aparecen en este gráfico porque en los otros dos grandes sectores (privado y Universitario) apenas supusieron el 0,5% de las infecciones.

Como información complementaria a la Figura 10, la anterior tabla muestra los valores de virus más frecuentes.

Virus	Administración	Sector Privado	Universidad	Total general
BredoZP.B	20,28%,	41,1%,	2,06%,	30,88%,
Dofoil	8,59%,	10,33%,	72,91%,	25,54%,
MIME_Overflow	3,31%,	6,79%,	0,64%,	5,17%,
Netsky.P	5,24%,	5,62%,	0,5%,	4,35%,
Bredo.ACX	0,01%,	4,62%,	0%,	3,34%,
Agent.YCB	2,25%,	3,96%,	0,24%,	3%,
Zbot.BUA	1,73%,	1,31%,	3,66%,	1,9%,
Bredo.ACY	0%,	2,58%,	0%,	1,87%,
Agent.YEY	0,02%,	2,53%,	0%,	1,83%,
Agent.YHM	0,01%,	2,06%,	0%,	1,49%,
Otros	58,55%,	19,1%,	19,98%,	20,62%,

Figura 10: Tabla de virus más detectados por sectores

Se puede ver que a cada sector les afecta más un tipo de virus diferente: En el ámbito universitario es *Dofoil* el virus más activo. Por el contrario, en la administración pública y en el sector privado el virus más activo fue *BredoZP.B*.

4.1.4. Virus por ámbito geográfico

La siguiente figura muestra el mapa autonómico de detecciones que está disponible de forma pública en el portal http://cert.inteco.es . Como resumen de las incidencias, la figura presenta el mapa calculado sobre los datos recibidos durante el cuarto trimestre de 2012.

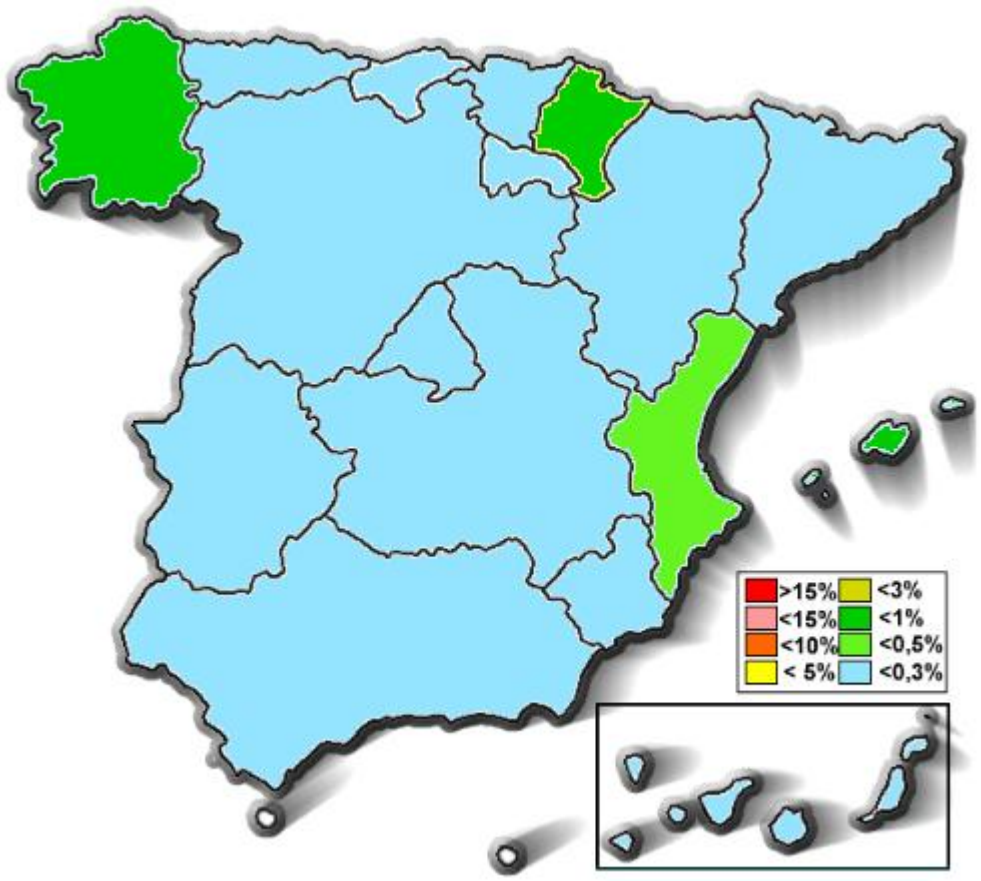

Figura 112: Mapa autonómico de detecciones de virus.

