INFORME MENSUAL

RED DE SENSORES DE INTECO

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

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 mes, 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 mes.

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

Por último, en el apartado con información de interés para esta red de sensores pero no relacionada con la información que reportan como son las vulnerabilidades y los eventos que se celebrarán los próximos dos meses.

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. 5052
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" está formada por **91 entidades** que albergan al menos un sensor y que están ubicados en diferentes sectores con el porcentaje de distribución que aparece en la figura.

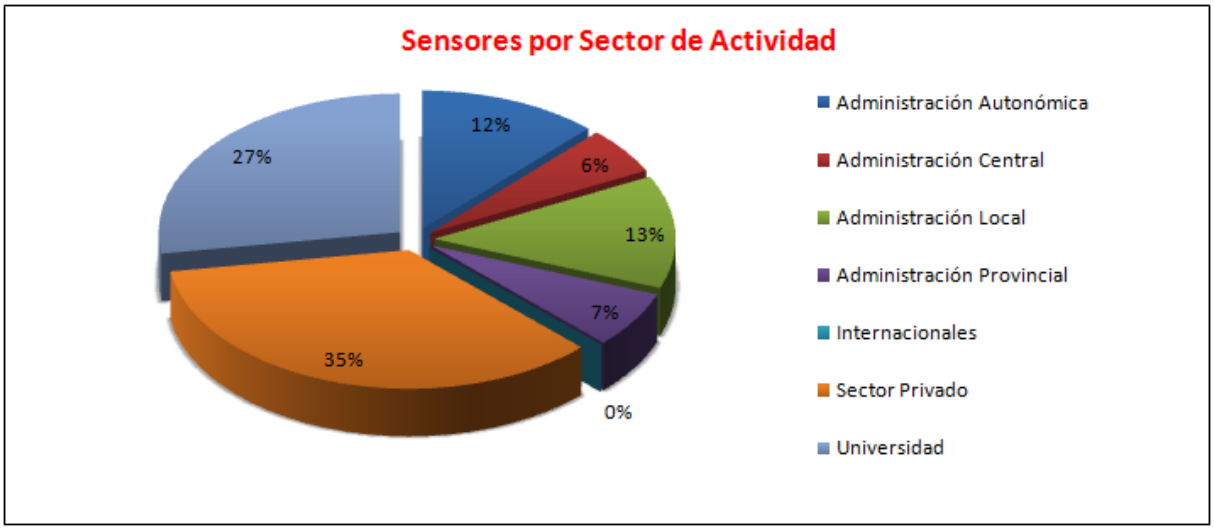

Figura 1: Distribución de los sensores por sector de actividad.

2.1. ACTIVIDAD DE LOS SENSORES

Como se puede ver, la actividad de los sensores se ha mantenido estable en los dos últimos meses. Se puede apreciar una gran diferencia del número de sensores este mes. Esto se debe a una reestructuración de la organización de los sensores, uniendo varios que procedían de la misma entidad.

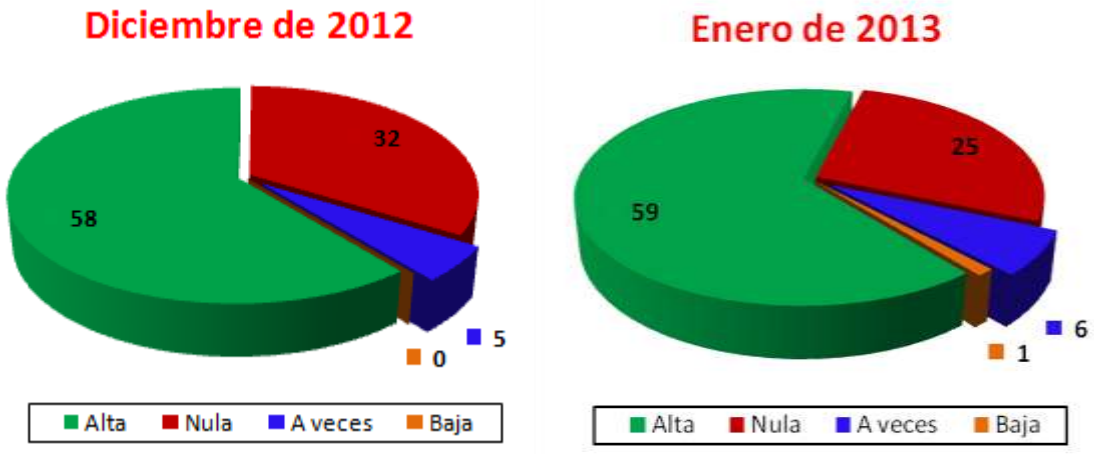

Figura 2: Distribución de sensores según frecuencia en el envío del informe.

3. DATOS DEL MES

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.

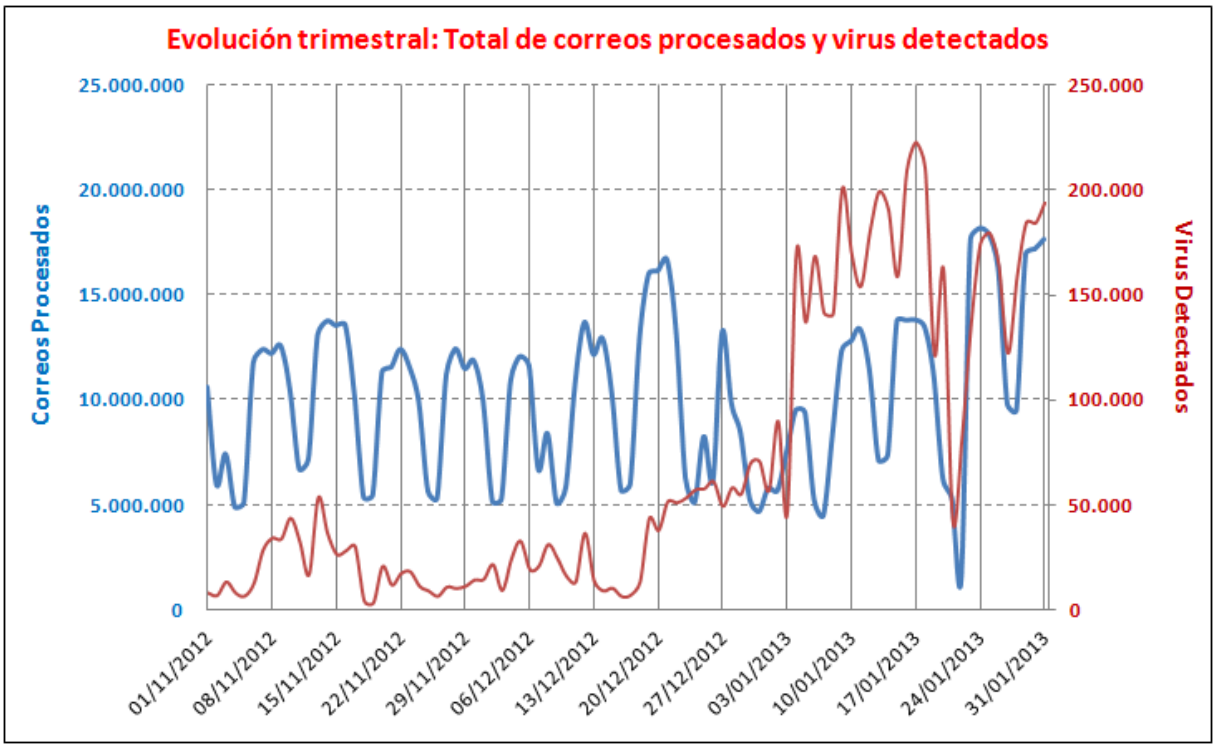

Figura 3: Evolución trimestral de correos procesados y virus detectados.

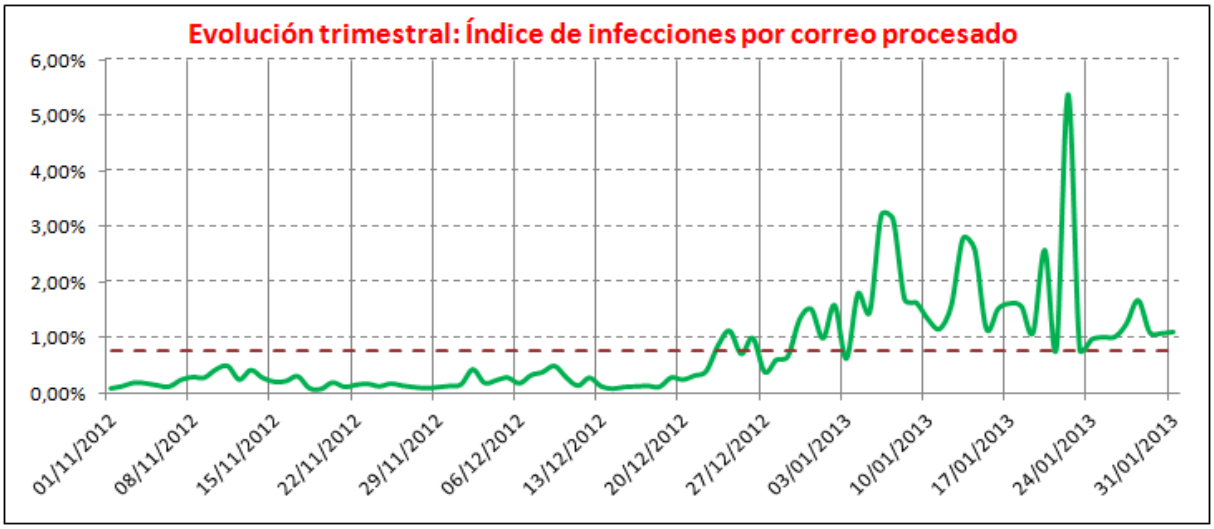

Figura 4: Evolución trimestral del índice de infecciones por correo procesado.

