INFORME MENSUAL

RED DE SENSORES DE INTECO

Red de Sensores de Inteco

Septiembre 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

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 celebrará 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 **111 entidades** que albergan al menos un sensor y que están ubicados en diferentes sectores con el porcentaje de distribución que aparece en la figura.

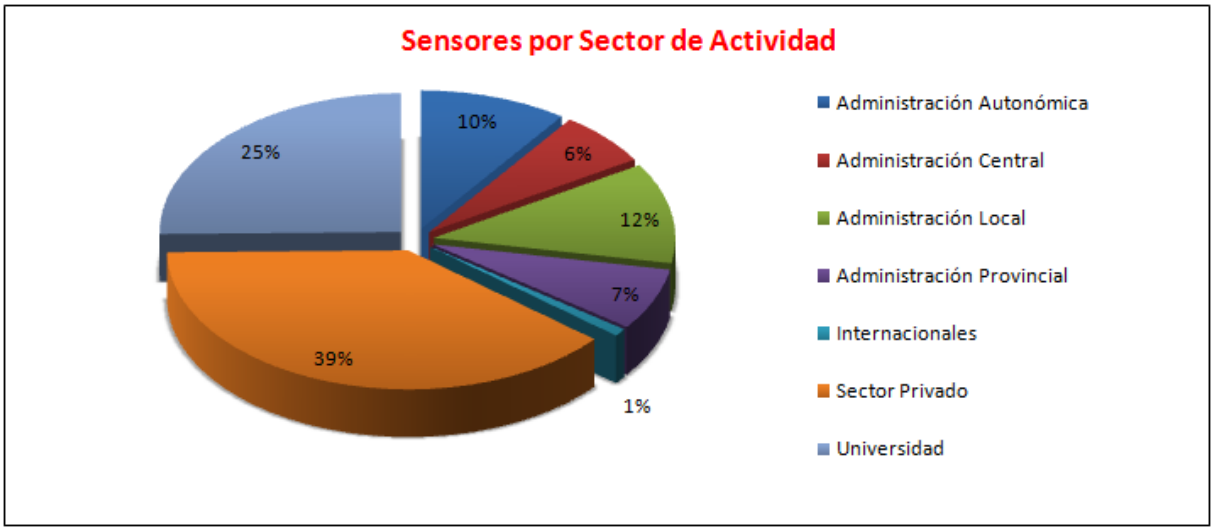

Figura 1: Distribución de los sensores por sector de actividad.

2.1. ACTIVIDAD DE LOS SENSORES

Como se puede ver, la actividad de los sensores se ha mantenido estable en los dos últimos meses. Algunos de los sensores inactivos serán dados de baja durante los próximos meses.

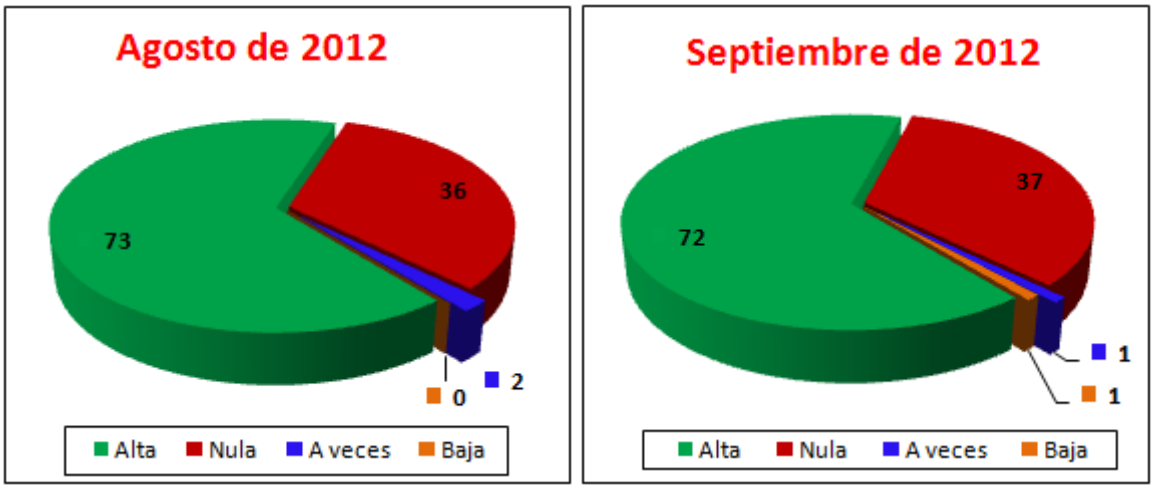

Figura 2: Distribución de sensores según frecuencia en el envío del informe.

A lo largo del mes de **Septiembre** un sensor se dio de baja de la Red de Sensores de INTECO. Se trató de la Universidad Politécnica de Cartagena.

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.