Los porcentajes de detección de cada comunidad se calculan sobre los datos de los sensores cuyo correo puede asociarse a un entorno geográfico determinado. Los Sensores de ámbito nacional o internacional, como pueden ser operadores de telecomunicaciones o proveedores de acceso a Internet que ofrecen su servicio en todo el territorio nacional, no computan para el cálculo de los porcentajes de detección por autonomía.

La siguiente tabla muestra el número de Sensores y correo procesado para cada una de las autonomías a lo largo de este trimestre.

Comunidad Autónoma	Muestra	Incidencias
Andalucía	37999	94610465
Aragón	207528	73456985

Asturias	20074	55830267
Canarias	2000	11368044
Cantabria	1	121666
Castilla-La Mancha	29503	64693883
Castilla y León	401	6338738
Catalunya	155536	116500552
Comunidad Valenciana	268202	61686328
Extremadura	161	818589
Galicia	476216	69322776
Islas Baleares	3991	407256
Madrid	7336	40224584
Murcia	18193	10099509
Navarra	71178	8209842
País Vasco	705	4035553

Figura 123: Sensores, correo y porcentaje de infección detectada por autonomía.

Se puede comprobar que es en Cataluña donde se procesan la mayor cantidad de los correos que nos ayudan a realizar estas gráficas. Sin embargo es en las Islas Baleares donde tienen un porcentaje de virus en correo más alto (0,56% de los correos con virus).

4.2. 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 se puede visitar: https://ersi.inteco.es/

4.2.1. Nivel de SPAM

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

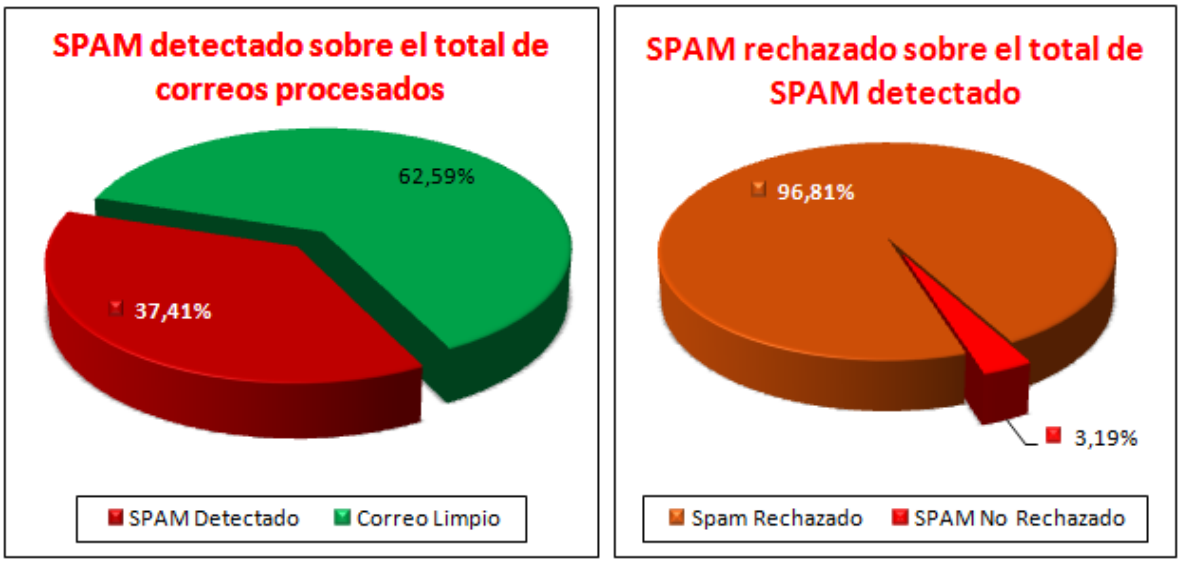

Figura 134: Nivel de SPAM detectado por la red de sensores.

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).

