INFORME MENSUAL

RED DE SENSORES DE INTECO

Noviembre 2012

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 MES 8

3.1. Correos electrónicos procesados 8

3.2. Virus 11

3.2.1. Top Virus del mes 11

3.2.2. Dispersión de antivirus en la Red de Sensores de INTECO 12

3.2.3. Virus por sectores de actividad 13

3.2.4. Virus por ámbito geográfico 15

3.3. SPAM 16

3.3.1. Nivel de SPAM del mes 17

3.3.2. Evolución temporal de totales 18

3.3.3. Evolución mensual del SPAM 18

3.3.4. Top 10 de países emisores de SPAM 19

4. NO SOLO SENSORES 20

4.1. Vulnerabilidades 20

4.1.1. Nivel de severidad de vulnerabilidades 20

4.1.2. Productos más afectados 20

4.1.3. Fabricantes más afectados 21

4.1.4. Vulnerabilidades más comunes según su tipo 22

4.2. Fraude Electrónico 22

4.2.1. Número total de incidentes de fraude 22

4.2.2. Número total de URLs fraudulentas 23

4.3. Avisos Tecnicos y no técnicos publicados 25

4.4. Eventos del mes (DICIEMBRE 2012) 26

4.4.1. II Congreso de Seguridad Navaja Negra 26

4.4.2. Segundo Taller Iberoamericano de Enseñanza e Innovación Educativa en Seguridad de la Información - TIBETS2012 26

4.4.3. Espacio TISEC 2012 27

4.4.4. VI Jornadas STIC 27

4.4.5. I Encuentro "Futuro y retos del universo digital móvil en la empresa" 27

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 y virus detectados. 9

Figura 6: Evolución mensual de correos procesados por sector de actividad. 9

Figura 7: Virus más activos en la red de sensores durante el mes. 11

Figura 8: Antivirus utilizados en los sensores. 12

Figura 9: Relación correos analizados sin virus/correos con virus detectado por antivirus. 12

Figura 10: Porcentaje de correos sin virus frente a correos con virus detectados por sectores de actividad. 13

Figura 11: Top virus por sectores de actividad. 13

Figura 12: Tabla de virus más detectados por sectores. 14

Figura 13: Mapa autonómico de detecciones de virus. 15

Figura 14: Sensores, correo y porcentaje de infección detectada por autonomía. 16

Figura 15: Nivel de SPAM detectado por la red de sensores. 17

Figura 16: Evolución temporal del SPAM detectado por la red de sensores. 18

Figura 17: Evolución mensual del SPAM a lo largo del año. 18

Figura 18: Top 10 países emisores de SPAM según datos recogidos por la RSI. 19

Figura 19: Vulnerabilidades emitidas por nivel de riesgo. 20

Figura 20: Productos más afectados por las últimas vulnerabilidades. 21

Figura 21: Fabricantes más afectados por las últimas vulnerabilidades. 21

Figura 22: Vulnerabilidades más comunes por tipo. 22

Figura 23: Evolución del número de incidentes de Fraude. 23

Figura 24: Evolución del número de URLs fraudulentas. 24

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 **100 entidades** que albergan al menos un sensor y que están ubicados en diferentes sectores con el porcentaje de distribución que aparece en la figura.

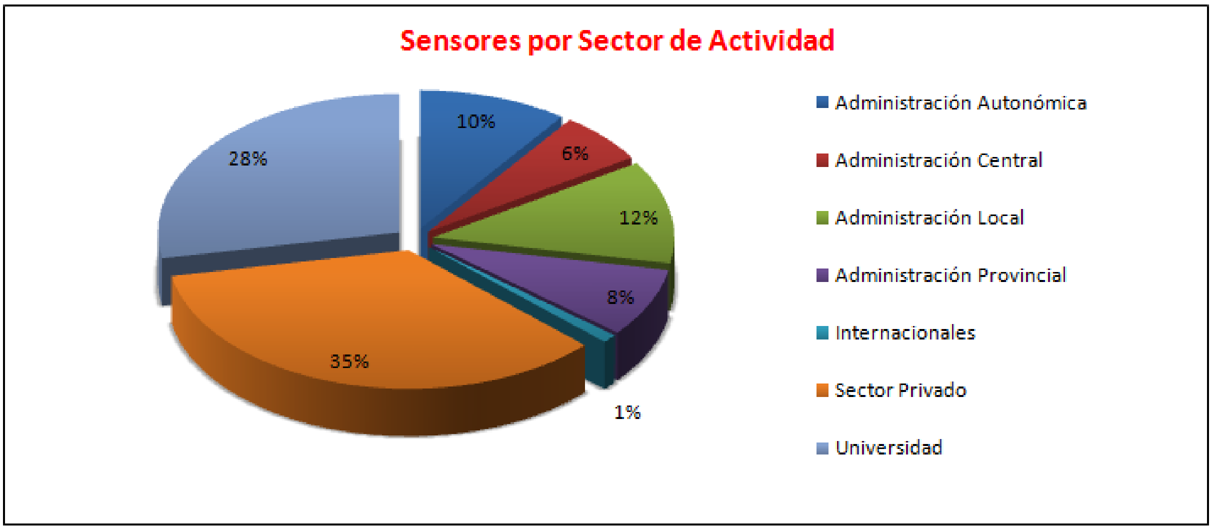

Figura 1: Distribución de los sensores por sector de actividad.

2.1. ACTIVIDAD DE LOS SENSORES

Como se puede ver, la actividad de los sensores se ha mantenido estable en los dos últimos meses. Tres sensores han pasado de enviar informes de forma regular a enviarlos de forma intermitente. A lo largo del mes de Noviembre dos sensores fueron dados de baja de la Red de Sensores de INTECO por inactividad:

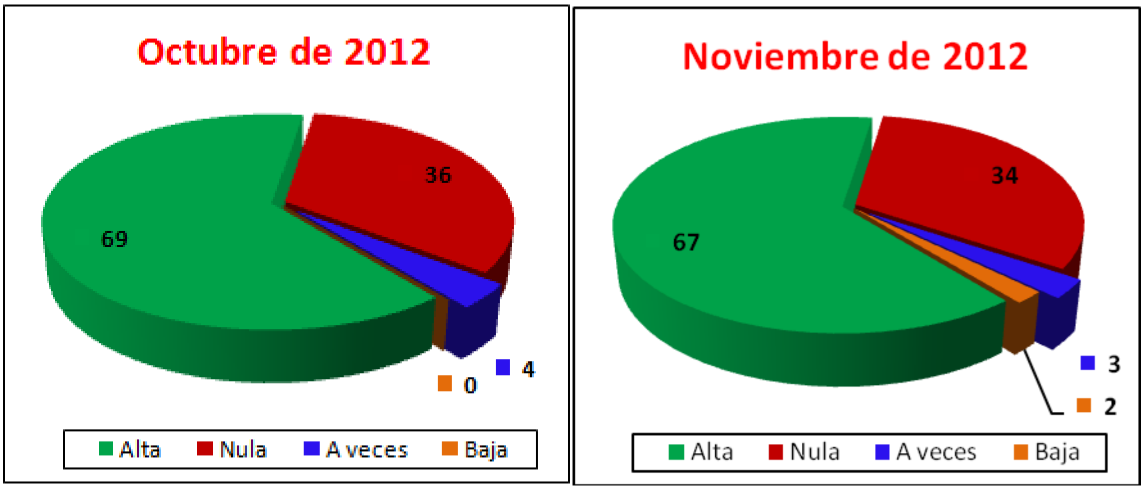

Figura 2: Distribución de sensores según frecuencia en el envío del informe.

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.