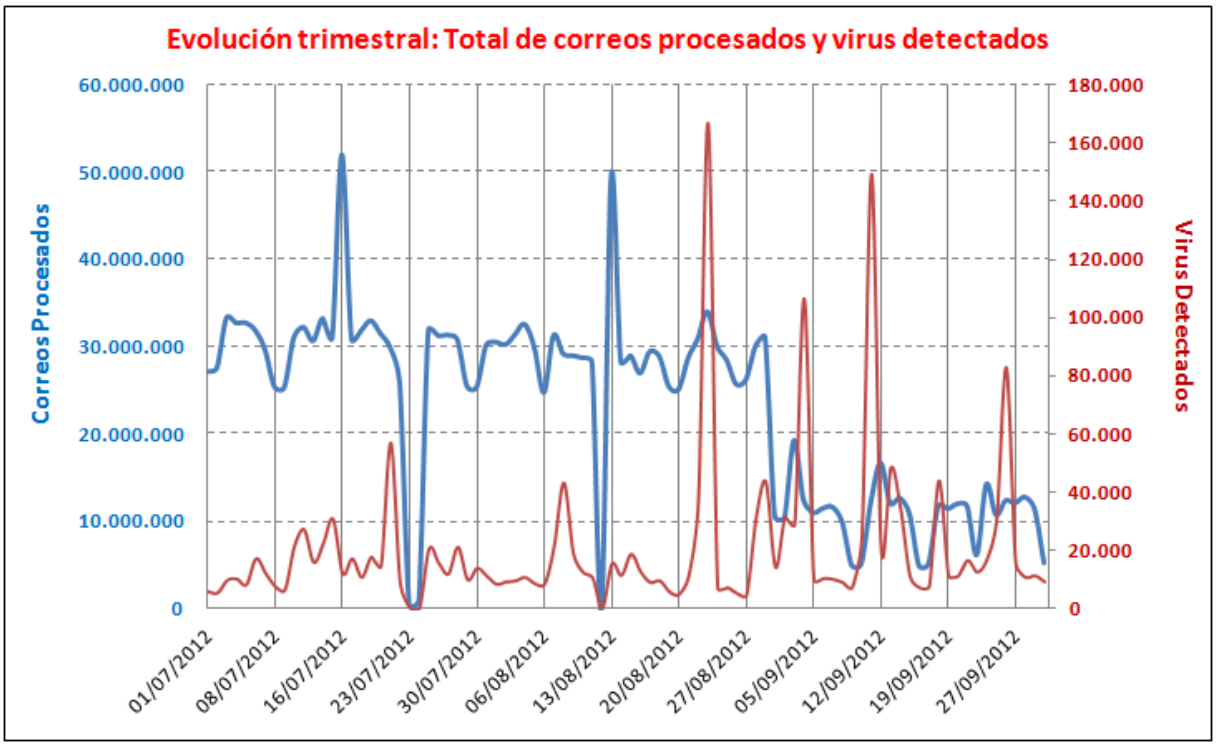

Figura 3: Evolución trimestral de correos procesados y virus detectados.

Como se puede ver desde el 1 de Septiembre, el número de correos procesados ha sufrido una drástica reducción, no así el número de virus detectados. La razón es la caída de una serie de sensores de un par de entidades, gran relevancia dentro de la Red de Sensores de INTECO. Dichos colaboradores han sido debidamente informados de este hecho y se están tomando las medidas que necesarias para recuperar sus envíos.

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

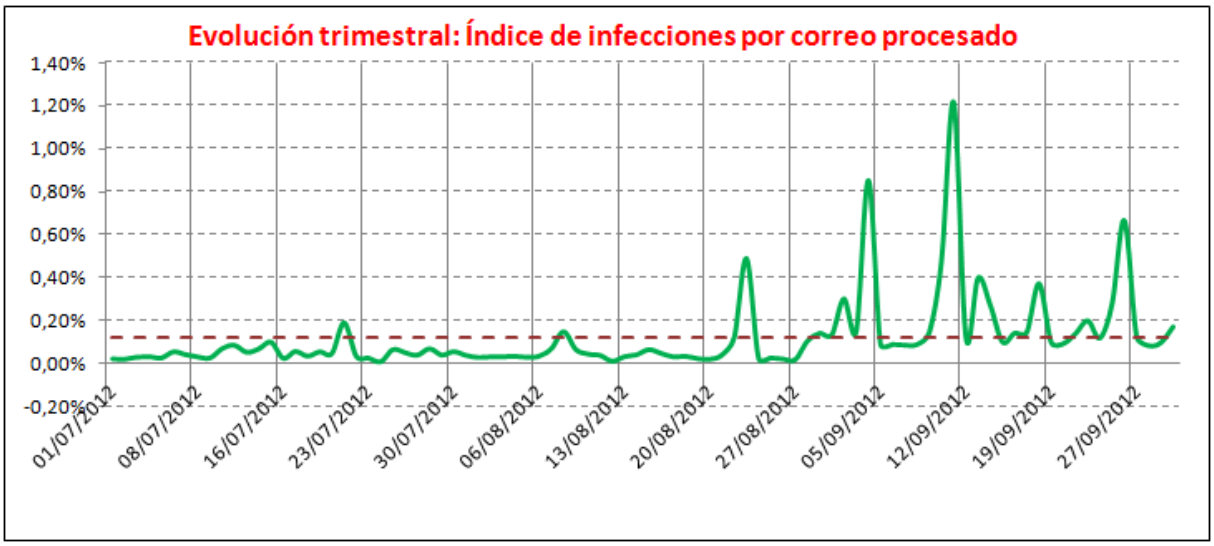

Figura 4: Evolución trimestral del índice de infecciones por correo procesado.

Como se puede ver, el porcentaje de correos infectados está en torno al **0,12%** de los correos recibidos (12 infecciones por cada 10000 correos).