4.2.2. Evolución temporal de totales

La figura muestra la evolución del SPAM a lo largo de estos tres meses. Son los datos de mensajes procesados, detectados y rechazados a lo largo de un periodo de tiempo dividido en intervalos, de un día en este caso.

Cabe señalar que el número de correos procesados y detectados como spam prácticamente se solapan y que el número de correos disminuye muchos fines de semana.

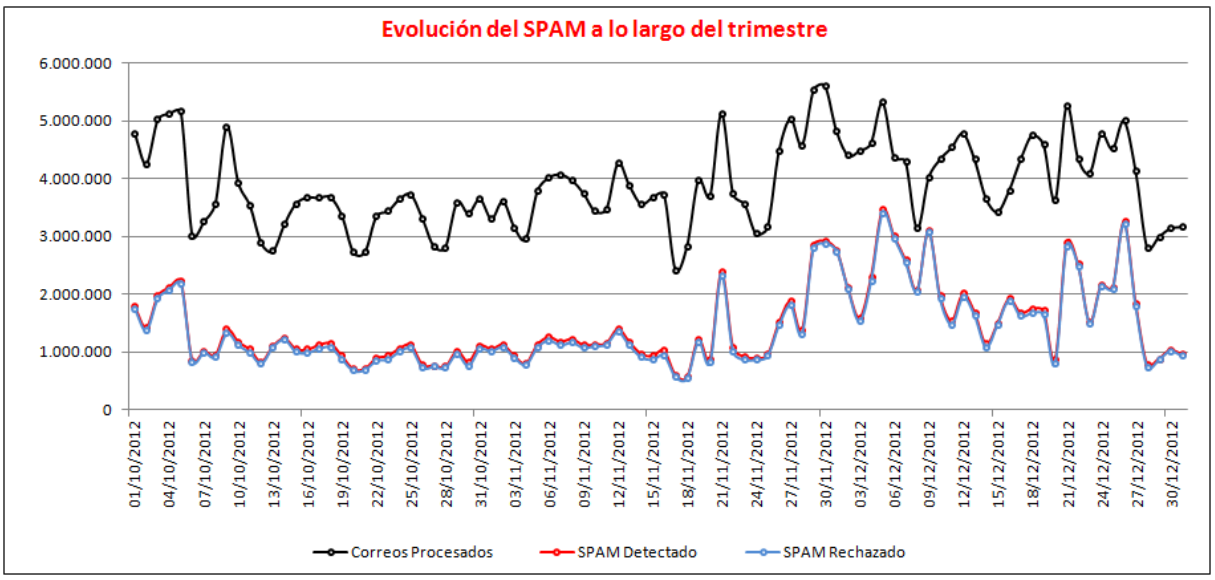

Figura 145: Evolución temporal del SPAM detectado por la red de sensores.

4.2.3. Evolución trimestral del SPAM

La siguiente figura muestra la evolución trimestral del nivel de SPAM detectado por la Red de Sensores a lo largo del último año. El nivel de SPAM se ha reducido hasta por debajo del 50% del correo electrónico, llegando a los poco menos de 200 millones de correos de SPAM.