Como se puede ver en la figura 4, el porcentaje de correos infectados se encuentra en torno al **0,76%** de los correos recibidos (76 infecciones por cada 10000 correos).

Un detalle de la evolución del correo procesado y las detecciones registradas en el mes de Enero aparece en la siguiente figura:

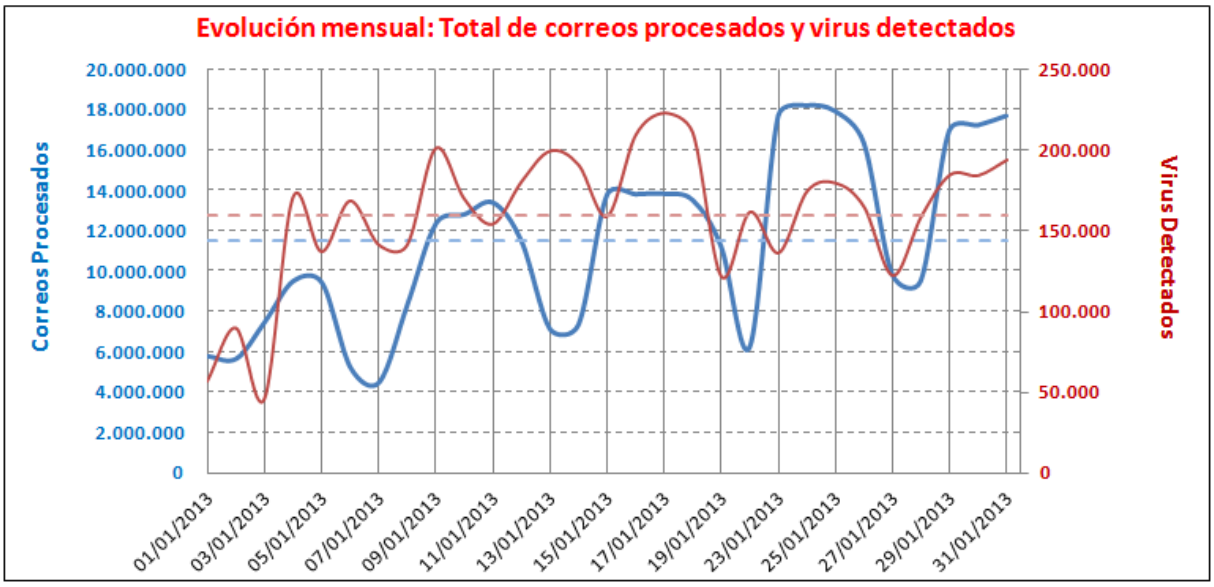

Figura 5: Evolución mensual de correos procesados y virus detectados.

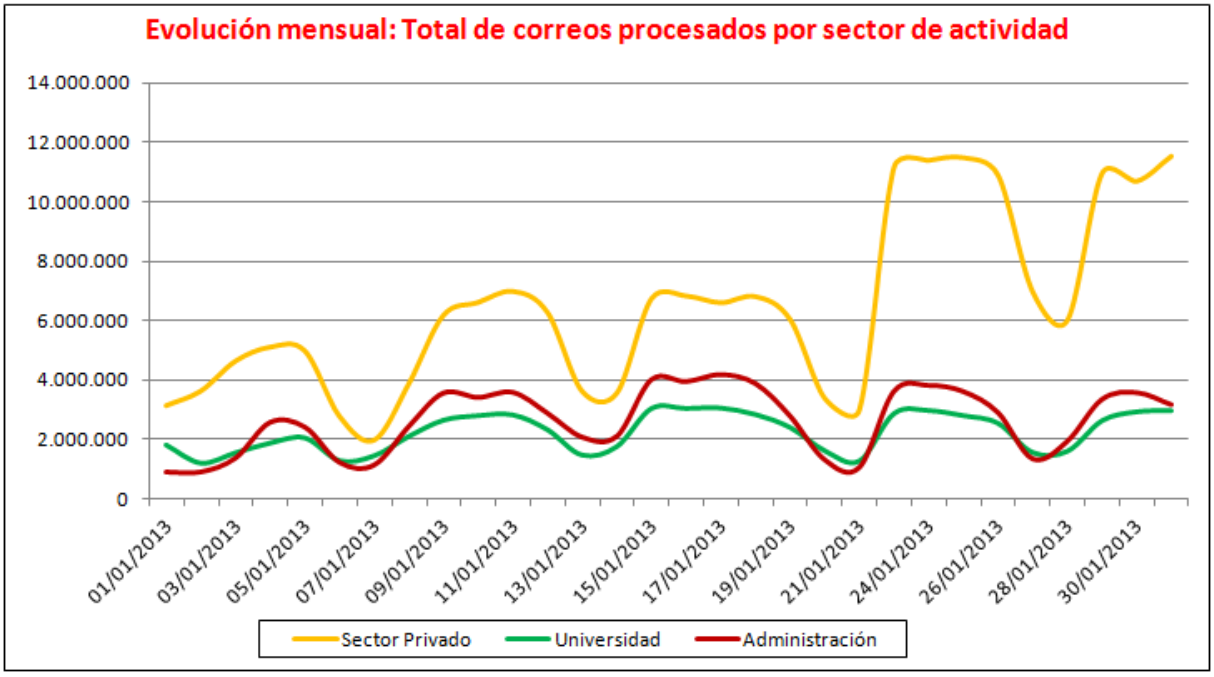

Figura 6: Evolución mensual de correos procesados por sector de actividad.

En figura 6 se muestra la aportación al volumen de correos procesados de los diferentes sectores de actividad durante el mes de Enero.

Puede apreciarse que el sector de actividad “Sector privado”, que constituye aproximadamente el 35% de los Sensores, es el sector que procesa más cantidad de mensajes (más del 50% del total de correos).

Esto es 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 proveedores de servicios de correo electrónico.

También se puede apreciar claramente en la gráfica la reducción del volumen de correos procesados en fines de semanas.

Además desde aproximadamente el 20 de Enero el volumen de tráfico de este sector ha aumentado considerablemente. La razón es la recuperación de un sensor que había dejado recientemente de enviar informes, Acens.

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 mes

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 mes de Enero.

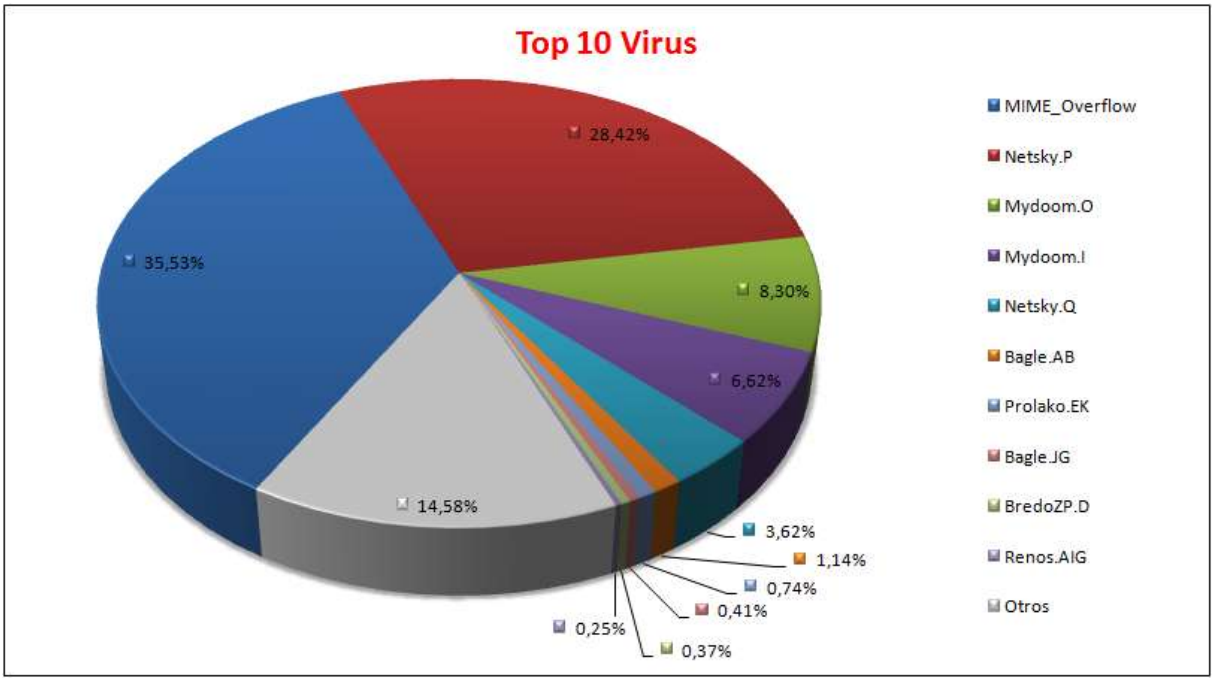

Figura 7: Virus más activos en la red de sensores durante el mes.