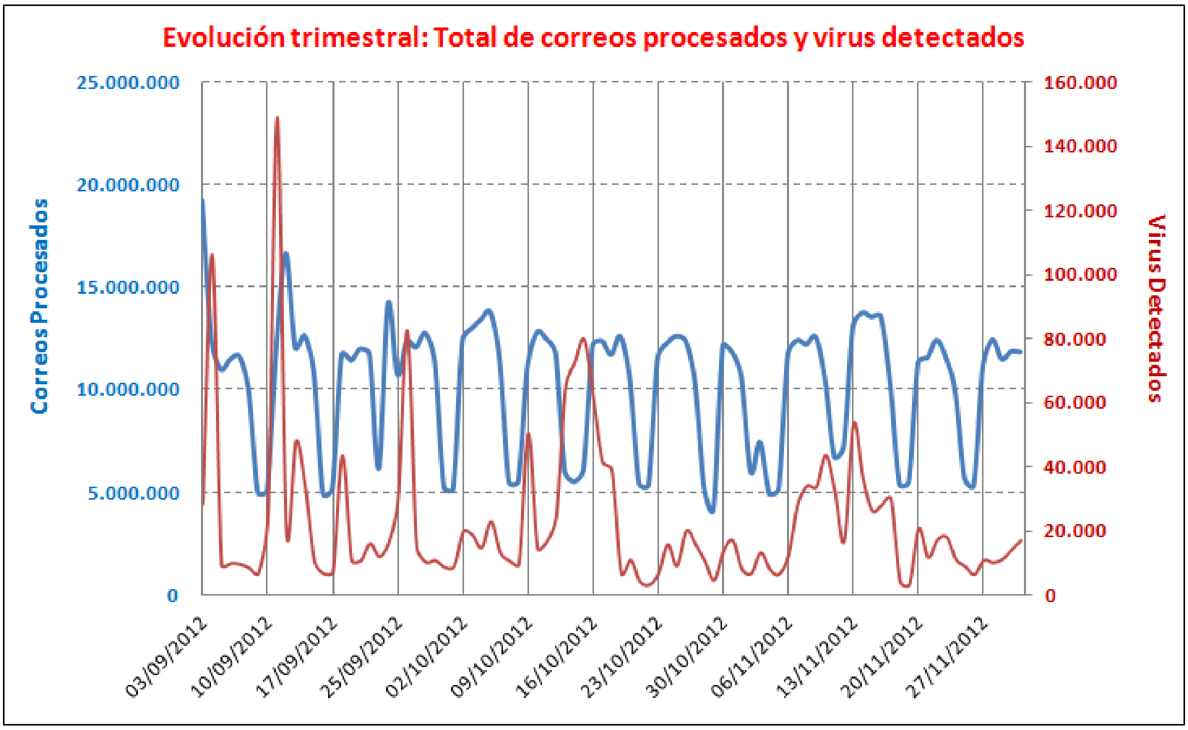

Figura 3: Evolución trimestral de correos procesados y virus detectados.

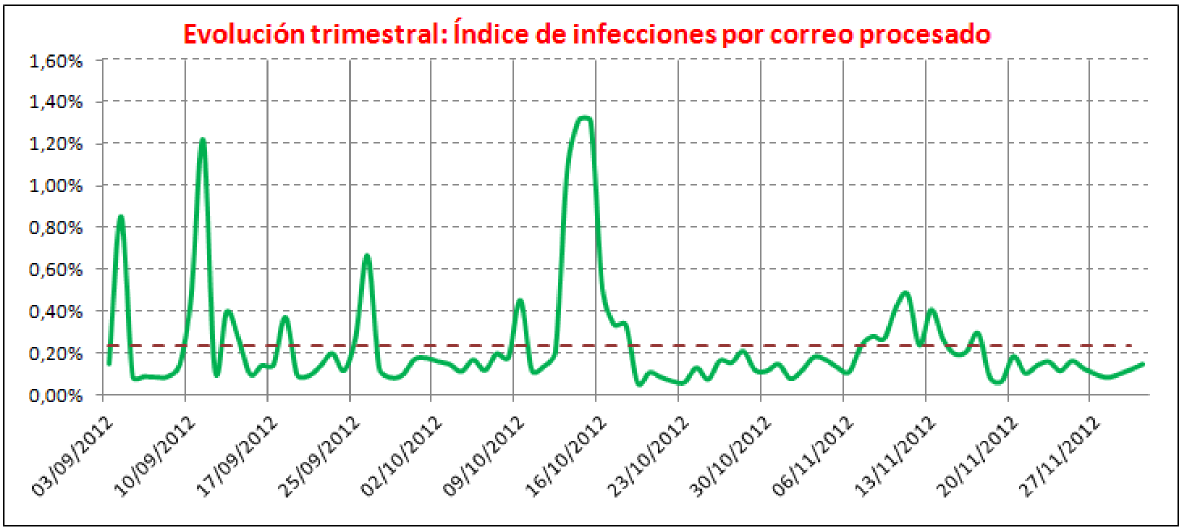

Figura 4: Evolución trimestral del índice de infecciones por correo procesado.

Como se puede ver en la figura 4, el porcentaje de correos infectados se encuentra en torno al **0,24%** de los correos recibidos (24 infecciones por cada 10000 correos).

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

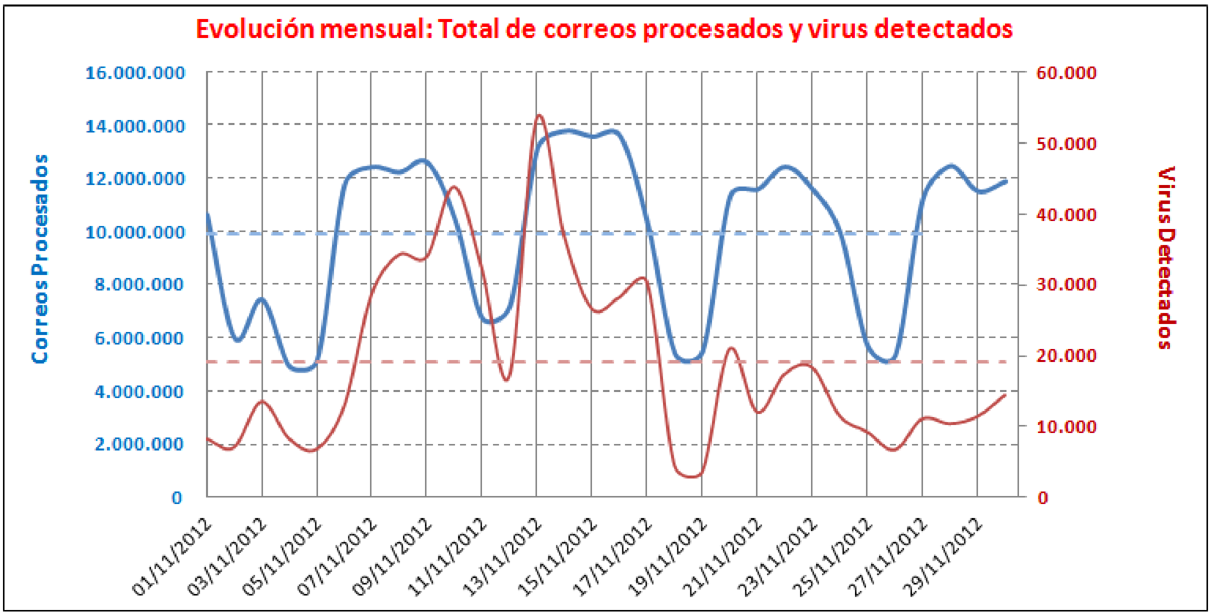

Figura 5: Evolución mensual de correos procesados y virus detectados.

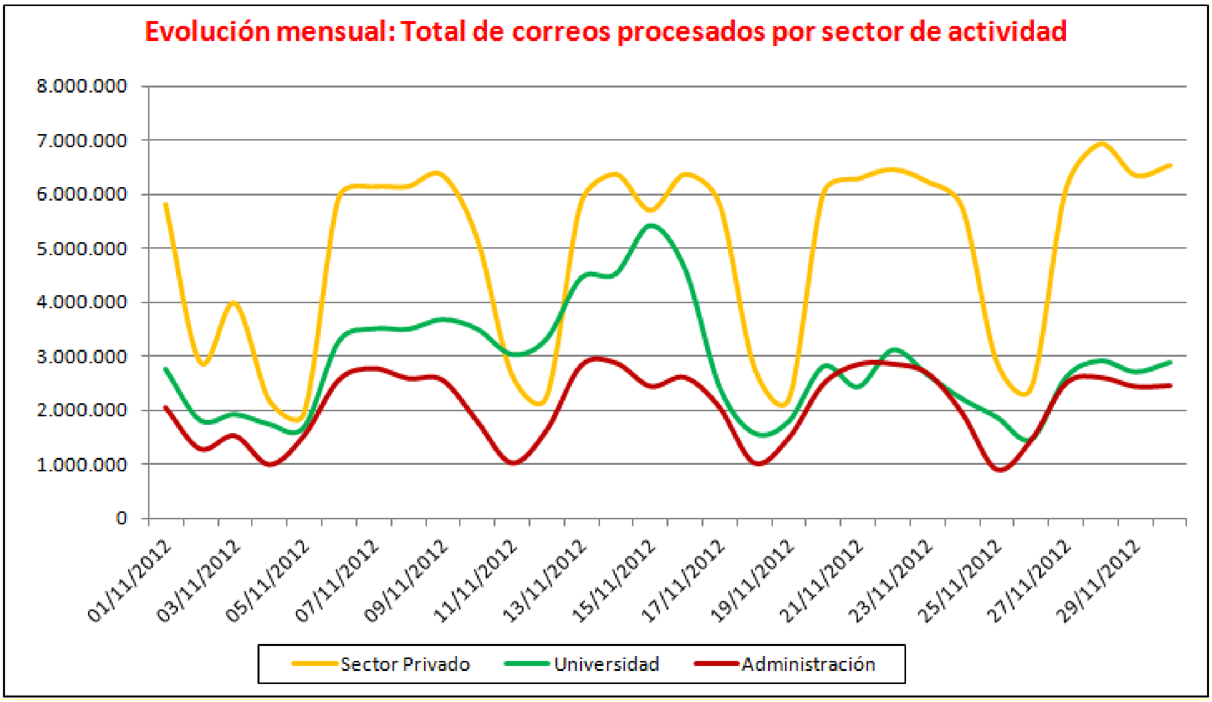

Figura 6: Evolución mensual de correos procesados por sector de actividad.