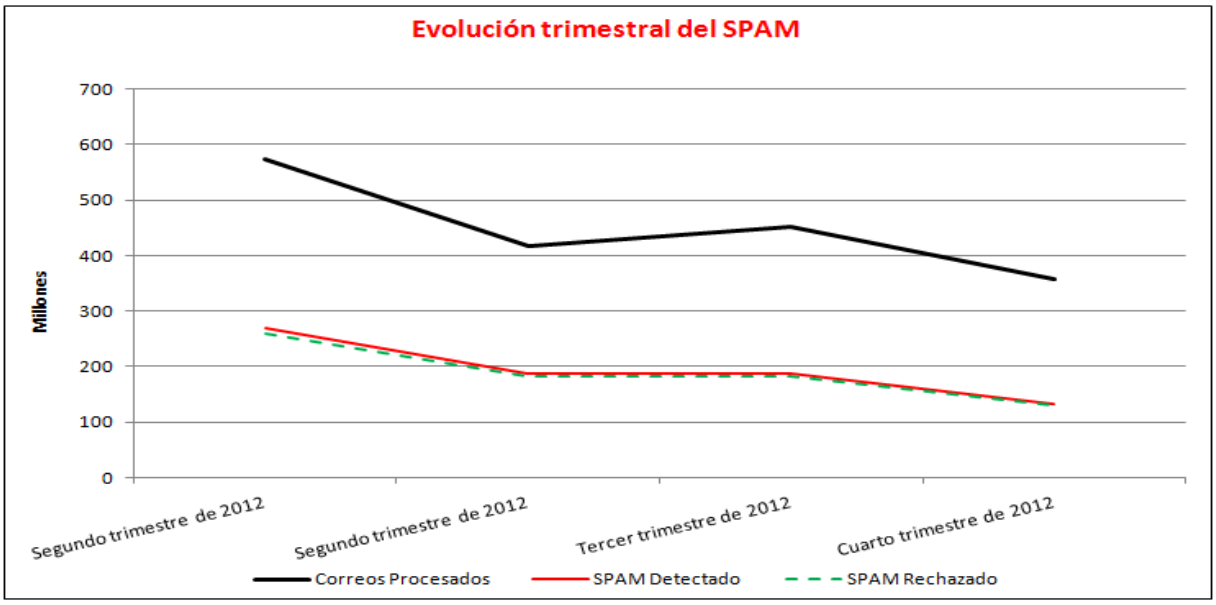

Figura 156: Evolución mensual del SPAM a lo largo del último año.

4.2.4. Top 10 de dominios emisores de SPAM.

La figura muestra los 10 países que envían mayor cantidad de SPAM. La información se muestra sesgada como spam rechazado, spam detectado y correos procesados.

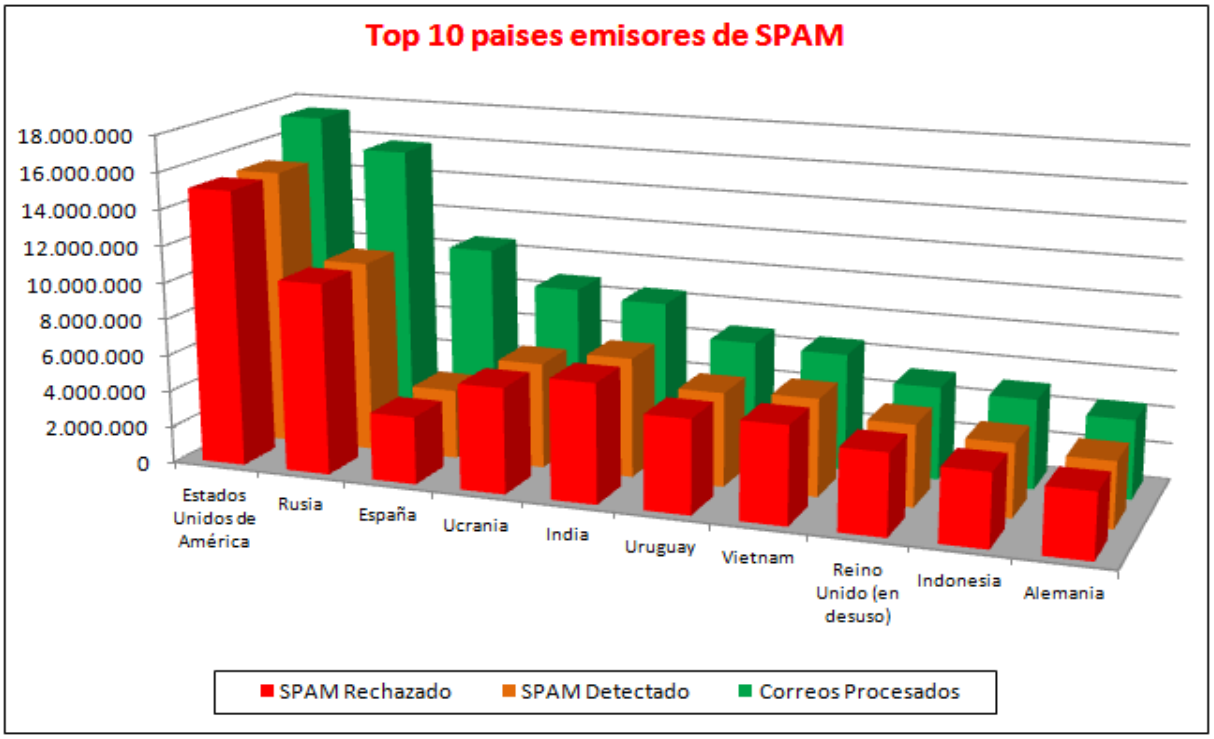

Figura 167: Top 10 países emisores de SPAM.