Este mes el virus más activo ha sido MIME_Overflow, con un 35,53% del total de virus detectados en la Red de Sensores. Le sigue *NetSky.P*, con un 28,42% y *MyDoom.O* con un 8,30%.

3.2.2. 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.

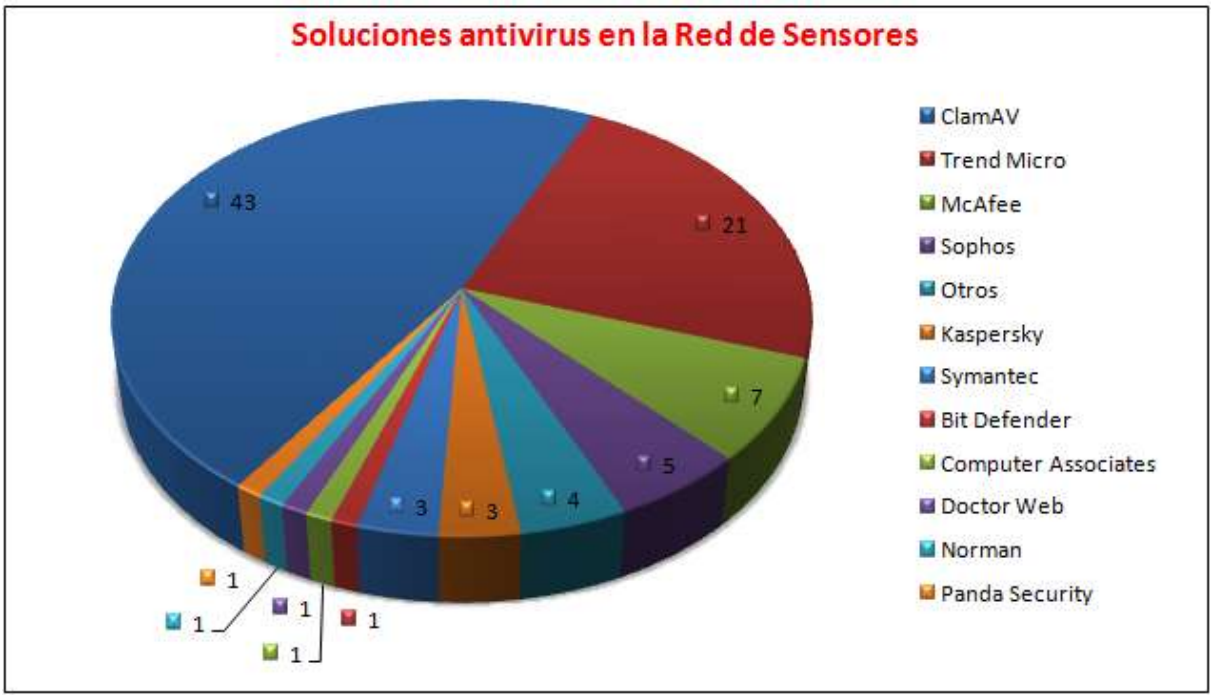

Figura 8: Antivirus utilizados en los sensores.

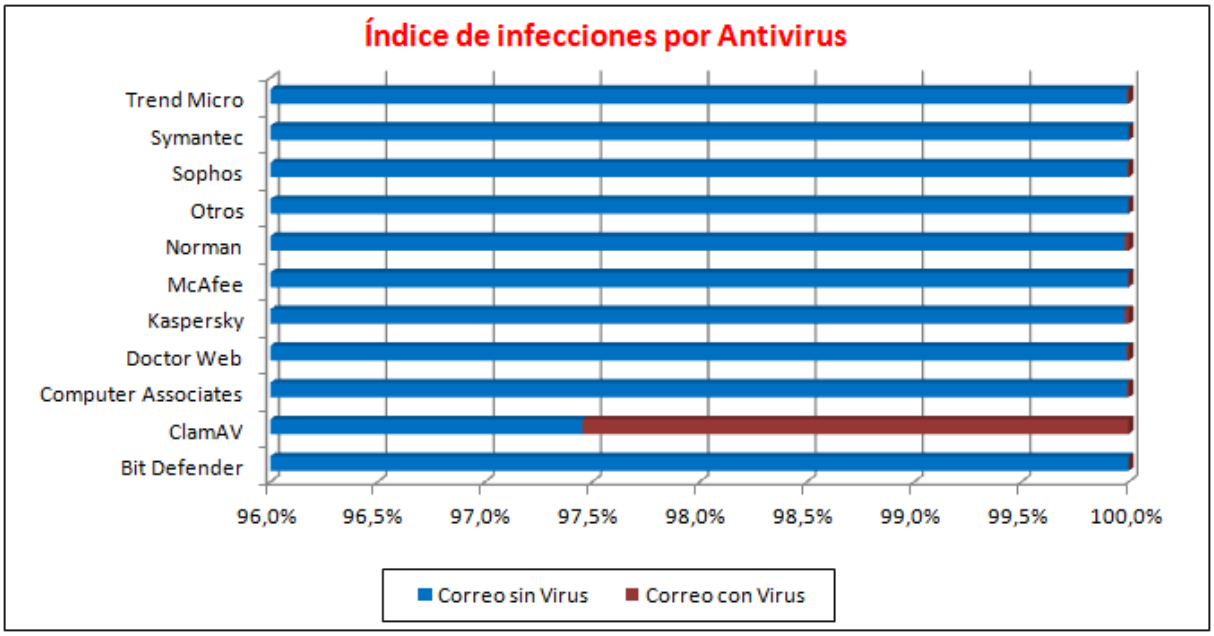

Figura 9: Relación correos analizados sin virus/correos con virus detectado por antivirus.

La Figura 9 muestra el porcentaje de detecciones sobre el volumen de correos procesados bajo cada una de las soluciones antivirus. Hay que tener en cuenta que el número de detecciones contabilizadas puede variar dependiendo tanto de la potencia del antivirus como por la presencia en la arquitectura de cada sensor de otros sistemas que, actuando como filtros previos, eliminen parte de los virus sin que éstos lleguen a contabilizarse.

3.2.3. 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.

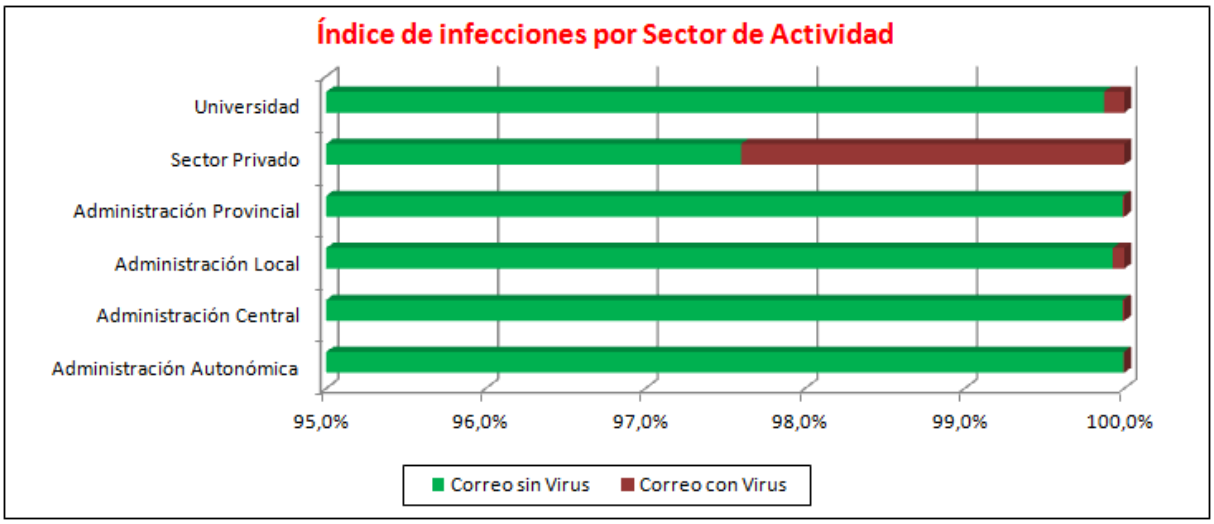

Figura 10: Porcentaje de correos sin virus frente a correos con virus detectados por sectores de actividad.