En la imagen anterior, se muestra la aportación al volumen de correos procesados de los diferentes sectores de actividad durante el mes de Noviembre.

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 (casi el 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.

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 Noviembre.

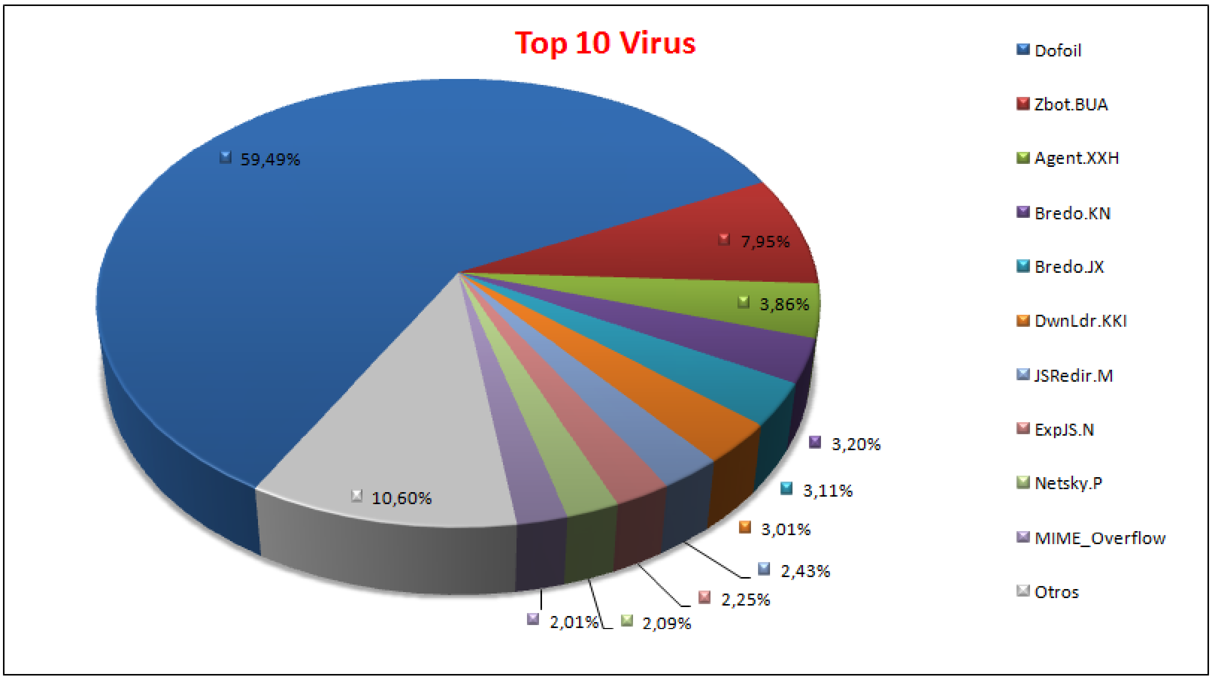

Figura 7: Virus más activos en la red de sensores durante el mes.

Este mes el virus más activo ha sido ha sido de nuevo *Dofoil*, con un 59,49% del total de virus detectados en la Red de Sensores. Le sigue *Zbot.BUA*, con un 7,95% y *Agent.XXH* con un 3,86%.

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.

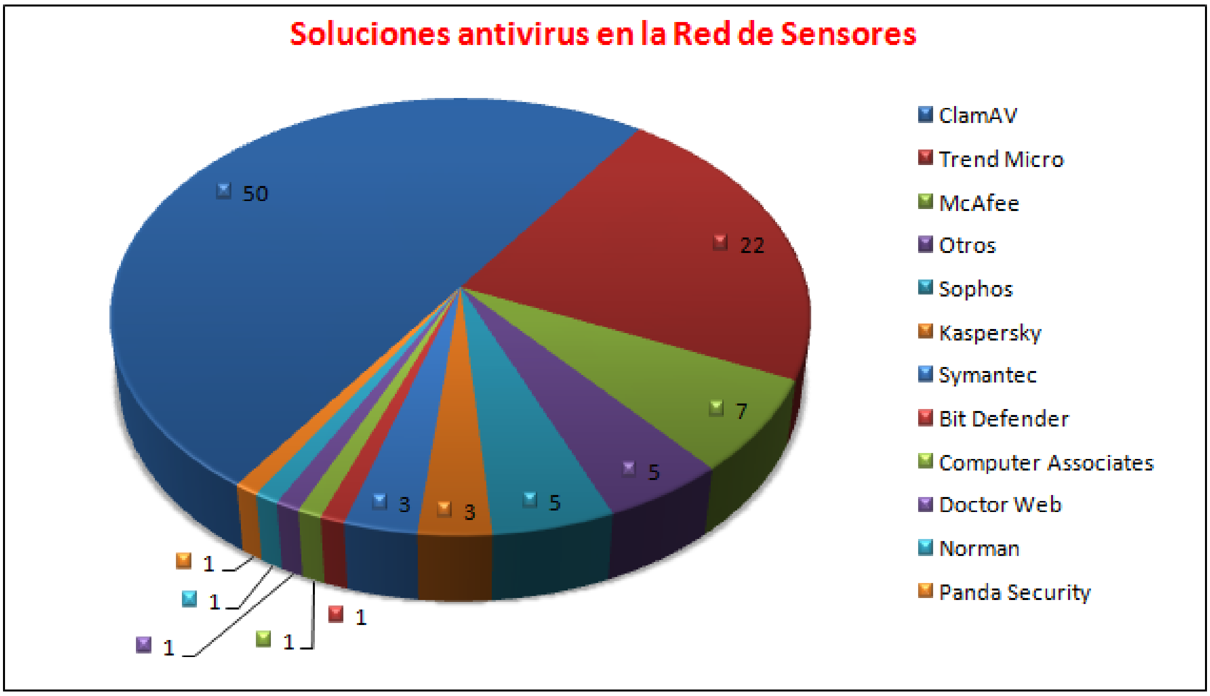

Figura 8: Antivirus utilizados en los sensores.

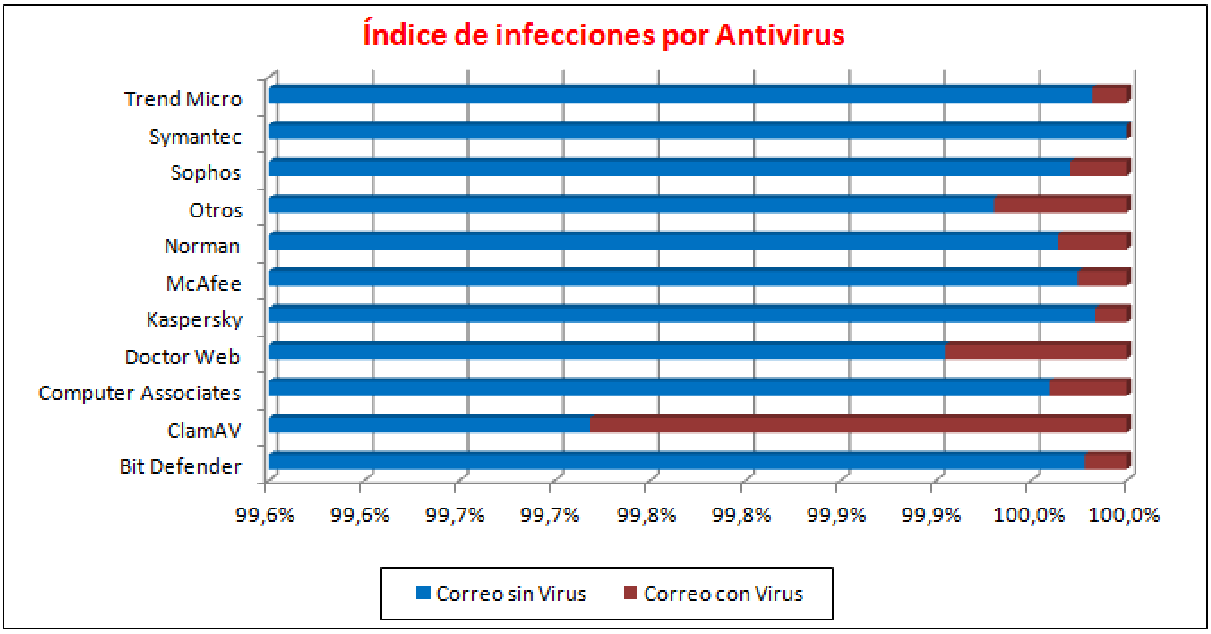

Figura 9: Relación correos analizados sin virus/correos con virus detectado por antivirus.