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

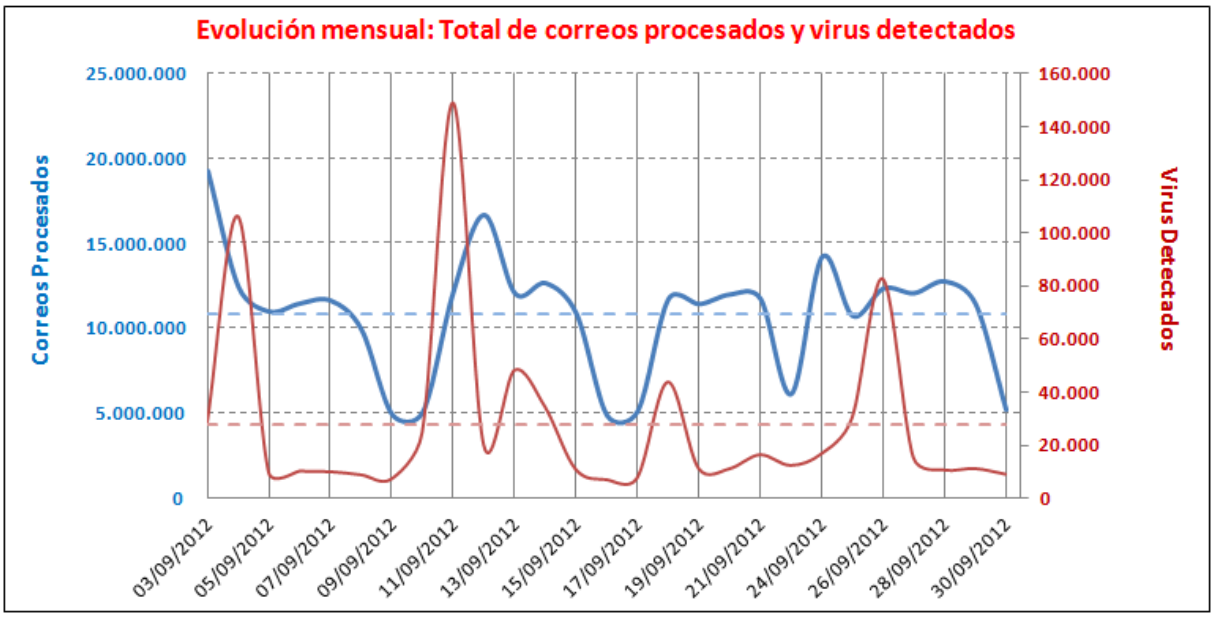

Figura 5: Evolución mensual de correos procesados y virus detectados.

A continuación se muestra la aportación al volumen de correos procesados de los diferentes sectores de actividad durante el mes de **Septiembre**.

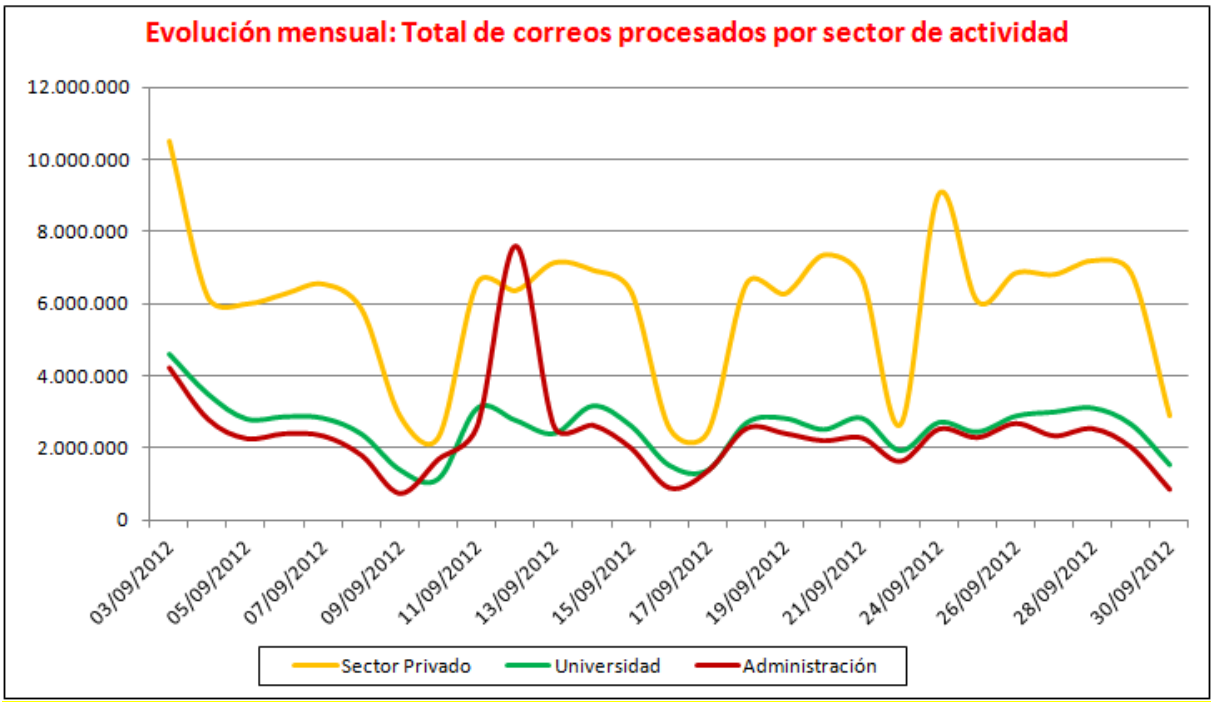

Figura 6: Evolución mensual de correos procesados por sector de actividad.

Puede apreciarse que el sector de actividad "Sector privado" que constituye aproximadamente el 38% de los Sensores, es el sector que procesa más cantidad de mensajes (más del 54% 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 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 **Septiembre**.