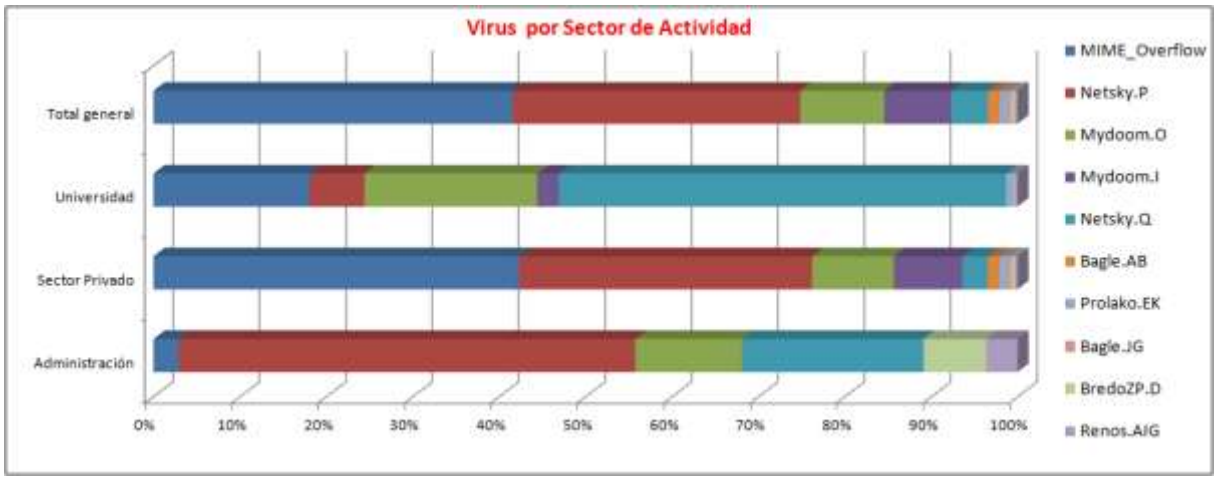

Figura 11: Top virus por sectores de actividad.

La Figura 11 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.

Como se puede ver el virus más activo es diferente según el tipo de sector de actividad, por ejemplo, en la administración el virus más activo fue *NetSky.P*. En el sector privado fue, sin embargo *MIME_Overflow*, mientras en las Universidades fue *NetSky.Q* el virus más generalizado.

Como información complementaria a la Figura 11, la siguiente tabla muestra los valores de virus más frecuentes.

Virus	Administración	Sector Privado	Universidad	Total general
MIME_Overflow	1,66%	**42,06%**	16,14%	41,1%
Netsky.P	**30,29%**	33,67%	5,65%	32,87%
Mydoom.O	7,05%	9,38%	17,83%	9,6%
Mydoom.I	0%	7,87%	2,23%	7,66%
Netsky.Q	12,03%	2,92%	**46,14%**	4,19%
Bagle.AB	0%	1,36%	0%	1,31%
Prolako.EK	0%	0,86%	0,76%	0,86%
Bagle.JG	0%	0,49%	0,08%	0,48%
BredoZP.D	4,15%	0,42%	0,13%	0,43%
Renos.AIG	2,07%	0,28%	0,21%	0,29%
Otros	42,74%	0,68%	10,83%	1,21%

Figura 12: Tabla de virus más detectados por sectores.

3.2.4. 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 del mes, la figura presenta el mapa calculado sobre los datos recibidos durante el mes de Enero.

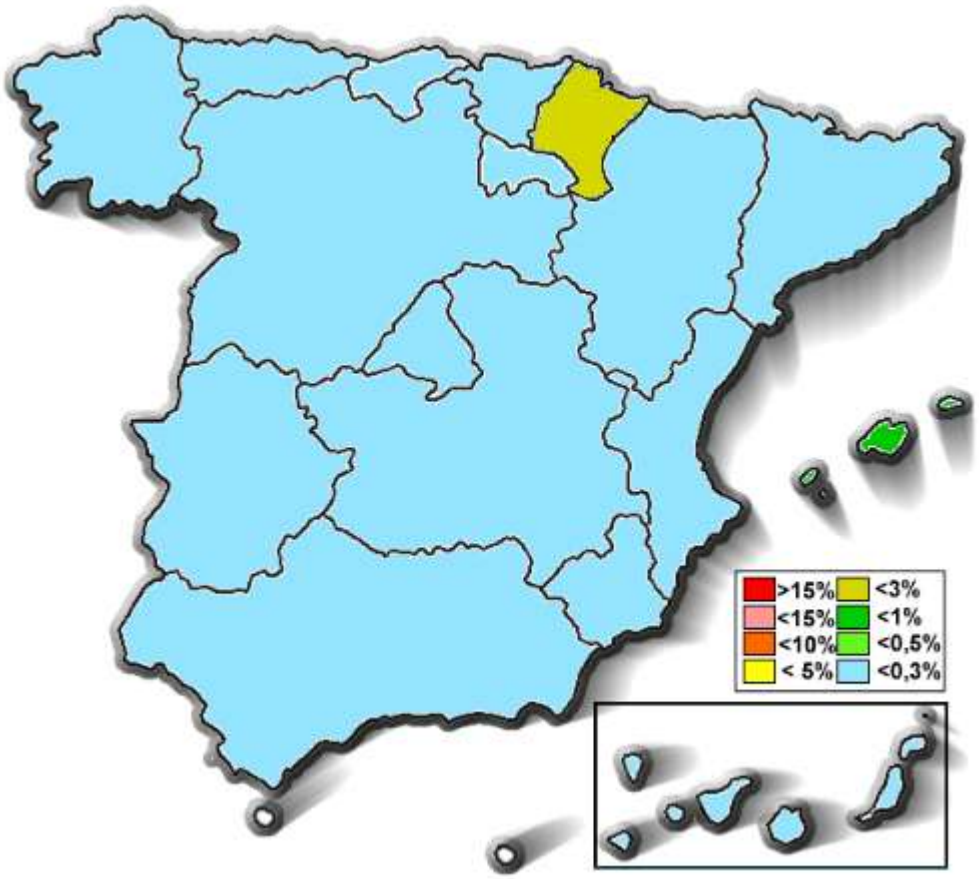

Figura 13: Mapa autonómico de detecciones de virus.

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 del pasado mes.

Comunidad autónoma	Muestra CCAA	Incidencias
Andalucía	29.030.062	0,0%
Aragón	16.995.607	0,03%
Canarias	1.540.355	0,0%
Cantabria	0	0,0%
Castilla y León	881.841	0,0%
Castilla-La Mancha	14.995.001	0,0%
Catalunya / Cataluña	32.376.882	0,22%
Ciudad Autónoma de Ceuta	0	0,0%
Ciudad Autónoma de Melilla	0	0,0%
Comunidad Foral de Navarra	4.616.622	2,02%
Comunidad de Madrid	11.953.054	0,0%
Comunitat Valenciana / Comunidad Valenciana	46.512.961	0,05%
Euskadi / País Vasco	1.306.568	0,0%
Extremadura	313.008	0,0%
Galicia / Galicia	14.379.545	0,03%
Illes Balears / Islas Baleares	178.952	0,03%
La Rioja	0	0,0%
Principado de Asturias	39.058.220	0,0%
Región de Murcia	3.819.381	0,0%

Muestra CCAA es el número de mensajes de correo electrónico analizados por los sensores de esa CCAA.

Incidencias es el número de estos mensajes en los que se ha detectado algún virus.

Figura 14: Sensores, correo y porcentaje de infección detectada por autonomía.

Como se puede ver, durante el pasado mes de Enero, fue la **Comunitat Valenciana** la que más muestras aportó a la red de Sensores. Sin embargo la comunidad con un porcentaje de correo infectado más alto (2,02%) fue **Navarra**, que también fue la comunidad con un número total de infecciones más alto (unas 93.000).