5. NO SOLO SENSORES

5.1. VULNERABILIDADES

5.1.1. Productos más afectados

La figura muestra los productos más afectados por las vulnerabilidades del último trimestre.

Nótese que sólo aparecen aquellos productos afectados por 15 o más nuevas vulnerabilidades.

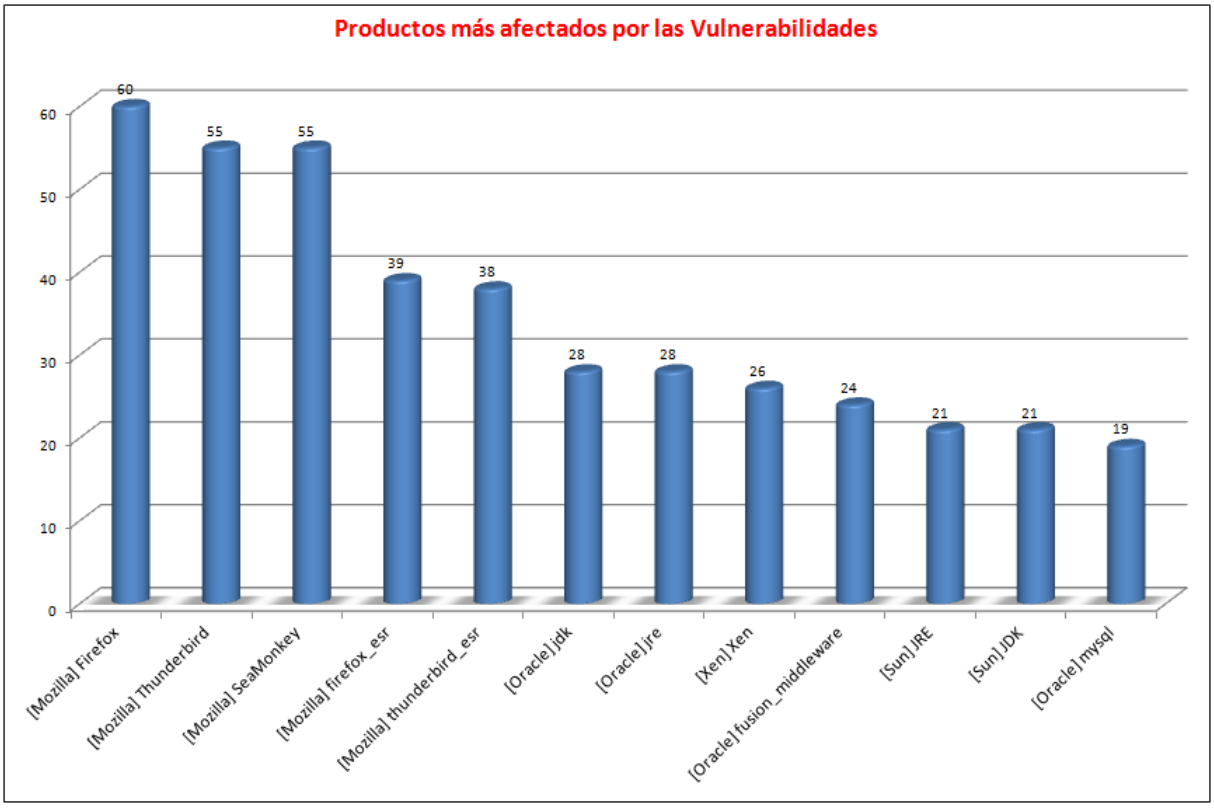

Figura 178: Productos más afectados por las últimas vulnerabilidades.

Este trimestre ha sido Mozilla Firefox el producto del que se han publicado más vulnerabilidades, seguido de Mozilla Thunderbird y de Mozilla SeaMonkey. Al final son las mismas vulnerabilidades para los 3 productos.

5.1.2. Fabricantes más afectados

La siguiente figura muestra los diez fabricantes más afectados por las vulnerabilidades detectadas en este trimestre.