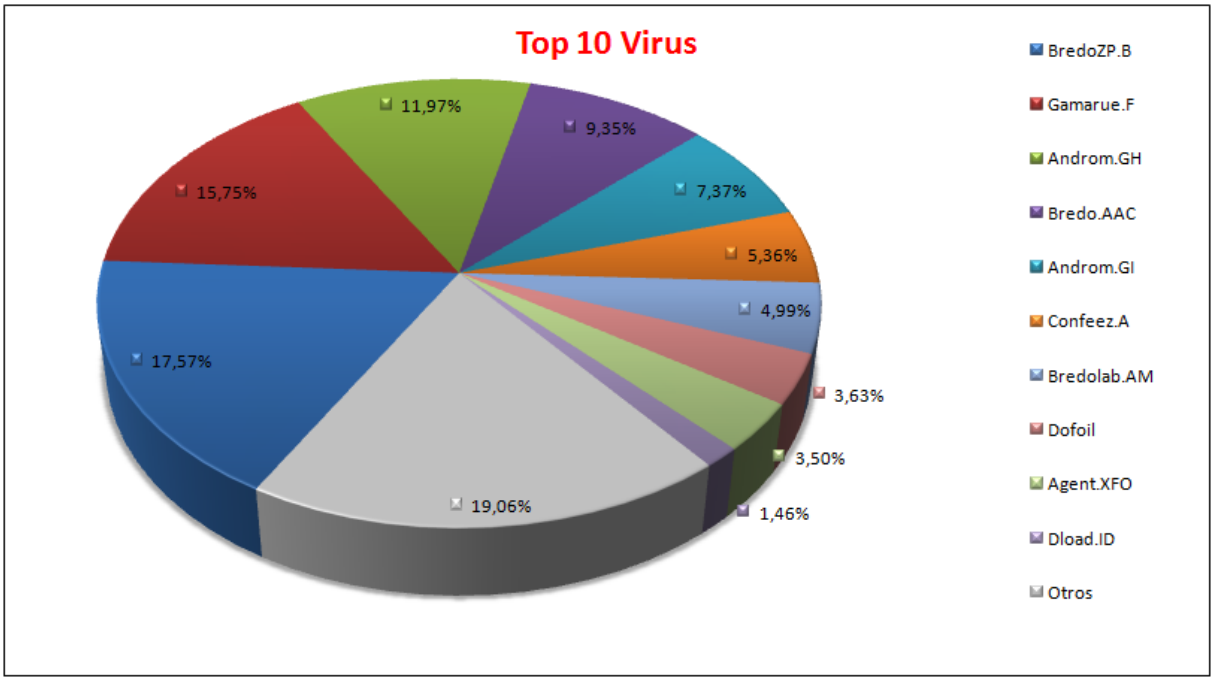

Figura 7: Virus más activos en la red de sensores durante el mes.

Este mes el reparto de virus activos ha sido mucho más equilibrado que otros meses, no llegando ningún virus a producir más del 20% de las infecciones detectadas. El más activo ha sido ha sido *BredoZP.B* con un 17,57% del total de virus detectados en la Red de Sensores. Le sigue *Gamarue.F*, con un 15,75% y *Androm.GH* con un 11,97%.

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.

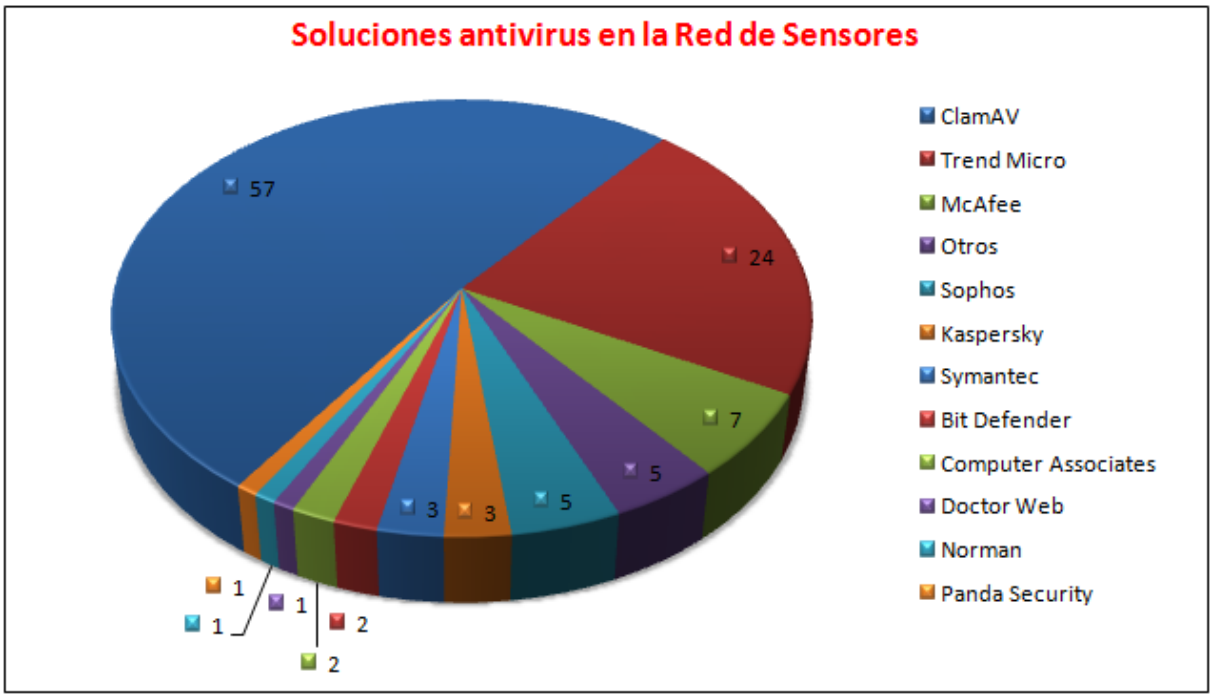

Figura 8: Antivirus utilizados en los sensores.