3.3. 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 recogida en los ficheros de registro (“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/

3.3.1. Nivel de SPAM del mes

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

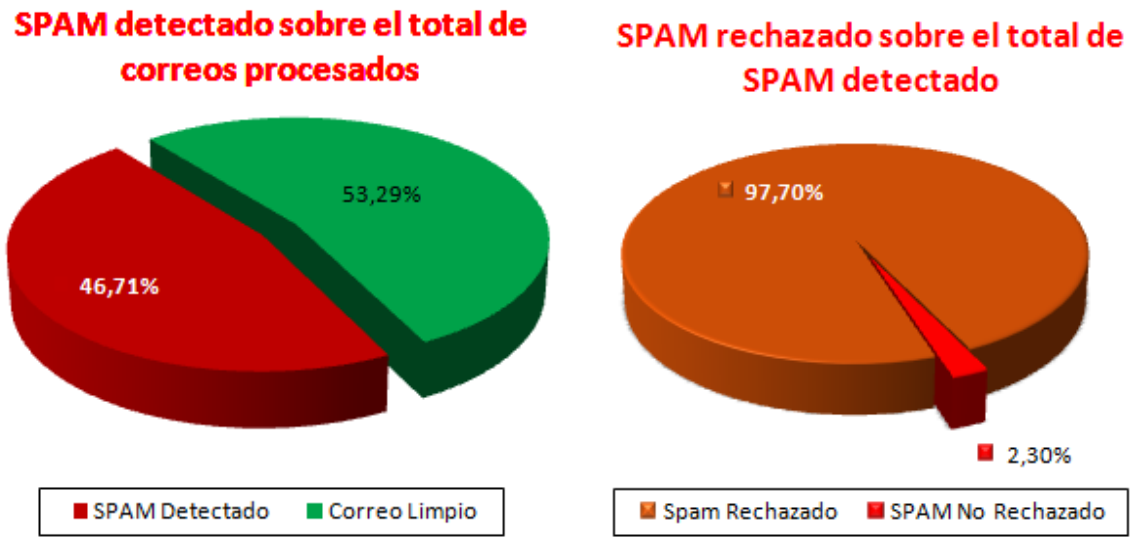

Figura 15: Nivel de SPAM detectado por la red de sensores.

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.

Durante el pasado mes de Enero, el nivel de SPAM en correo fue de un **46,71%** del número total de correos procesados. 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).

3.3.2. Evolución temporal de totales

La siguiente figura muestra la evolución del SPAM a lo largo del pasado mes. Son los datos de mensajes procesados, detectados y rechazados a lo largo del pasado mes de Enero. Como se puede ver las líneas roja y azul se solapan puesto que la práctica totalidad del SPAM detectado es rechazado por las aplicaciones antispam.

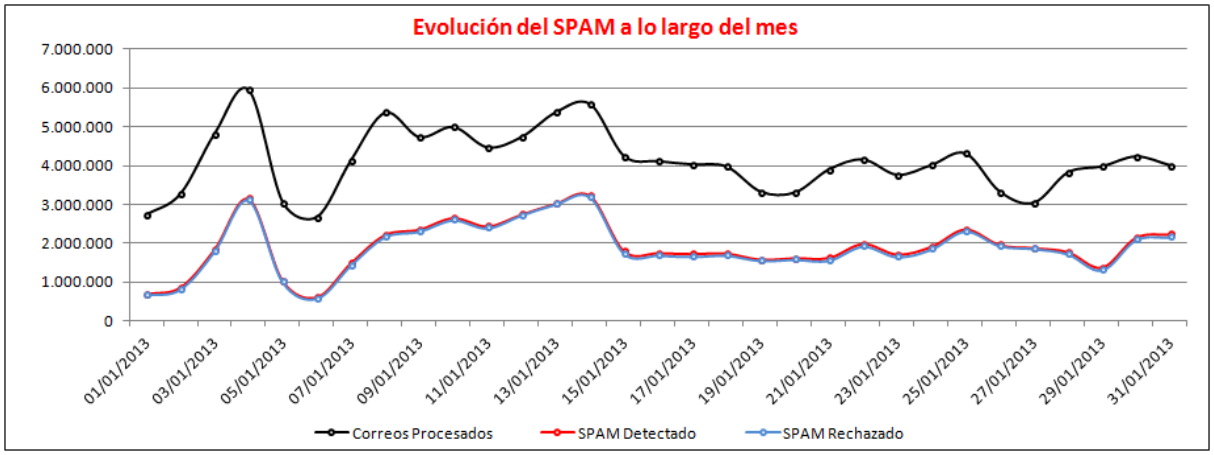

Figura 16: Evolución temporal del SPAM detectado por la red de sensores.

3.3.3. Evolución mensual del SPAM

La siguiente figura muestra la evolución del nivel de SPAM detectado por la Red de Sensores en los últimos 10 meses. La línea azul muestra el porcentaje de SPAM detectado en correo y se mide con el eje de la derecha. Este mes se ve un cambio de tendencia, tras 9 meses de descenso del nivel de SPAM este mes volvemos a ver una importante subida.

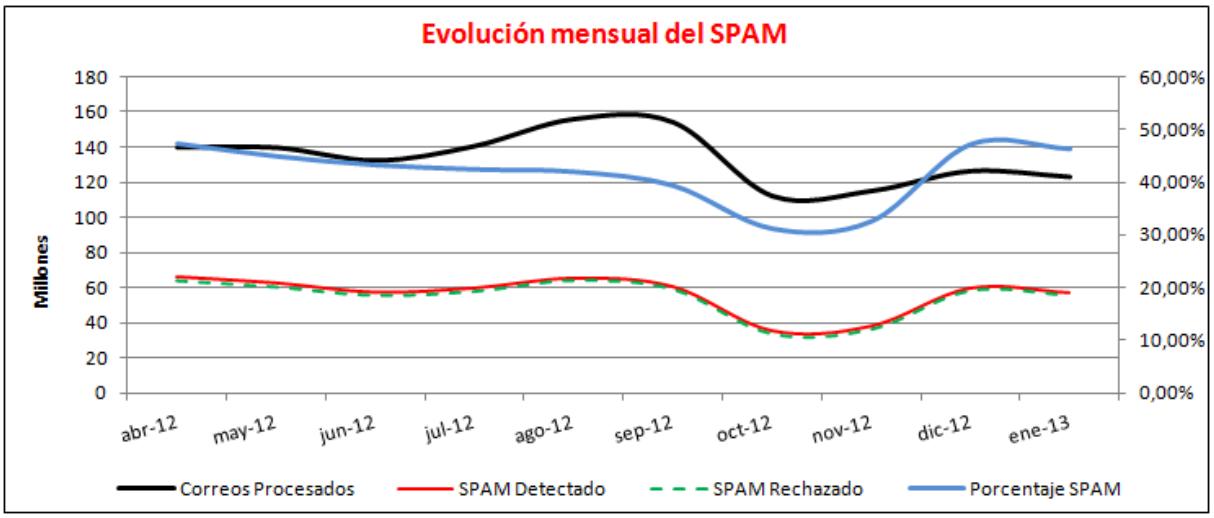

Figura 17: Evolución mensual del SPAM a lo largo del año.

3.3.4. Top 10 de países emisores de SPAM

La figura muestra los países emisores de SPAM. La información se muestra sesgada como SPAM rechazado, SPAM detectado y correos procesados.

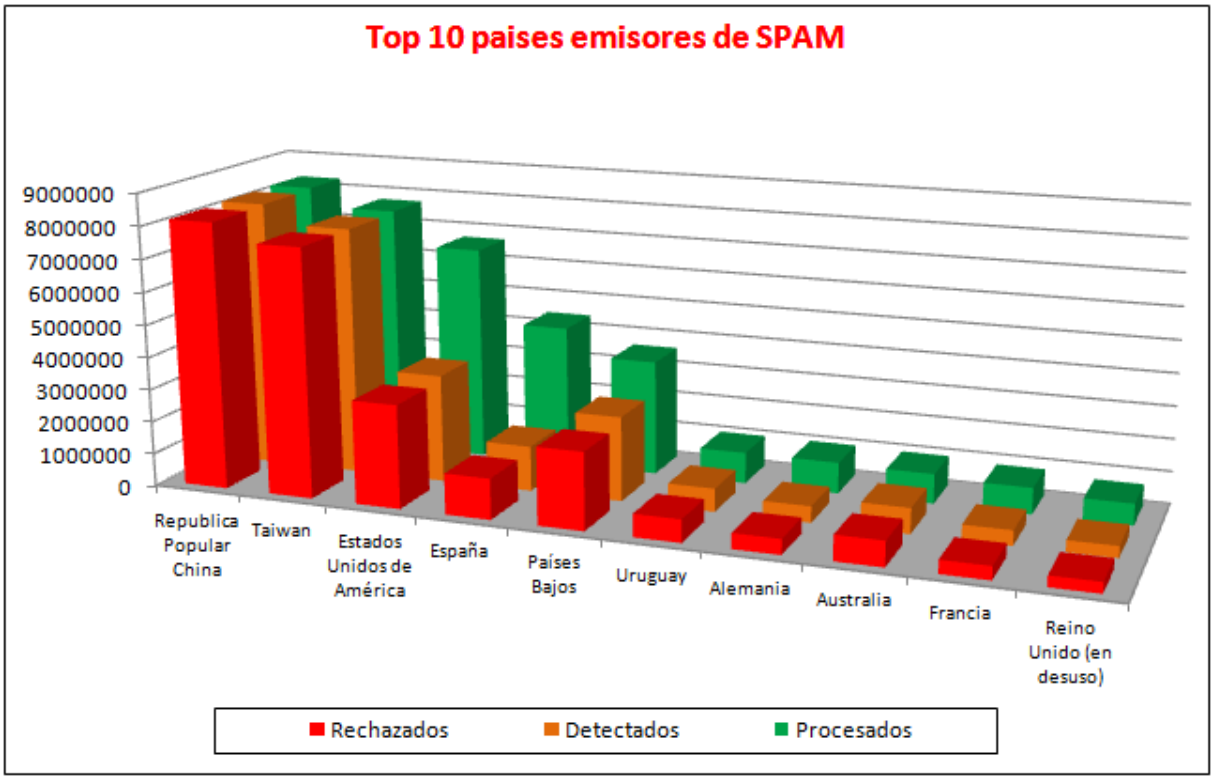

Figura 18: Top 10 países emisores de SPAM según datos recogidos por la RSI.