3.2.3. Virus por sectores de actividad

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.

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.

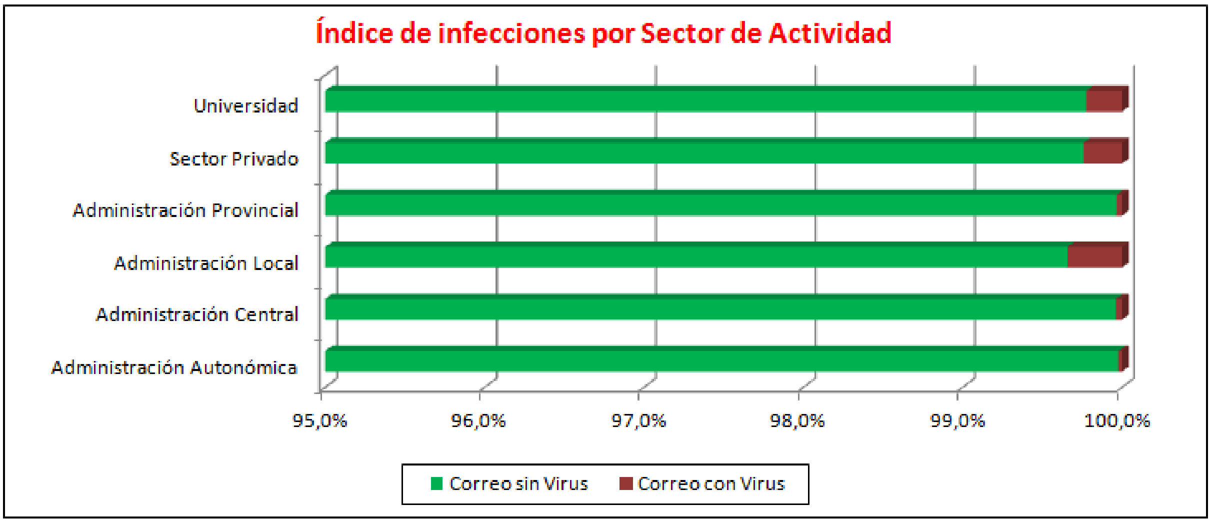

Figura 10: Porcentaje de correos sin virus frente a correos con virus detectados por sectores de actividad.

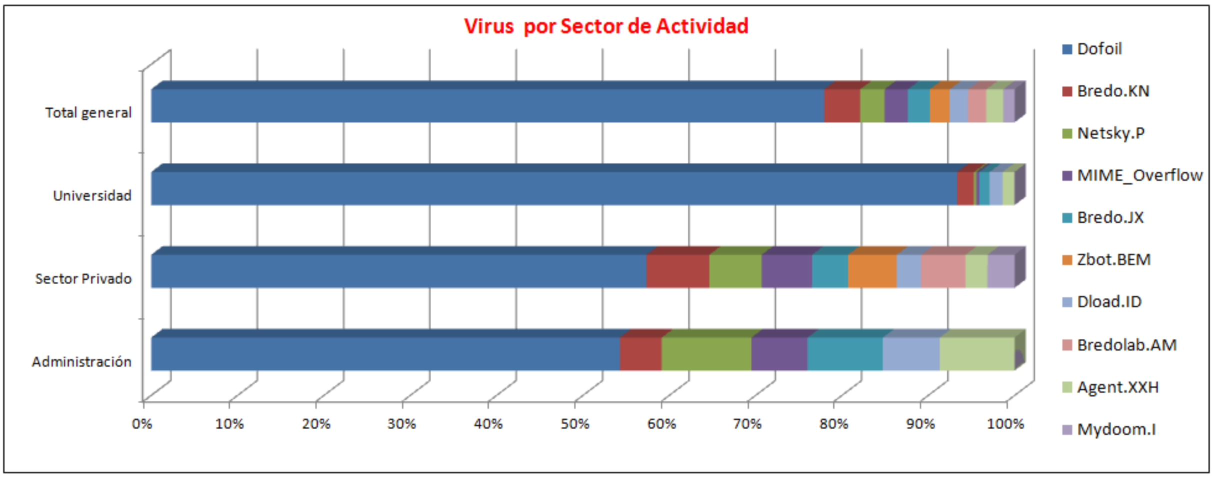

Figura 11: Top virus por sectores de actividad.

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

Virus	Administración	Sector Privado	Universidad	Total general
Dofoil	32,08%,	53,9%,	90,85%,	74,04%,
Bredo.KN	2,87%,	6,84%,	1,9%,	3,98%,
Netsky.P	6,14%,	5,71%,	0,28%,	2,68%,
MIME_Overflow	3,84%,	5,48%,	0,34%,	2,56%,
Bredo.JX	5,16%,	3,91%,	1,15%,	2,39%,
Zbot.BEM	0%,	5,29%,	0%,	2,2%,
Dload.ID	3,89%,	2,65%,	1,47%,	2,02%,
Bredolab.AM	0%,	4,83%,	0%,	2,01%,
Agent.XXH	5,13%,	2,42%,	1,32%,	1,87%,
Mydoom.I	0%,	2,94%,	0,03%,	1,24%,
Otros	40,89%,	6,02%,	2,65%,	5,01%,

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 Noviembre.

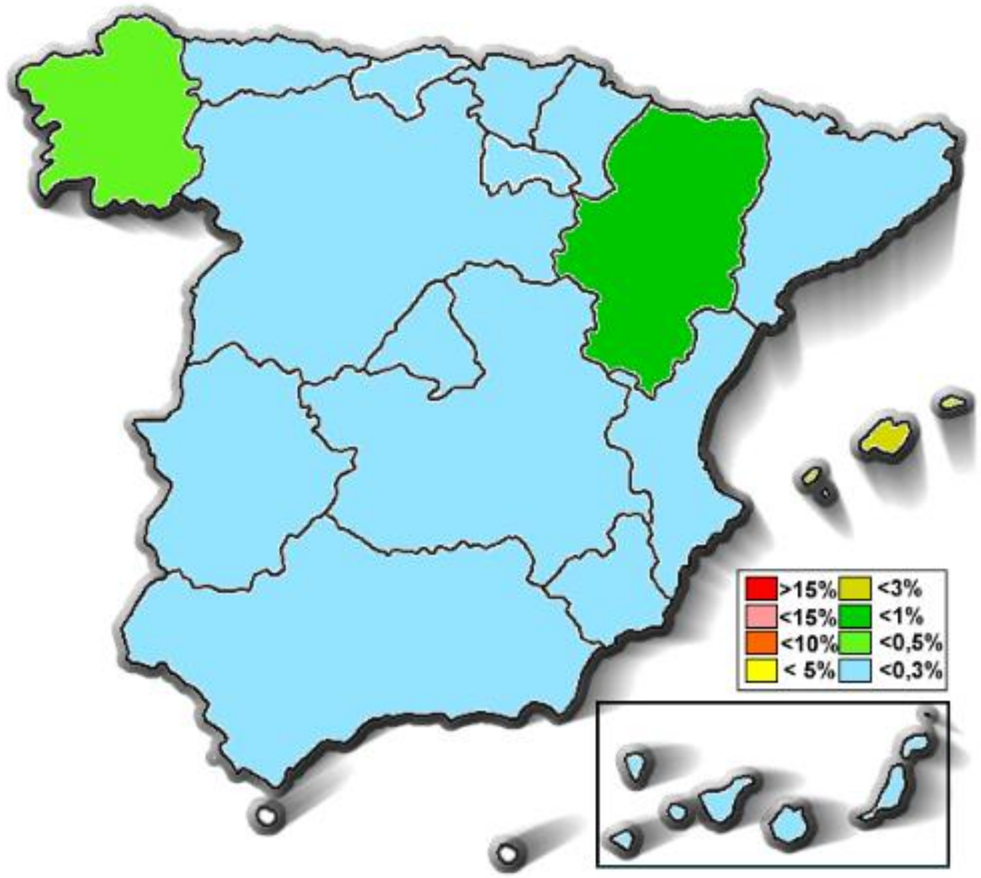

Figura 13: Mapa autonómico de detecciones de virus.