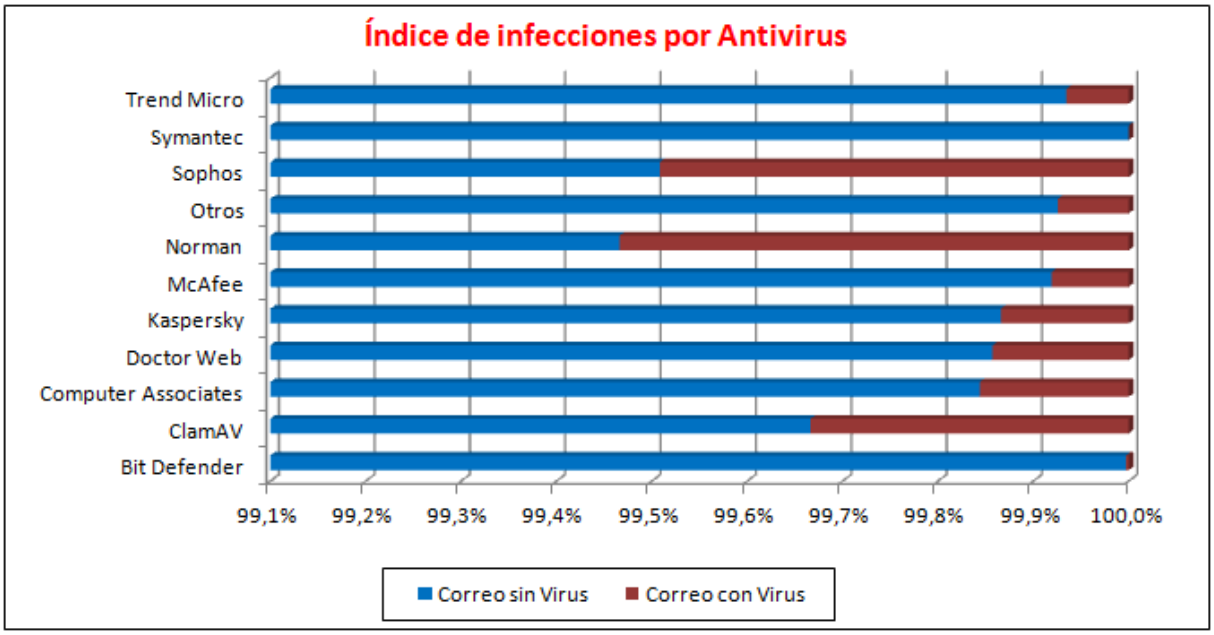

Figura 9: Relación correos analizados sin virus/correos con virus detectado por antivirus.

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.

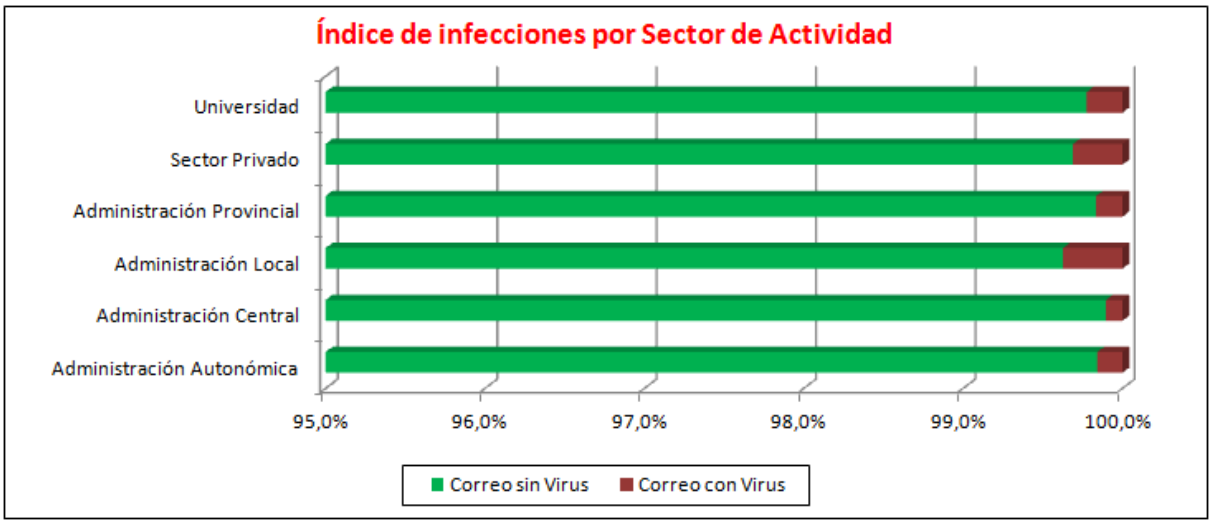

Figura 10: Porcentaje de correos sin virus frente a correos con virus detectados por sectores de actividad.

El siguiente gráfico 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.

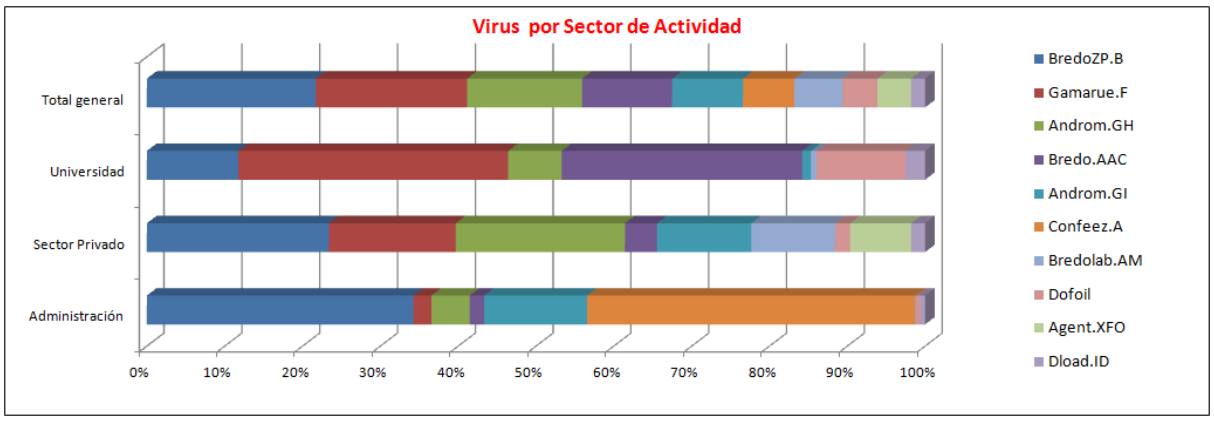

Figura 11: Top virus por sectores de actividad.