Se puede comprobar que, a lo largo del último mes, los países que más SPAM han mandado a direcciones de correo españolas han sido **China** y **Taiwan**. Además cabe mencionar que más del 99% de los correos que proceden de estos países son SPAM.

4. NO SOLO SENSORES

4.1. VULNERABILIDADES

4.1.1. 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 mes de Enero.

A lo largo del pasado mes se emitieron un total de **443** vulnerabilidades, con un nivel de severidad mayoritariamente **medio y alto**. Los niveles de severidad de las vulnerabilidades publicadas aparecen en la siguiente figura.

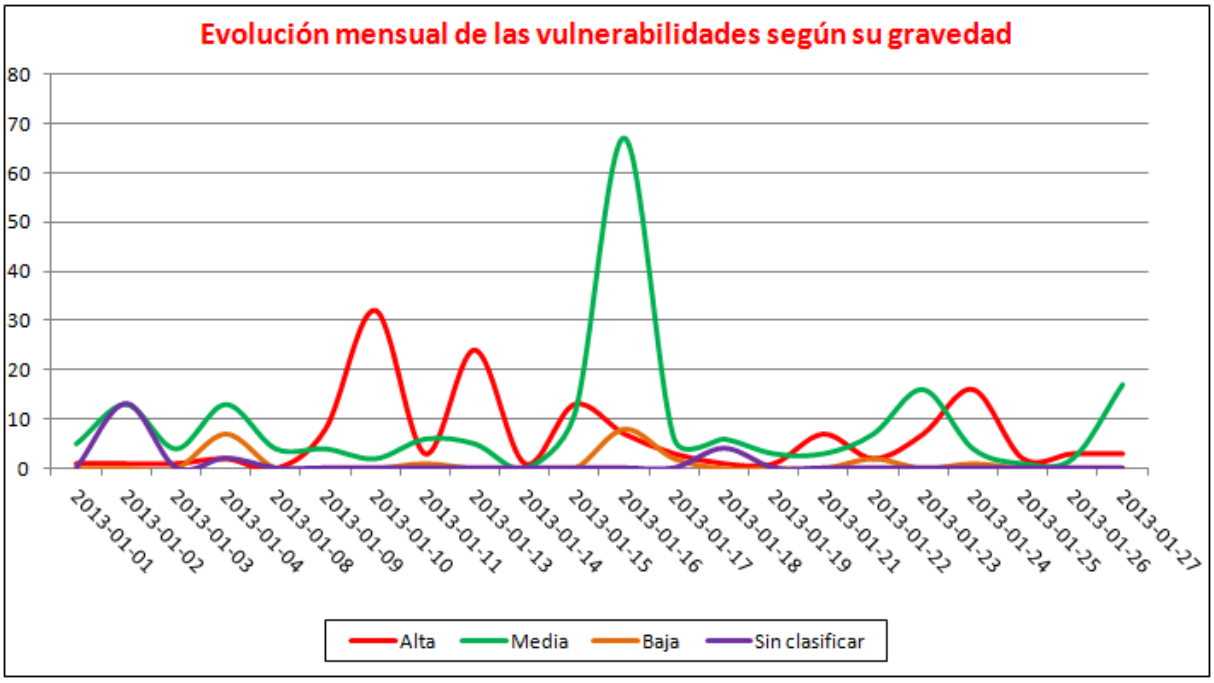

Figura 19: Vulnerabilidades emitidas por nivel de riesgo.

4.1.2. Productos más afectados

La figura muestra los productos más afectados por las vulnerabilidades del último mes. Nótese que sólo aparecen aquellos productos afectados por **diez** o más nuevas vulnerabilidades. Entre paréntesis aparece el fabricante.

Figura 20: Productos más afectados por las últimas vulnerabilidades.

4.1.3. Fabricantes más afectados

La figura muestra los diez fabricantes más afectados por las vulnerabilidades detectadas en el mes de Enero.

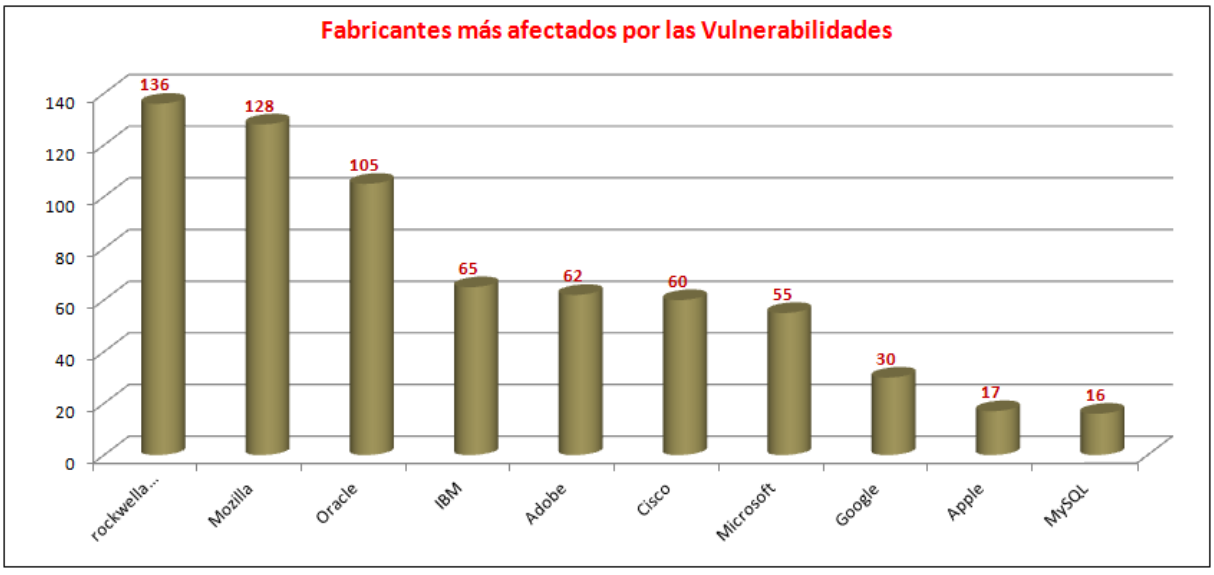

Figura 21: Fabricantes más afectados por las últimas vulnerabilidades.

4.1.4. Vulnerabilidades más comunes según su tipo

El siguiente gráfico muestra los tipos de vulnerabilidades más comunes registradas en el mes de Enero. Cabe mencionar que una misma vulnerabilidad puede ser considerada de diferentes tipos.