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	31.215.708	0,06%
Aragón	25.244.172	0,51%
Canarias	2.508.366	0,01%
Cantabria	0	0,0%
Castilla y León	2.034.827	0,0%
Castilla-La Mancha	18.226.352	0,06%
Catalunya / Cataluña	31.543.310	0,18%
Ciudad Autónoma de Ceuta	0	0,0%
Ciudad Autónoma de Melilla	0	0,0%
Comunidad Foral de Navarra	2.525.547	0,02%
Comunidad de Madrid	11.423.087	0,01%
Comunitat Valenciana / Comunidad Valenciana	17.760.375	0,19%
Euskadi / País Vasco	1.396.354	0,02%
Extremadura	310.967	0,02%
Galicia / Galicia	15.215.779	0,32%
Illes Balears / Islas Baleares	123.702	1,15%
La Rioja	0	0,0%
Principado de Asturias	15.191.815	0,0%
Región de Murcia	3.842.040	0,0%

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

Como se puede ver, durante el pasado mes de Noviembre, fue **Catalunya** la comunidad que más muestras aportó a la red de Sensores, aunque la que tuvo un número total de infecciones más elevado (unas 500.000) fue **Aragón.** Pero la comunidad con un porcentaje de correo infectado más alto (1,15%) fueron las **Islas Baleares**.

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.

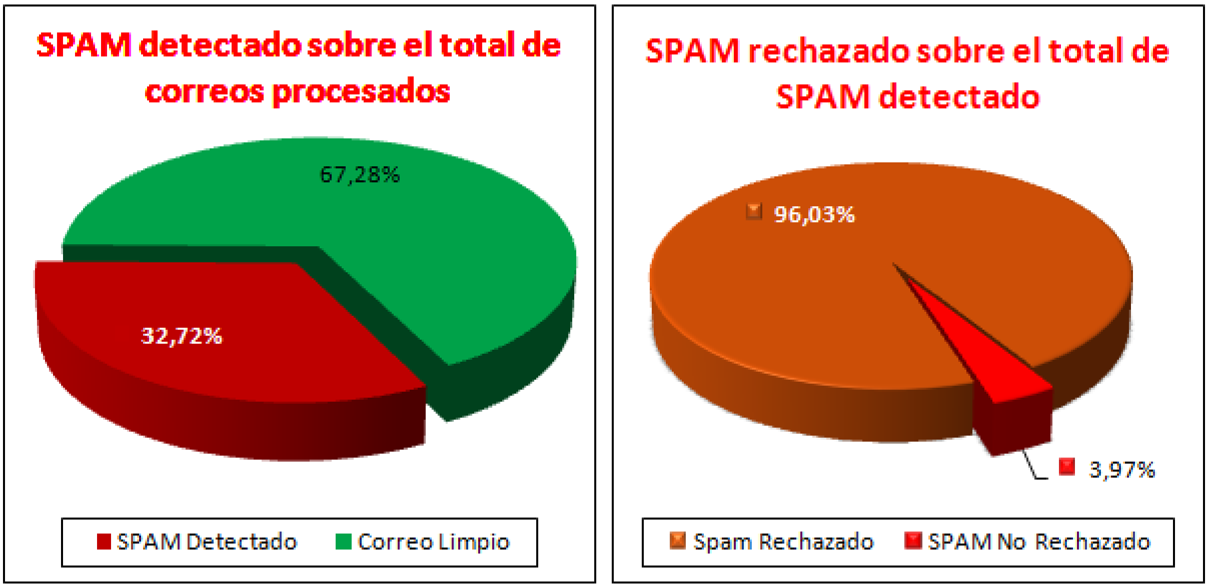

Figura 15: Nivel de SPAM detectado por la red de sensores.

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 Noviembre, el nivel de SPAM en correo fue de un **32,72%** 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 Octubre. 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.

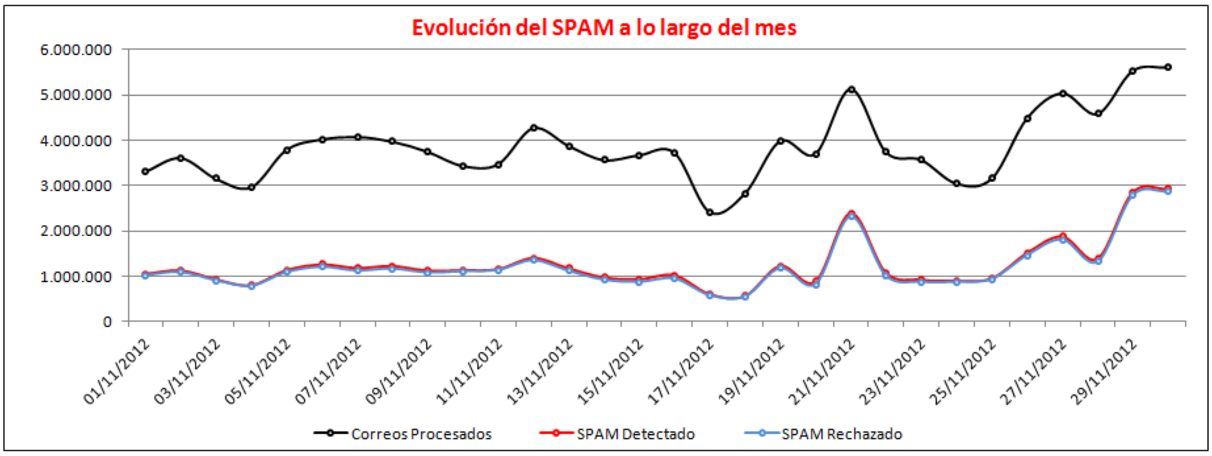

Figura 16: Evolución temporal del SPAM detectado por la red de sensores.

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 12 meses. La línea azul muestra el porcentaje de SPAM detectado en correo y se mide con el eje de la derecha. Como se puede ver el nivel del SPAM se encuentra en su nivel más bajo en lo que va de año.

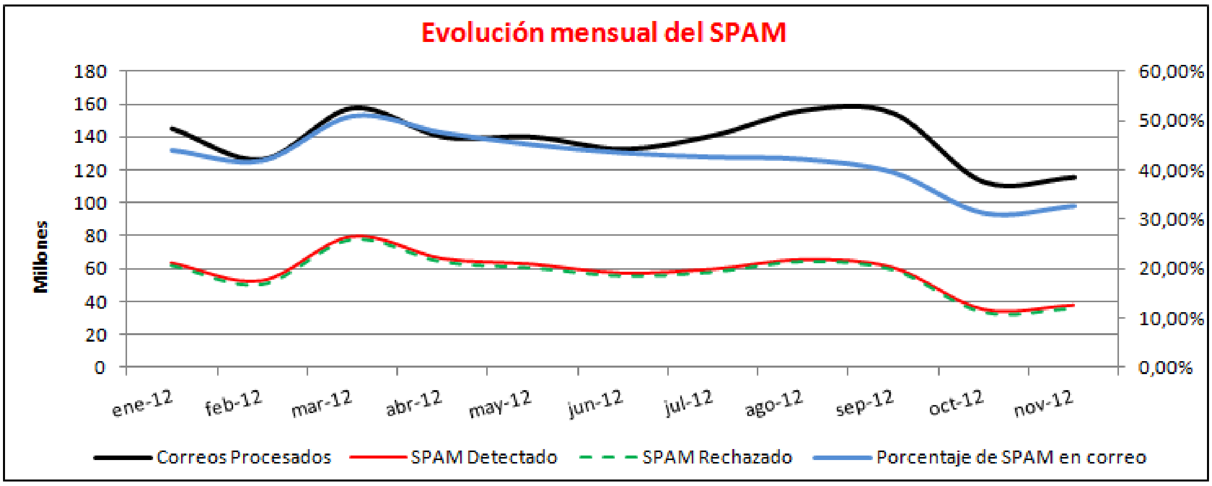

Figura 17: Evolución mensual del SPAM a lo largo del año.

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.