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

Virus	Administración	Sector Privado	Universidad	Total general
BredoZP.B	30,79%,	20,86%,	10,81%,	19,56%,
Gamarue.F	2,07%,	14,52%,	31,95%,	17,53%,
Androm.GH	4,43%,	19,41%,	6,34%,	13,33%,
Bredo.AAC	1,65%,	3,66%,	28,47%,	10,41%,
Androm.GI	11,9%,	10,82%,	1,03%,	8,2%,
Confeez.A	37,93%,	0%,	0%,	5,96%,
Bredolab.AM	0,11%,	9,6%,	0,67%,	5,56%,
Dofoil	0,44%,	1,73%,	10,54%,	4,04%,
Agent.XFO	0%,	6,98%,	0%,	3,9%,
Dload.ID	0,54%,	1,59%,	2,3%,	1,63%,
Otros	10,14%,	10,82%,	7,88%,	9,87%,

Figura 12: Tabla de virus más detectados por sectores.

Como se puede ver, en cada uno de los ámbitos principales de la Red de Sensores, el virus más activo es diferente. Mientras que en la administración el virus más activo es *Confeez.A*, en el sector privado, los que más han afectado han sido *BredoZP.B* y *Androm.GH* y en el ámbito universitario ha sido *Gamarue.F* el más peligroso.

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 **Septiembre**.

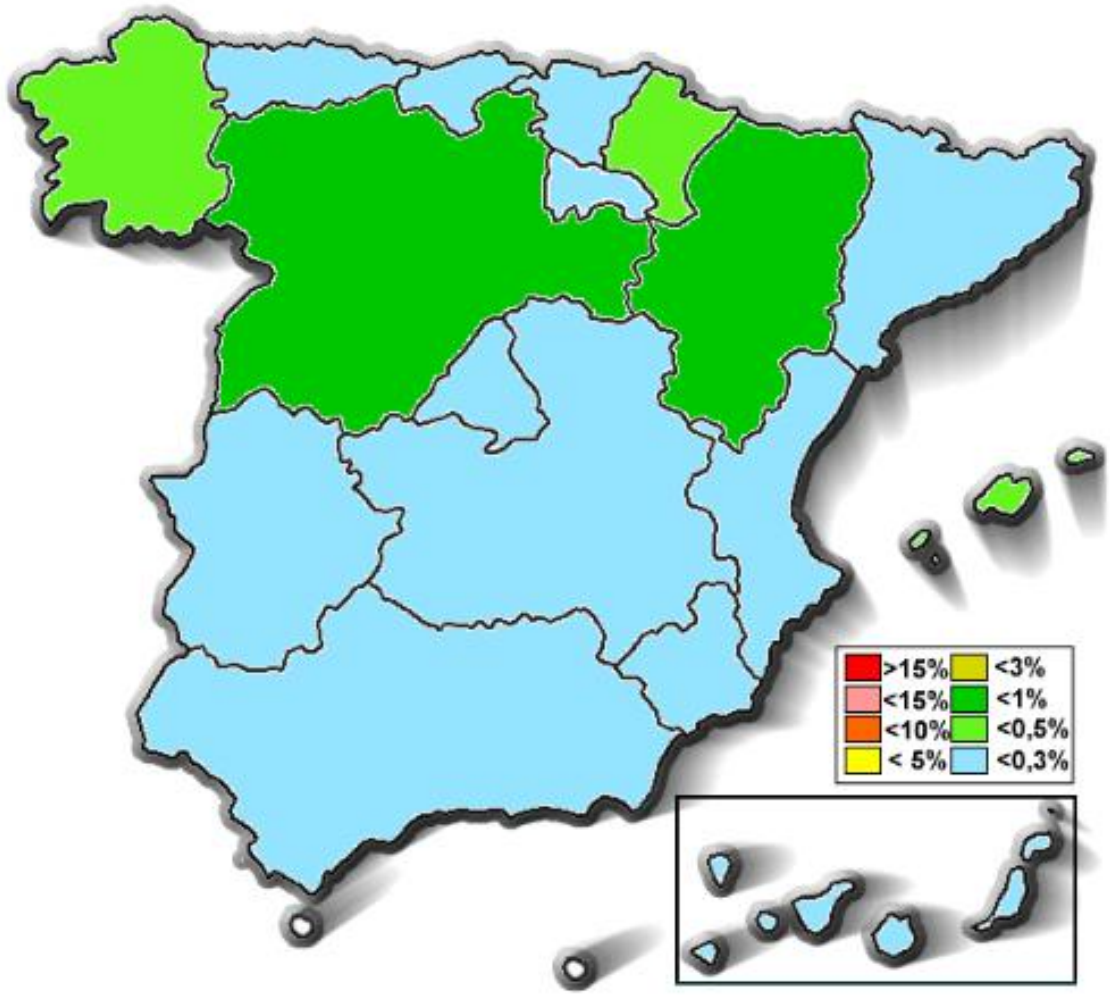

Figura 13: Mapa autonómico de detecciones de virus.