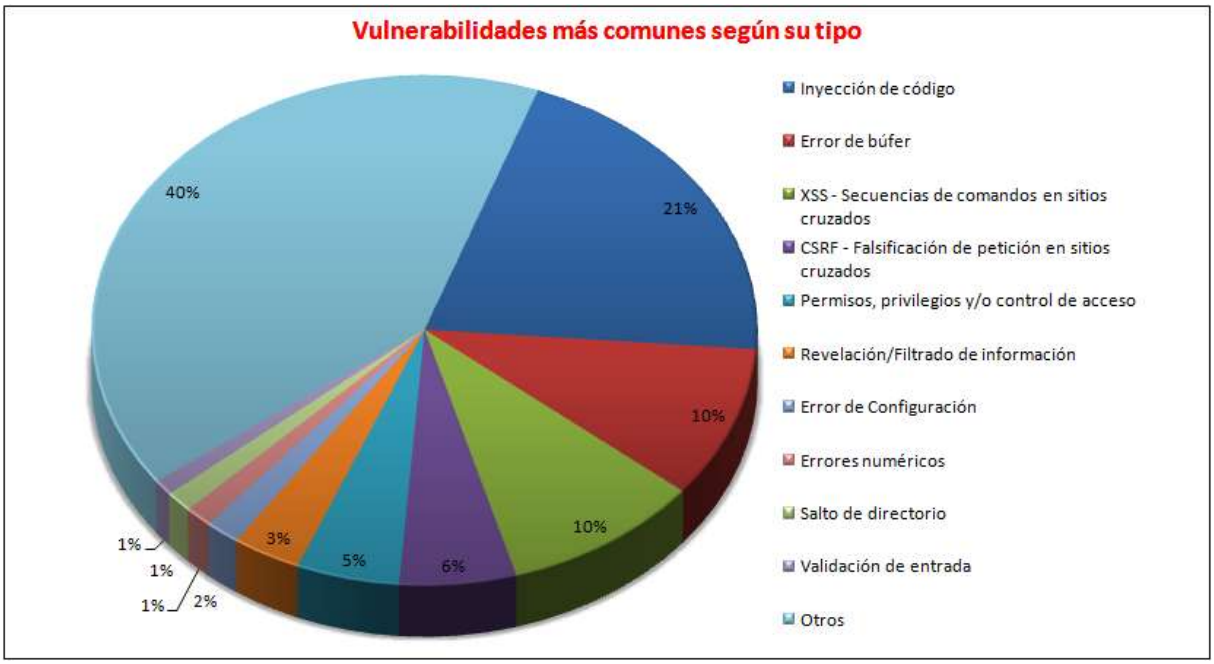

Figura 22: Vulnerabilidades más comunes por tipo

4.2. FRAUDE ELECTRÓNICO

4.2.1. Número total de incidentes de fraude

La siguiente figura muestra el número total de incidentes de fraude registrados en el Repositorio de Fraude de INTECO-CERT a lo largo del último año.

Los datos de incidentes de fraude tratados por INTECO-CERT a lo largo del último año son:

Mes	Incidentes de Fraude	Mes	Incidentes de Fraude
Febrero 2012	518	**Agosto 2012**	874
Marzo 2012	732	**Septiembre 2012**	969
Abril 2012	618	**Octubre 2012**	841
Mayo 2012	723	**Noviembre 2012**	670

Junio 2012	1002	**Diciembre 2012**	846
Julio 2012	723	**Enero 2013**	941

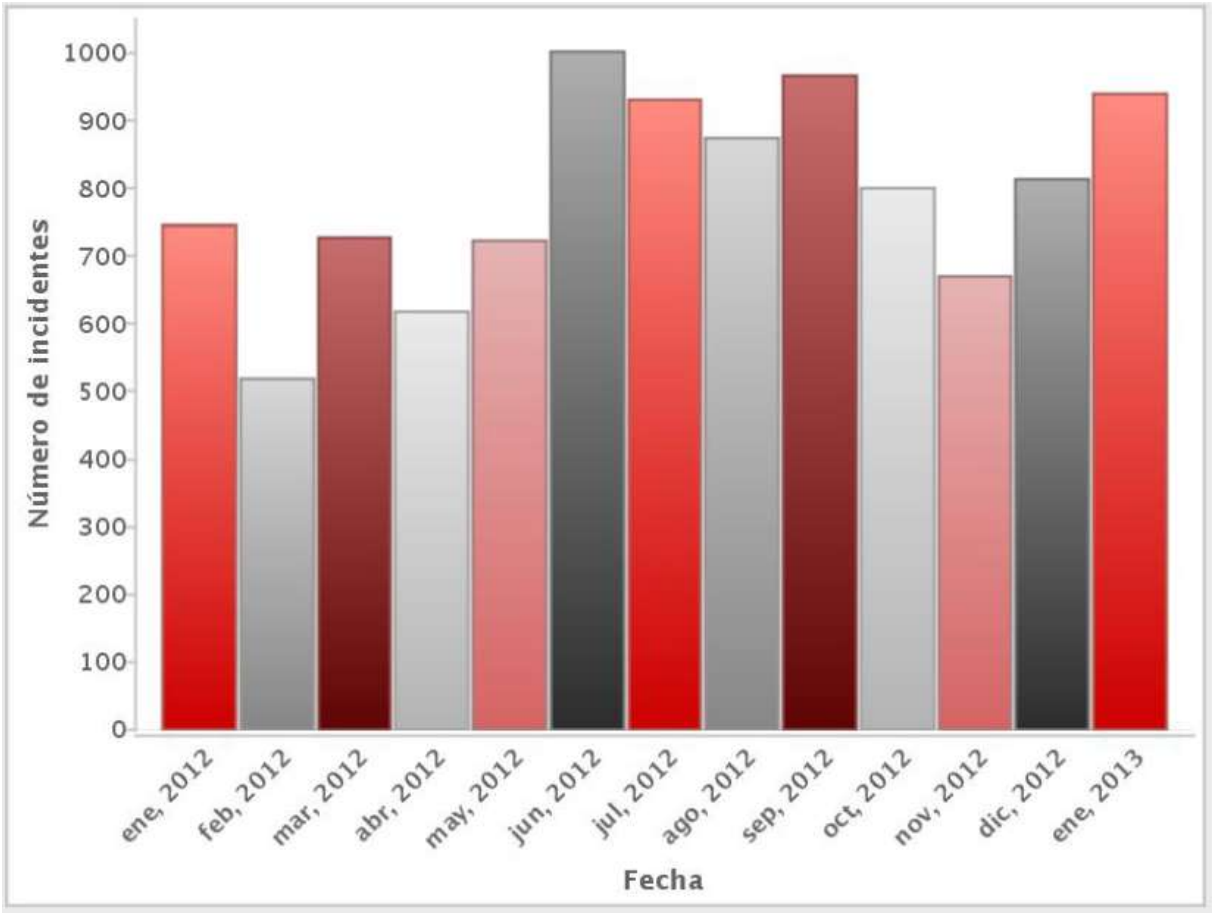

Figura 23: Evolución del número de incidentes de Fraude.

4.2.2. Número total de URLs fraudulentas

La siguiente figura revela la evolución del número de URLs con contenido fraudulento registradas en el Repositorio de Fraude de INTECO-CERT a lo largo del último año.

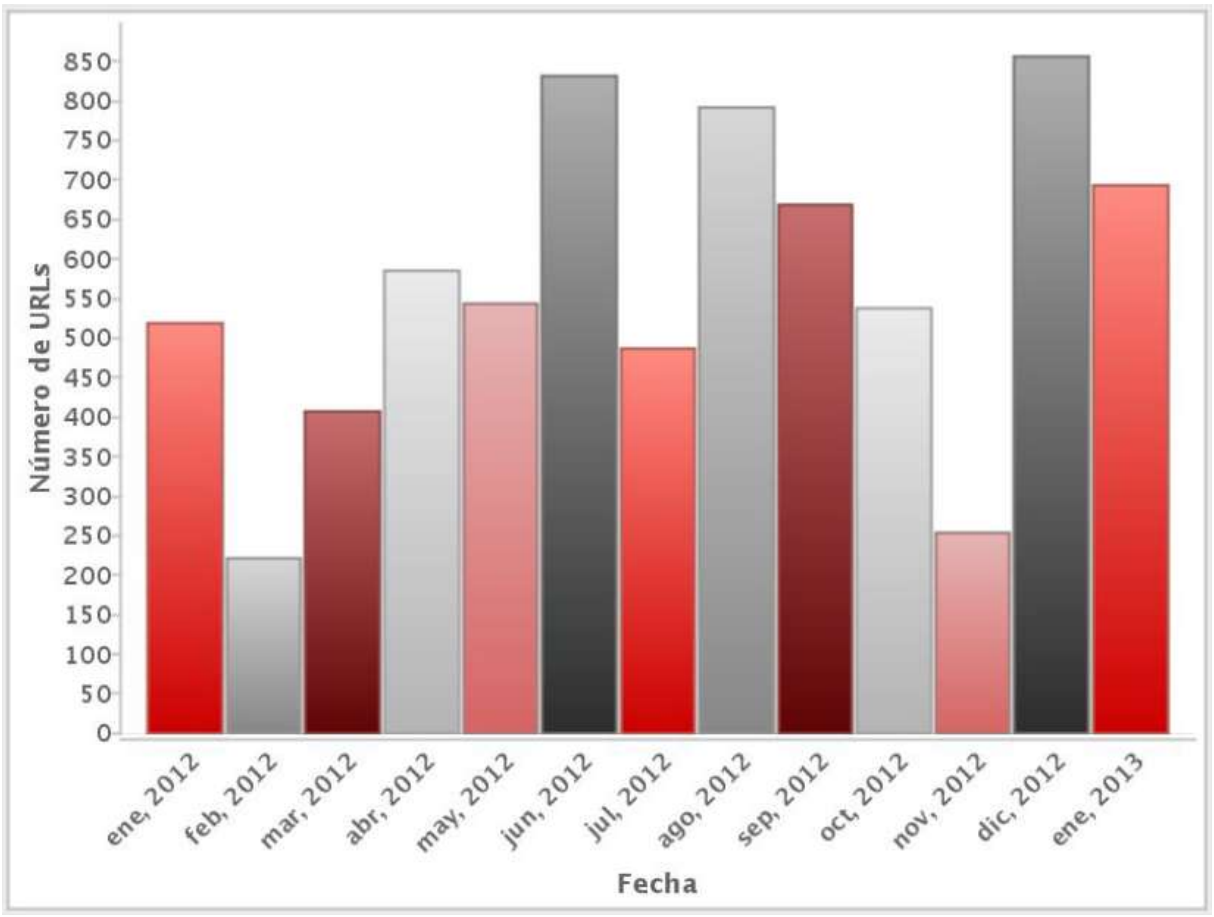

Figura 24: Evolución del número de URLs fraudulentas.