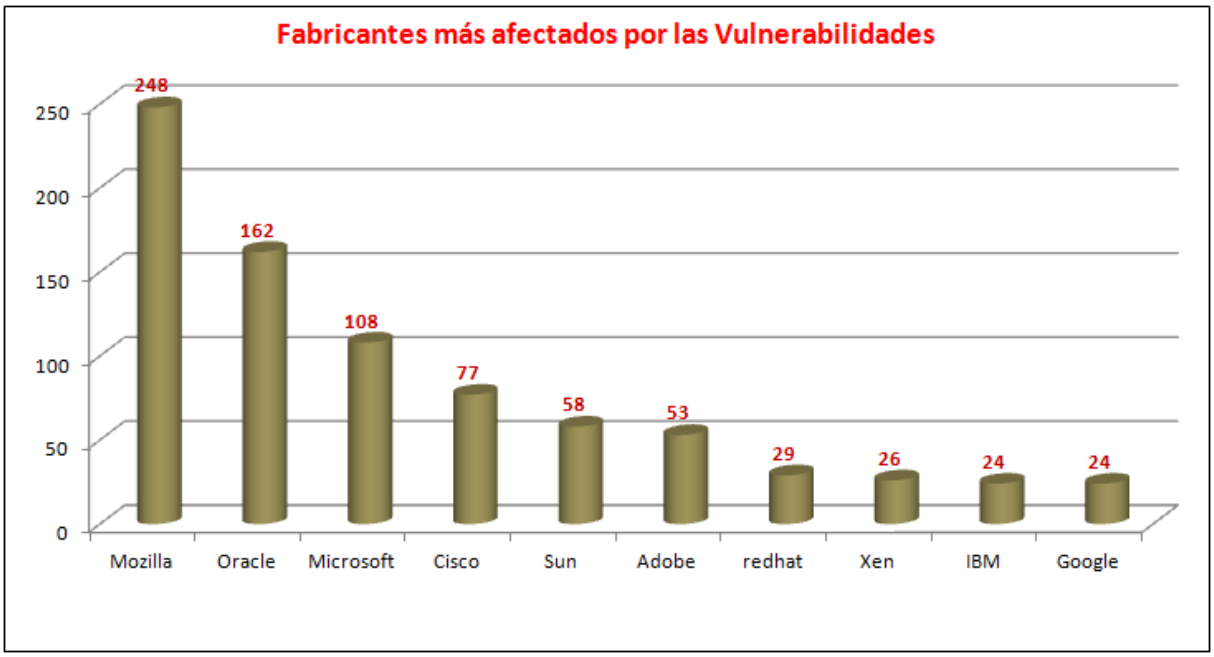

Figura 18: Fabricantes más afectados por las últimas vulnerabilidades.

5.1.3. 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 cuarto trimestre de 2012.