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	27.442.362	0,13%
Aragón	11.961.219	0,83%
Canarias	1.014.016	0,02%
Cantabria	816.923	0,0%
Castilla y León	1.719.438	0,74%
Castilla-La Mancha	17.120.431	0,06%
Catalunya / Cataluña	32.450.960	0,09%
Ciudad Autónoma de Ceuta	0	0,0%
Ciudad Autónoma de Melilla	0	0,0%
Comunidad Foral de Navarra	2.731.909	0,49%
Comunidad de Madrid	10.661.224	0,07%
Comunitat Valenciana / Comunidad Valenciana	18.856.001	0,19%
Euskadi / País Vasco	1.255.805	0,05%
Extremadura	94.050	0,05%
Galicia / Galicia	33.619.442	0,34%
Illes Balears / Islas Baleares	101.944	0,47%
La Rioja	0	0,0%
Principado de Asturias	23.700.815	0,0%
Región de Murcia	3.800.628	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, es **Galicia** la comunidad que más muestras aporta a la red de Sensores y la que tiene número total de infecciones más elevado (Unas 110.000), mientras que **Aragón** es la comunidad que más infecciones reporta en porcentaje (0,83%).

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 sobre el SPAM 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.

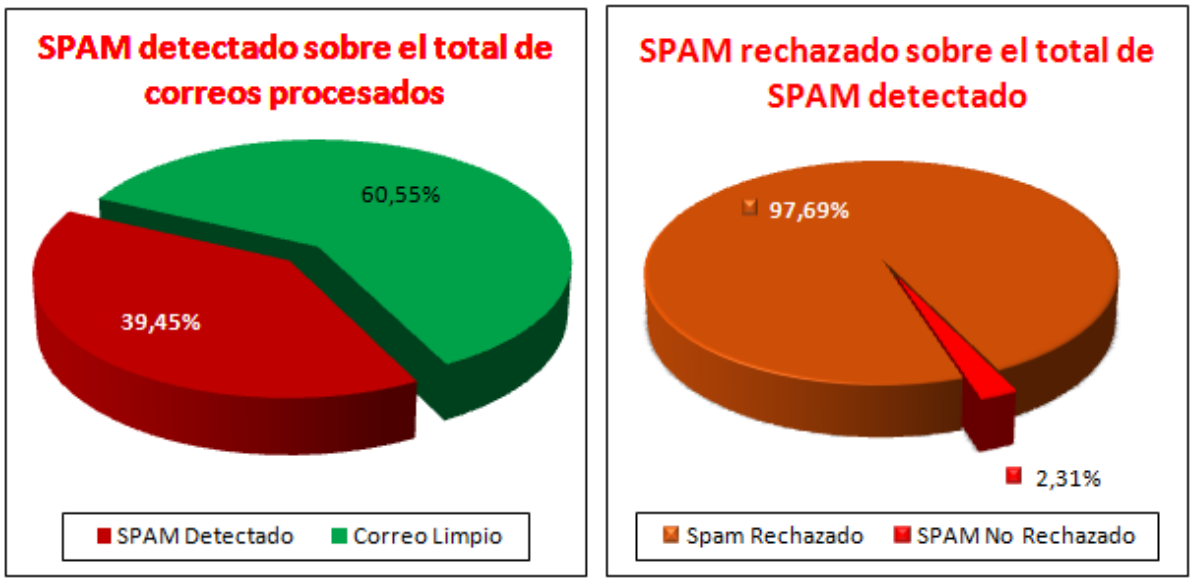

Figura 15: Nivel de SPAM detectado por la red de sensores.

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 **Septiembre**, el nivel de SPAM en correo fue de un **39,45%** 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 de un periodo de tiempo dividido en intervalos, de un día en este caso.

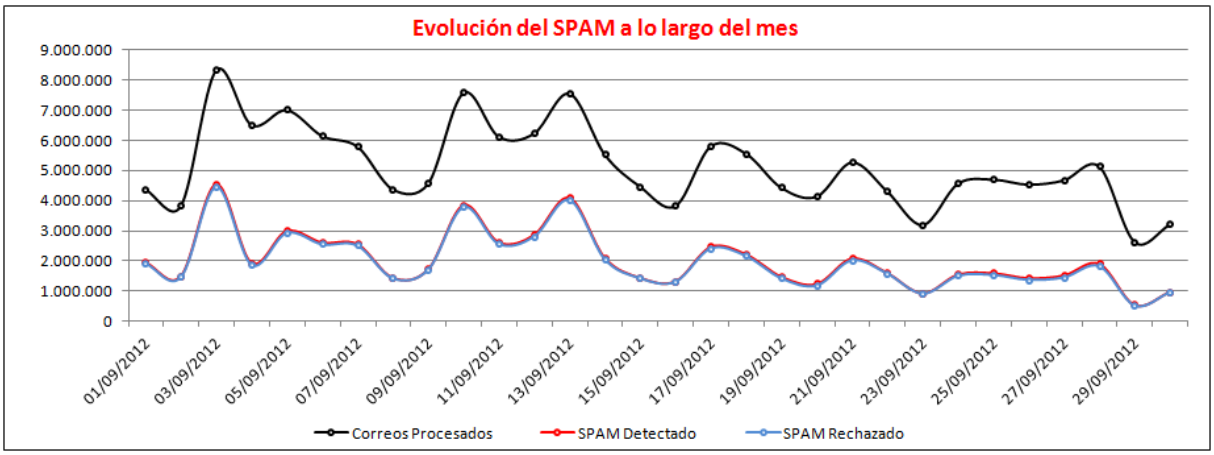

Figura 16: Evolución temporal del SPAM detectado por la red de sensores.

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 ha reducido ligeramente a lo largo del último año.