A continuación se muestra una tabla con los valores de la gráfica anterior:

Mes	URLs fraudulentas	Mes	URLs fraudulentas
Febrero 2012	221	**Agosto 2012**	793
Marzo 2012	403	**Septiembre 2012**	666
Abril 2012	585	**Octubre 2012**	536
Mayo 2012	541	**Noviembre 2012**	253
Junio 2012	831	**Diciembre 2012**	856
Julio 2012	542	**Enero 2013**	693

4.3. AVISOS TECNICOS Y NO TÉCNICOS PUBLICADOS

A lo largo del mes de Enero, INTECO publicó los siguientes avisos de seguridad:

Aviso de Seguridad	Fecha
Boletines de seguridad de Microsoft de enero 2013 https://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/boletines_seguridad_microsoft_enero_2013_20130109_1	09/01/2013
Vulnerabilidad 0-day en el correo web de Yahoo! https://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/vulnerabilidad_0day_correo_web_yahoo_20130109	09/01/2013
Vulnerabilidad 0-day en Java https://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/vulnerabilidad_0day_java_20130111	11/01/2013
Parche para la vulnerabilidad 0-day en Java 7 https://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/parche_vulnerabilidad_java_0day_20130114	14/01/2013
Actualización de PHP a las versiones 5.4.11 y 5.3.21 https://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/actualizacion_php_versiones_5411_5321_20130118	18/01/2013
Actualización de seguridad de Wordpress para versiones anteriores a 3.5.1 https://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/actualizacion_seguridad_wordpress_versiones_anteriores_351_20130126	26/01/2013
Vulnerabilidades críticas en el protocolo UPnP https://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/vulnerabilidades_criticas_protocolo_upnp_20130131	31/01/2013

4.4. EVENTOS DEL MES (FEBRERO Y MARZO 2013)

4.4.1. Primera Conferencia Internacional en Computación verde, Tecnología e Innovación

En el evento se debatirán cuestiones relacionadas con, entre otras: smart grids y microgrids, sistemas distribuidos de ahorro de energía de alta escala, como grids, clouds y servicios de computación, análisis del ciclo de vida de los equipamientos IT, sistemas de ahorro de energía en computación, etc.

- Fecha: 04 al 06 de Marzo de 2013
- Lugar: Kuala Lumpur, Malasia
- Precio: 550 dólares
- Más información: http://sdiwc.net/conferences/2013/Malaysia4/

4.4.2. IX Ciclo de Conferencias UPM TASSI: Ciberdefensa

Nueva conferencia del IX ciclo de conferencias de la UPM. En este caso se hablará de la Ciberdefensa y la ciberseguridad, que son un tema estratégico para cualquier país. El ponente será Juan Carlos Batanero.

- Fecha: 6 de Marzo de 2013
- Lugar: Sala de Grados 3005 EUITT, UPM
- Precio: Gratuito
- Más información: http://www.lpsi.eui.upm.es/GANLESI/GANLESI.htm

4.4.3. HOMSEC 2013

HOMSEC, el Salón Internacional de Tecnologías de Seguridad y Defensa llega a su cuarta edición en 2013 consolidado como la principal plataforma expositiva y profesional en España para los sectores de Seguridad y Defensa. Gracias a ello, es punto de contacto de las Administraciones, las empresas y los centros de I+D+i, presentando necesidades y ofertando soluciones. También es plataforma de negocios y colaboración de las empresas fabricantes y suministradoras de productos, sistemas y servicios frente a los responsables de administraciones públicas, fuerzas armadas y cuerpos de seguridad del estado tanto nacionales como extranjeros. Y por último es punto de encuentro de las empresas españolas y europeas del sector con los países iberoamericanos, África y Asia.

Esta 4ª edición superará tanto la participación de visitantes como el número de expositores de pasadas ediciones, e incorporará nuevas actividades complementarias del salón: Business Point, II Congreso Internacional Atenea, HOMSEC Innova, Espacio para la Simulación, Presentaciones de Empresas y un amplio programa de contenidos en sus diferentes ciclos de conferencias.

- Fecha: 12 al 15 de Marzo de 2013
- Lugar: Feria de Madrid / Pabellón 7
- Precio: Consultar
- Más información: http://www.homsec.es/

4.4.4. IADIS International Conference: eSociety 2013

Este congreso trata de abarcar tanto los aspectos técnicos como los no técnicos de la Sociedad de la Información. Se tratarán aspectos como eBusiness, eCommerce, eLearning, nuevos medios y eSociety, servicios digitales en la eSociedad, etc.

- Fecha: 13 al 16 de Marzo de 2013
- Lugar: Lisboa, Portugal
- Precio: 460-670€
- Más información: http://www.esociety-conf.org/

4.4.5. XI Seminario Iberoamericano de Seguridad de las Tecnologías de la Información

El evento pretende ser un debate científico y tecnológico y la exposición de proyectos e iniciativas relacionadas con las principales temáticas convocadas en cada uno de los eventos que forman parte de la convención y de la feria.

- Fecha: 18 al 22 de Marzo de 2013
- Lugar: La Habana, Cuba
- Precio: Consultar
- Más información: http://www.informaticahabana.cu/es/inicio

4.4.6. IX Ciclo de Conferencias UPM TASSI: Ciberdelincuencia

Nueva conferencia del IX ciclo de conferencias de la UPM. En este caso se hablará de la Ciberdelincuencia, que es uno de los ámbitos delicitivos de más rápido crecimiento. El ponente ser Oscar de la Cruz.

- Fecha: 20 de Marzo de 2013
- Lugar: Sala de Grados 3005 EUITT, UPM
- Precio: Gratuito
- Más información: http://www.lpsi.eui.upm.es/GANLESI/GANLESI.htm

4.4.7. EvoRisk

Evorisk son 5 conferencias simultáneas que se realizan cada primavera y que representan la continuidad en la investigación en temas como la inteligencia computacional para la gestión del riesgo, seguridad y aplicaciones de defensa.

- Fecha: 3-5 de Abril de 2013
- Lugar: Viena, Austria
- Precio: Consultar
- Más información: http://www.evostar.org

4.4.8. IX Ciclo de Conferencias UPM TASSI: Gobernando la seguridad hacia los objetivos corporativos

Nueva conferencia del IX ciclo de conferencias de la UPM. En este caso se hablará de la e-governance, y su adecuación a los objetivos de la empresa. El ponente será Antonio Ramos.

- Fecha: 3 de Abril de 2013
- Lugar: Sala de Grados 3005 EUITT, UPM
- Precio: Gratuito
- Más información: http://www.lpsi.eui.upm.es/GANLESI/GANLESI.htm

4.4.9. European Round 2013

Dirigido a estudiantes de grado, máster y doctorado de países europeas con el lema “Ciberseguridad para la siguiente generación”.

- Fecha: 4 al 6 de Abril de 2013

- Lugar: RWTH Aachen University, Aachen, Alemania
- Precio: Consultar
- Más información: http://www.kaspersky.com/about/events/educational-events/European_Round_2013

4.4.10. 3rd Annual Cyber Security Summit

El objetivo del congreso es analizar las estrategias prioritarias, los factores de riesgo potenciales y amenazas.

- Fecha: 11 y 12 de Abril de 2013
- Lugar: Praga, República Checa
- Precio: 300-1600€
- Más información: http://ebcg.biz/ebcg-business-events/15/3rd-annual-cyber-security-summit/

4.4.11. Security Forum

Foro internacional dirigido al sector de la seguridad que pretende estimular el intercambio de conocimiento y el networking con exposición de productos, servicios y debate.

- Fecha: 17 y 18 de Abril de 2013
- Lugar: Centro de Convenciones Internacional de Barcelona
- Precio: 290-340€
- Más información: http://www.securityforum.es

4.4.12. IX Ciclo de Conferencias UPM TASSI: Seguridad en sistemas: explotando vulnerabilidades

Nueva conferencia del IX ciclo de conferencias de la UPM. En este caso se hablará de la explotación de vulnerabilidades. El ponente será Alejandro Ramos, de securitybydefault.

- Fecha: 17 de Abril de 2013
- Lugar: Sala de Grados 3005 EUITT, UPM
- Precio: Gratuito
- Más información: http://www.lpsi.eui.upm.es/GANLESI/GANLESI.htm