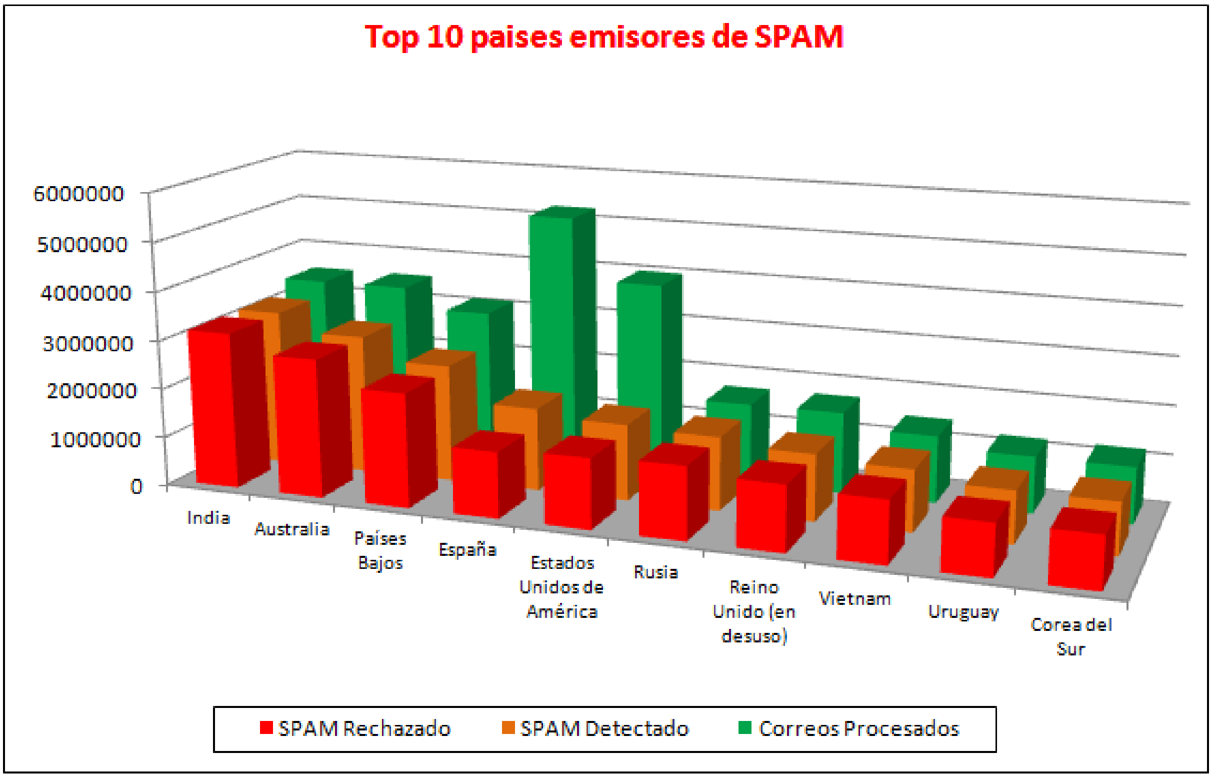

Figura 18: Top 10 países emisores de SPAM según datos recogidos por la RSI.

Se puede comprobar que, a lo largo del último mes, los países que más SPAM han mandado a direcciones de correo españolas han sido **India, Australia** y **Países Bajos**. Es de destacar el caso de la India, puesto que más del 92% del correo recibido de ese país es SPAM. Existen países con un porcentaje de SPAM enviado superior, pero no con una cantidad de correo tan grande (3,5 millones de correos procesados).

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 Octubre.

A lo largo del pasado mes se emitieron un total de **510** vulnerabilidades, con un nivel de severidad mayoritariamente **medio y alto**. Los niveles de severidad de las vulnerabilidades publicadas aparecen en la siguiente figura.

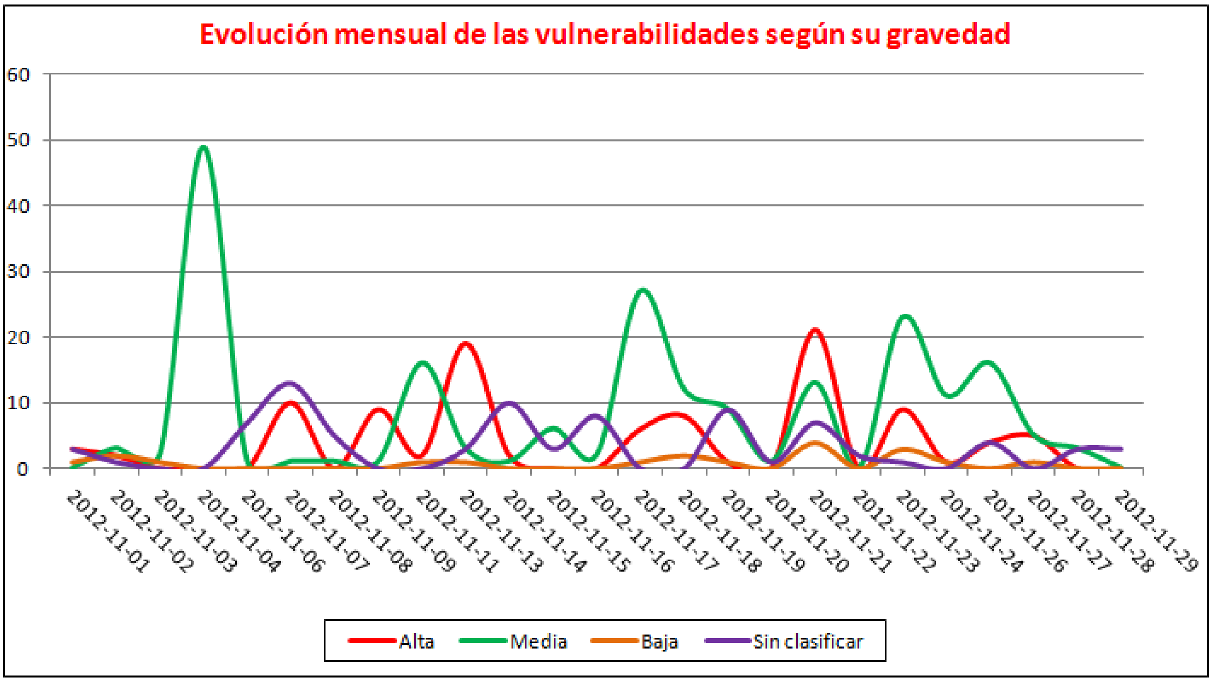

Figura 19: Vulnerabilidades emitidas por nivel de riesgo.

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 Noviembre.

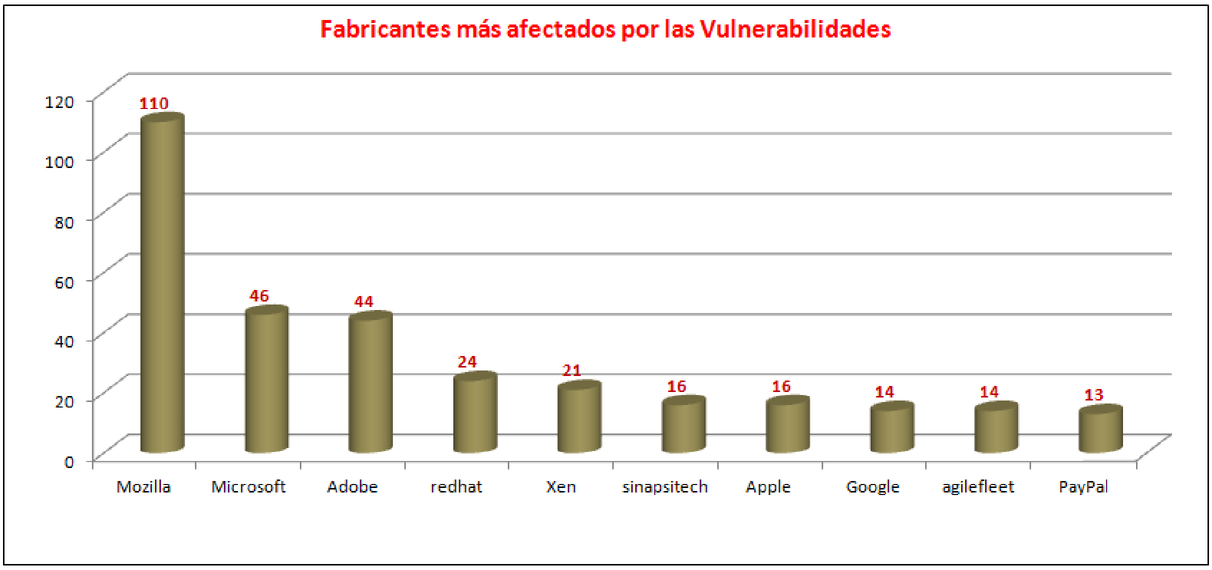

Figura 21: Fabricantes más afectados por las últimas vulnerabilidades.