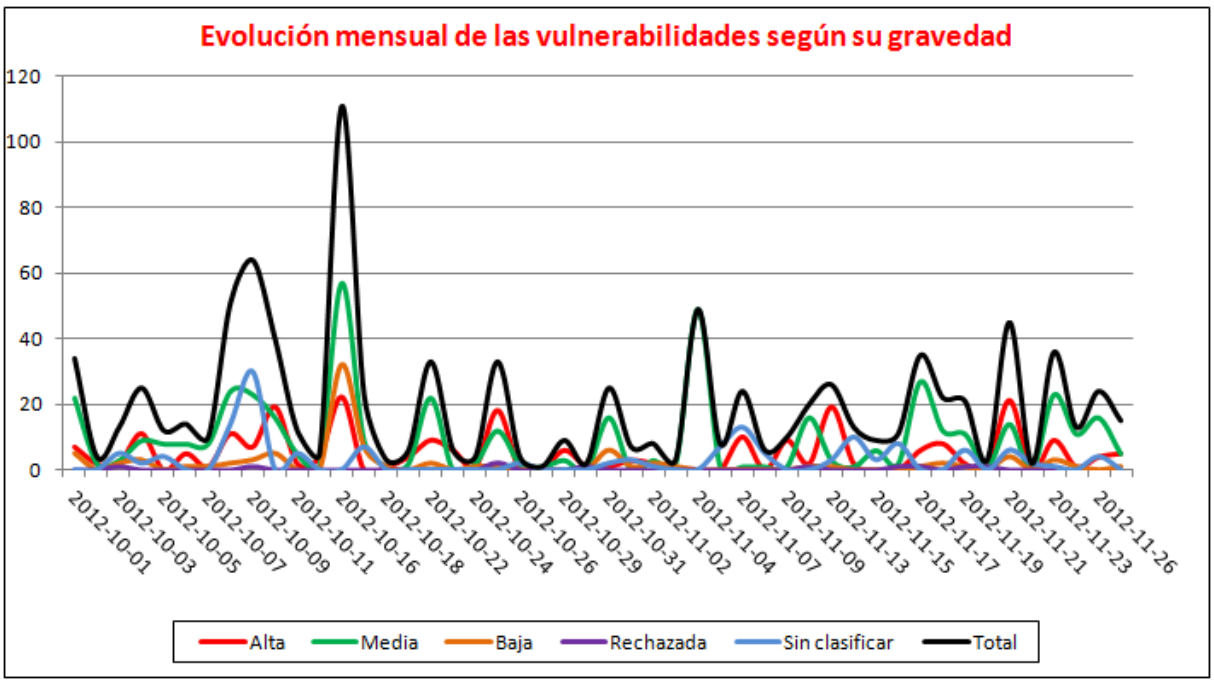

Figura 190: Vulnerabilidades emitidas por nivel de riesgo.

A lo largo del pasado trimestre se emitieron un total de **1259** vulnerabilidades. Los niveles de severidad de las vulnerabilidades publicadas aparecen en la figura anterior.

5.1.4. Vulnerabilidades más comunes según su tipo

El siguiente gráfico muestra los tipos de vulnerabilidades más comunes registradas este cuarto trimestre de 2012.

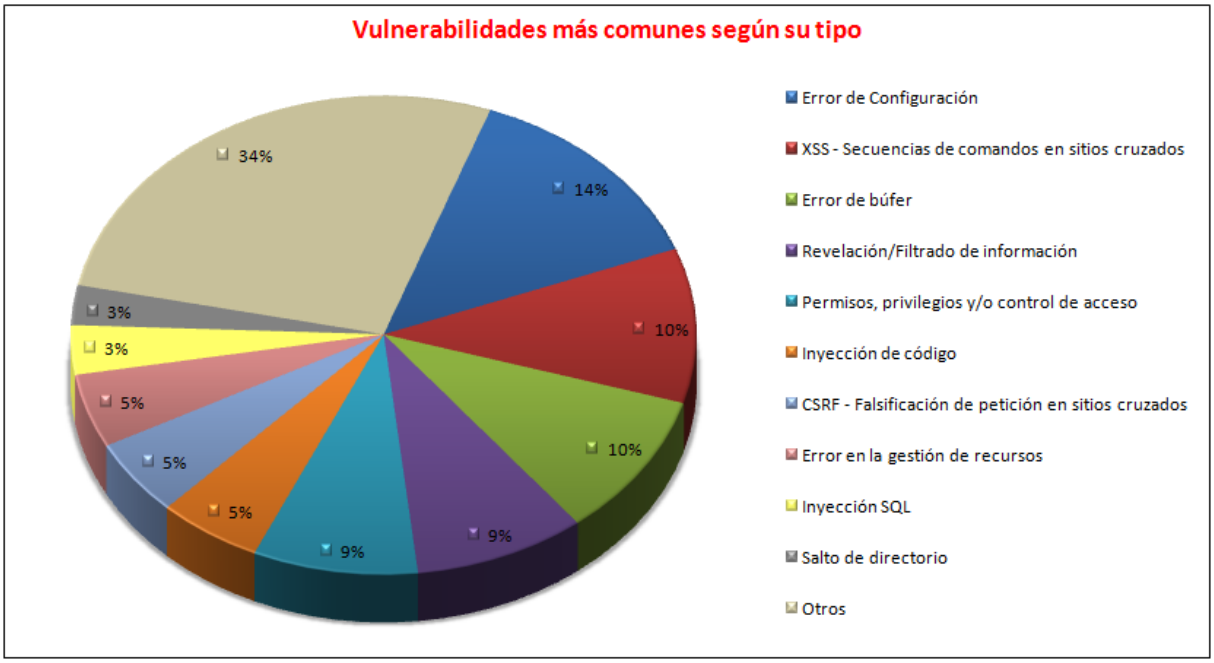

Figura 201: Vulnerabilidades más comunes por tipo.