4.1.4. Vulnerabilidades más comunes según su tipo

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

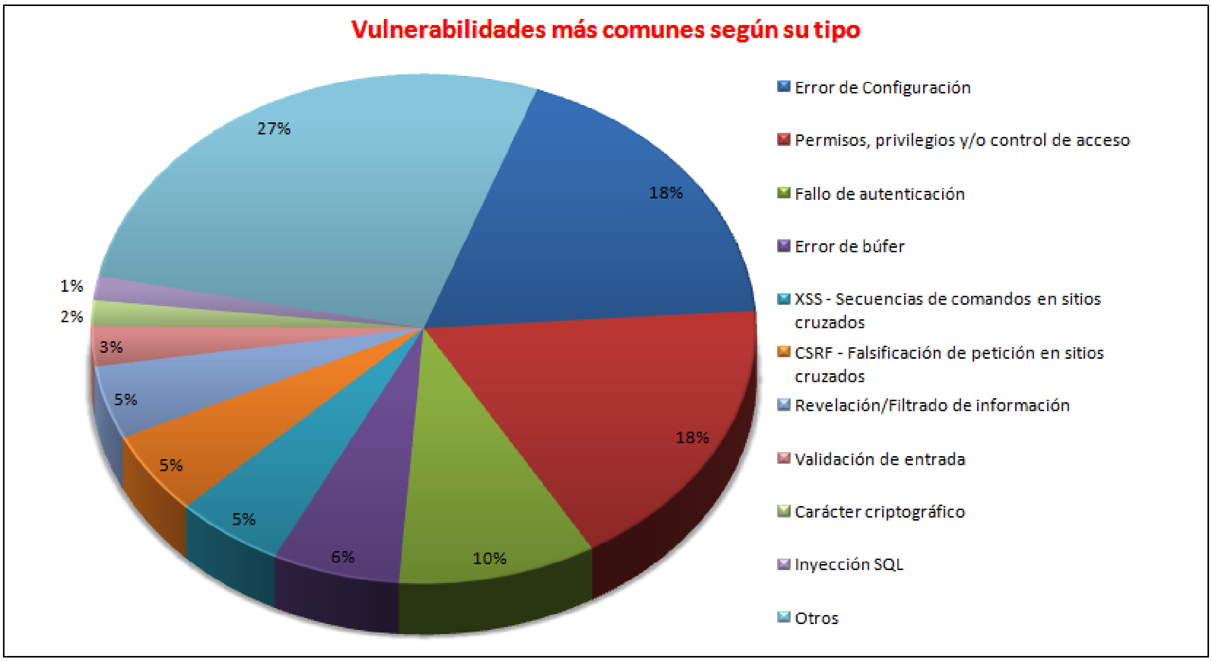

Figura 22: Vulnerabilidades más comunes por tipo.

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
Diciembre 2011	768	**Junio 2012**	1002
Enero 2012	744	**Julio 2012**	723
Febrero 2012	518	**Agosto 2012**	874
Marzo 2012	732	**Septiembre 2012**	969

Abril 2012	618	**Octubre 2012**	841
Mayo 2012	723	**Noviembre 2012**	670

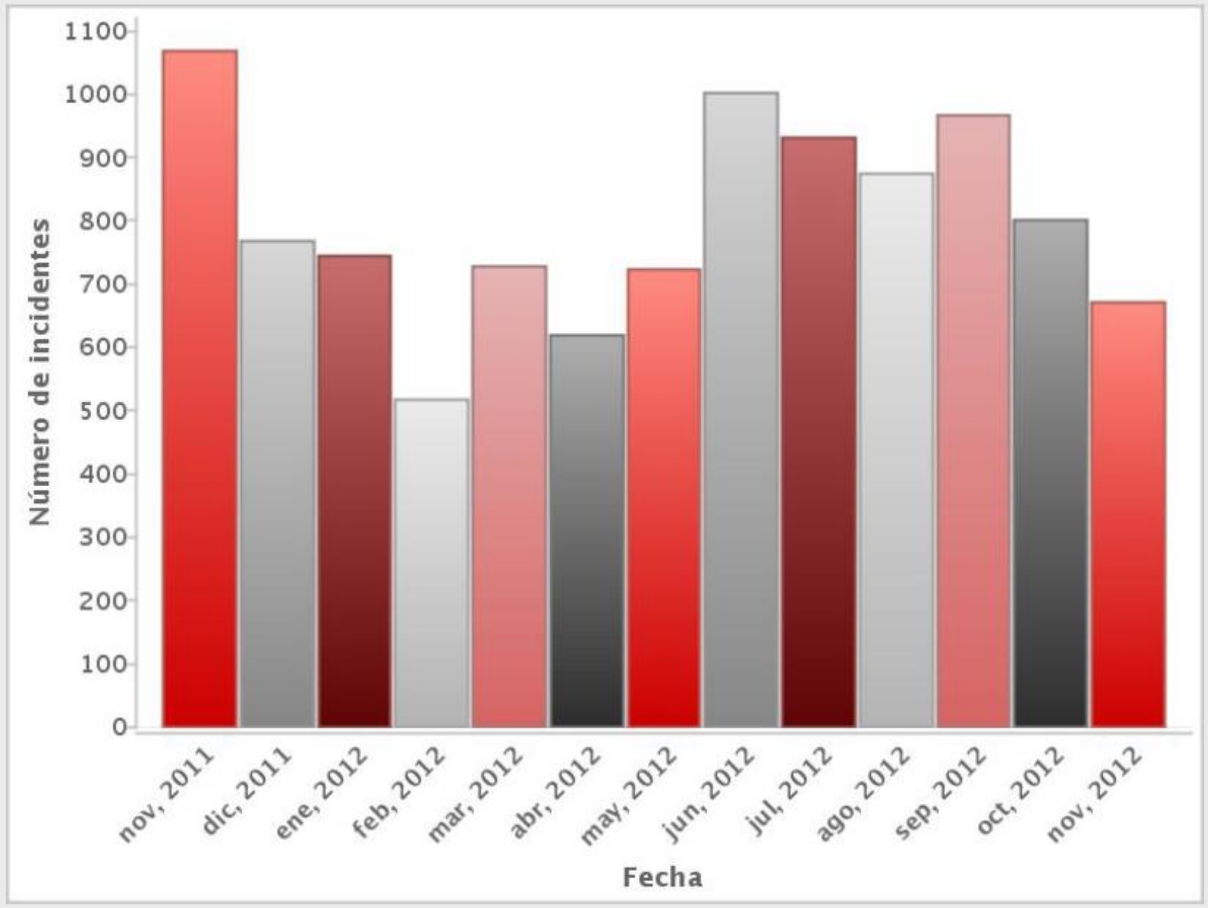

Figura 23: Evolución del número de incidentes de Fraude.

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.

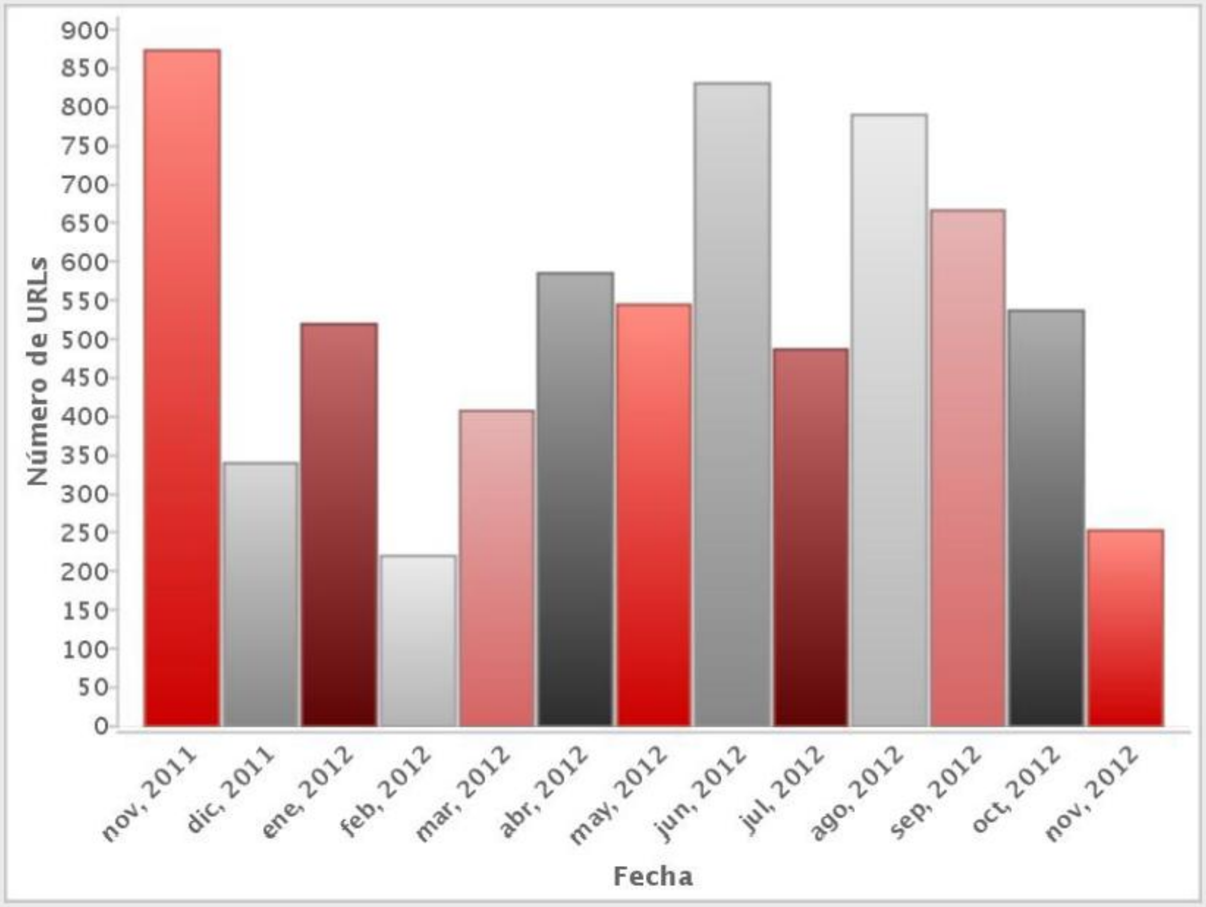

Figura 24: Evolución del número de URLs fraudulentas.

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

Mes	URLs fraudulentas	Mes	URLs fraudulentas
Diciembre 2011	339	**Junio 2012**	831
Enero 2012	519	**Julio 2012**	542
Febrero 2012	221	**Agosto 2012**	793
Marzo 2012	403	**Septiembre 2012**	666
Abril 2012	585	**Octubre 2012**	536
Mayo 2012	541	**Noviembre 2012**	253

4.3. AVISOS TECNICOS Y NO TÉCNICOS PUBLICADOS

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

Aviso de Seguridad	Fecha
Nuevos bulos se difunden a través de WhatsApp https://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_no_tecnicos/nuevos_bulos_se_difunden_traves_whatsapp_20121128	28/11/2012
Boletines de seguridad de Microsoft de Noviembre 2012 https://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/boletines_seguridad_microsoft_noviembre_2012_20121114	14/11/2012
Actualizaciones de seguridad 2.5.8 y 3.0.1 para Joomla! https://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/actualizaciones_seguridad_258_301_joomla_20121112	12/11/2012
Vulnerabilidades en appliances de seguridad Cisco Ironport para email y web https://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/vulnerabilidad_adobe_x_permite_evitar_sandbox_20121109	10/11/2012
Vulnerabilidad en Adobe X permite evitar la sandbox http://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/vulnerabilidad_gestion_credenciales_varios_modelos_camaras_ip_20121016	09/11/2012
Publicado Quicktime 7.7.3 para Windows https://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/publicado_quicktime_773_windows_20121109	09/11/2012
Actualizaciones de seguridad para Flash Player https://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/actualizaciones_seguridad_flash_player_20121107	07/11/2012
Avisos de seguridad de Cisco Prime DCNM y Cisco Unified MeetingPlace Web Conferencing https://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/avisos_seguridad_cisco_prime_dcnm_cisco_unified_meetingplace_web_conferencing_20121101	01/11/2012

4.4. EVENTOS DEL MES (DICIEMBRE 2012)

4.4.1. II Congreso de Seguridad Navaja Negra

Conferencias centradas en la seguridad informática en Albacete. Impartidas por un grupo de voluntarios apasionados de la seguridad y con ganas de compartir sus conocimientos y de carácter gratuito.

- Fecha 30 de Noviembre y 1 de Diciembre
- Lugar: Albacete
- Precio: Gratuito
- Más información: http://www.navajanegra.com

4.4.2. Segundo Taller Iberoamericano de Enseñanza e Innovación Educativa en Seguridad de la Información - TIBETS2012

Es un evento promovido por la red temática Criptored, en el que se presentarán ponencias y desarrollarán foros abiertos para debatir lo que se está haciendo, y lo que debería hacerse, en cuanto a la enseñanza e innovación educativa en Seguridad de la Información en Iberoamérica. Con el lema "por una mejor enseñanza de la Seguridad de la Información", TIBETS sugiere un reto y una cima de calidad a la que todos los centros e institutos de investigación desean llegar en la enseñanza y la formación de esta especialidad en los países iberoamericanos.

Los temas de interés incluyen experiencias docentes y presentación de nuevas asignaturas en seguridad de la información; adecuación de las asignaturas de seguridad a formatos de e-learning y MOOC; presentación de postgrados, propuestas de formación en seguridad de la información; metodologías docentes utilizadas en la impartición de asignaturas de seguridad; software de apoyo a la docencia y prácticas de seguridad de la información; desarrollo de competencias en seguridad de la información; innovaciones educativas realizadas en enseñanza de seguridad de la información; control anti-plagio en la presentación de trabajos finales, tesinas y tesis; proyectos de vinculación empresa - universidad en seguridad de la información; perfiles que la empresa requiere versus perfiles de egreso en universidades; cursos empresariales de seguridad de la información en los países iberoamericanos; agendas de investigación en temas especializados o emergentes en enseñanza; desarrollo de competencias en seguridad de la información; planes de estudios especializados en seguridad de la información; y encuestas de necesidades laborales en seguridad de la información.

- Fecha: 03-05 de Diciembre de 2012
- Lugar: Loja, Ecuador

- Precio: Consultar
- Más información: http://www.utpl.edu.ec/tibets

4.4.3. Espacio TISEC 2012

La revista SIC organiza esta jornada matutina de puertas abiertas (previa solicitud de inscripción) durante la cual se especificará la posición de las autoridades de control acerca de la Nube, se brindarán puntos de vista orientados a la fijación de cláusulas en contratos de servicios en Nube, se especificarán qué técnicas y herramientas orientadas a la protección del dato serían imprescindibles para el cumplimiento legal, y se debatirán los pros y contras del uso de la Nube desde una perspectiva amplia: AEPD, usuarios, prestadores y proveedores de tecnologías.

- Fecha 4 de Diciembre
- Lugar: Madrid. Hotel Novotel Campo de las Naciones
- Precio: Consultar
- Más información: http://www.revistasic.com/tisec

4.4.4. VI Jornadas STIC

Un año más, el CERT Gubernamental español organiza estas VI Jornadas STIC, en las que compartir con todas las Administraciones y sectores estratégicos (públicos y privados) los riesgos y amenazas del ciberespacio, así como las últimas tendencias para hacerles frente.

- Fecha 11 y 12 de Diciembre
- Lugar: Madrid
- Precio: Consultar
- Más información: https://www.ccn-cert.cni.es/index.php?option=com_content&view=article&id=3185&Itemid=198&lang=es

4.4.5. I Encuentro "Futuro y retos del universo digital móvil en la empresa"

En 2013 más de 1.190 millones de profesionales de todo el mundo utilizarán la tecnología móvil, según un estudio de IDC. Esto supone que un 34,9% de la población activa trabajará mediante smartphones, tabletas u otras soluciones basadas en la tecnología cloud computing. En este contexto, se hace esencial la supervisión del Chief Information Oficcer (CIO). El CIO debe asumir su papel dentro de la estrategia corporativa de la empresa y trabajar para que el nuevo paradigma tecnológico favorezca a su cadena de valor, sin perjuicio de la seguridad.

Por este motivo, los CIO deben analizar los servicios de Tecnologías de la Información (TI) de sus empresas, sobre todo aquellos que operan en la nube, para definir nuevos protocolos de seguridad de la información o de participación en las redes sociales, entre otros ámbitos clave. Además, han de afrontar nuevos retos que integren las nuevas estrategias empresariales en auge como el bring your own device (BYOD), que lleva cada vez a más profesionales a utilizar dispositivos móviles personales para fines laborales.

- Fecha: 18 de Diciembre
- Lugar: Madrid
- Precio: Consultar
- Más información: http://conferenciasyformacion.us6.list-manage2.com/track/click?u=37923ce944dea1dd2cd741768&id=44d00cb3d6&e=95d17a6703