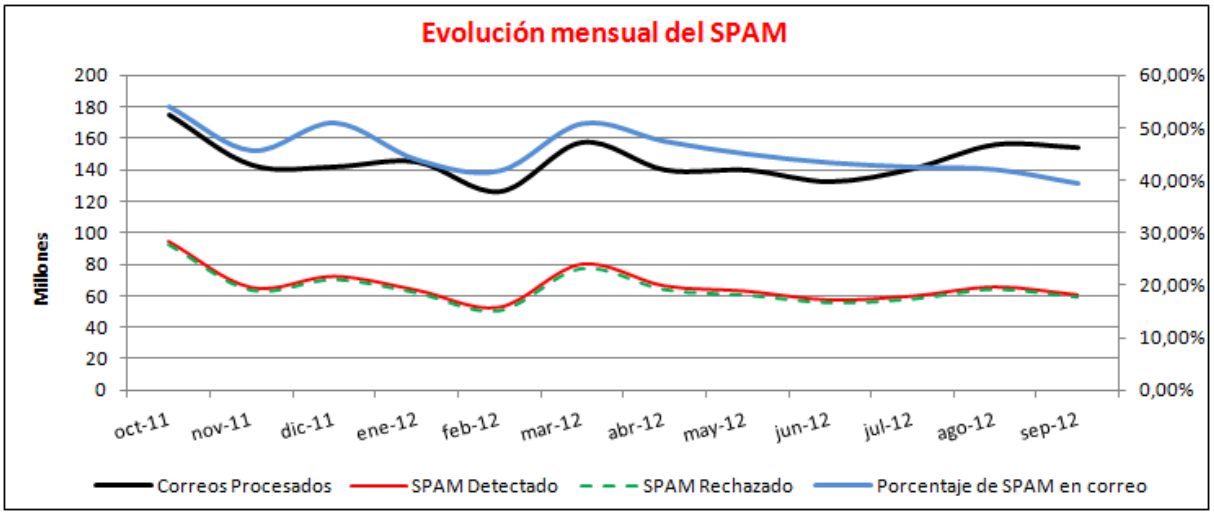

Figura 17: Evolución mensual del SPAM a lo largo del año.

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.

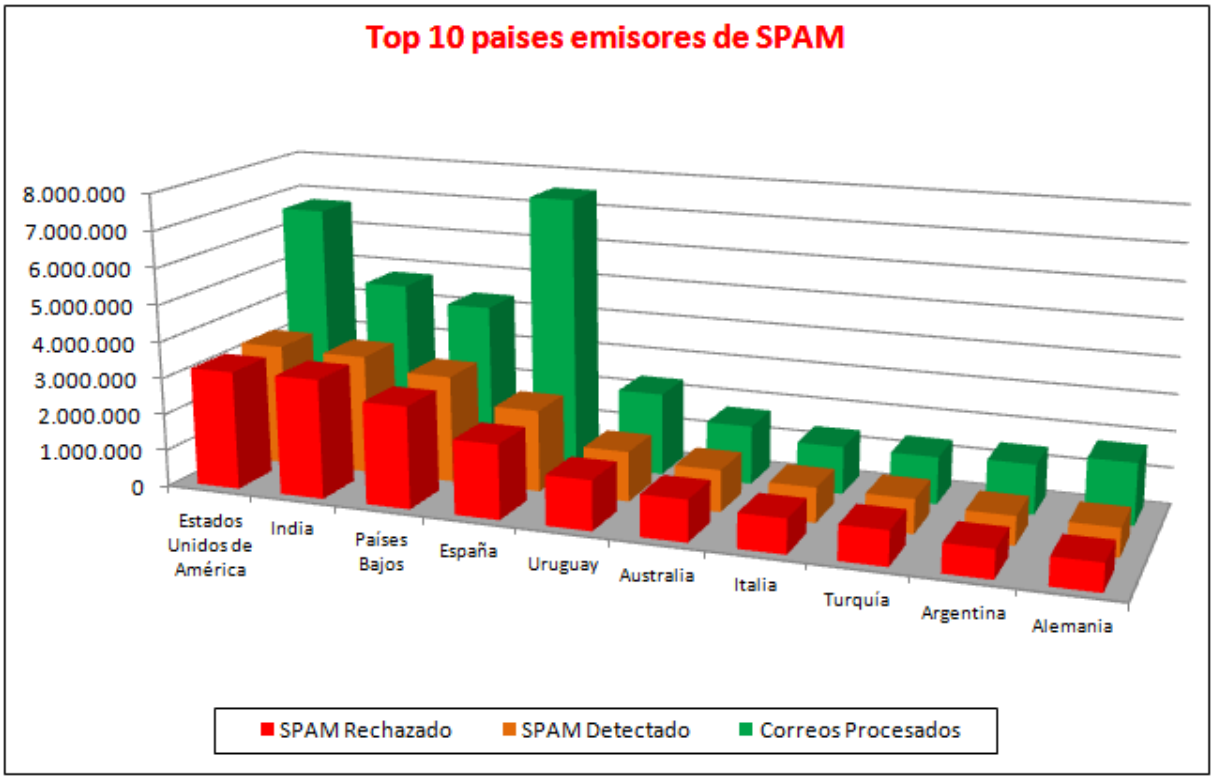

Figura 18: Top 10 países emisores de SPAM según datos recogidos por la RSI.

Se puede comprobar que, a lo largo del último mes, los países que más SPAM han mandado a direcciones de correo españolas han sido **Estados Unidos, India** y **Países Bajos**.

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 **Septiembre**.

A lo largo del pasado mes se emitieron un total de **670** vulnerabilidades, con un nivel de severidad mayoritariamente de nivel **medio y alto**. Los niveles de severidad de las vulnerabilidades publicadas aparecen en la siguiente figura.

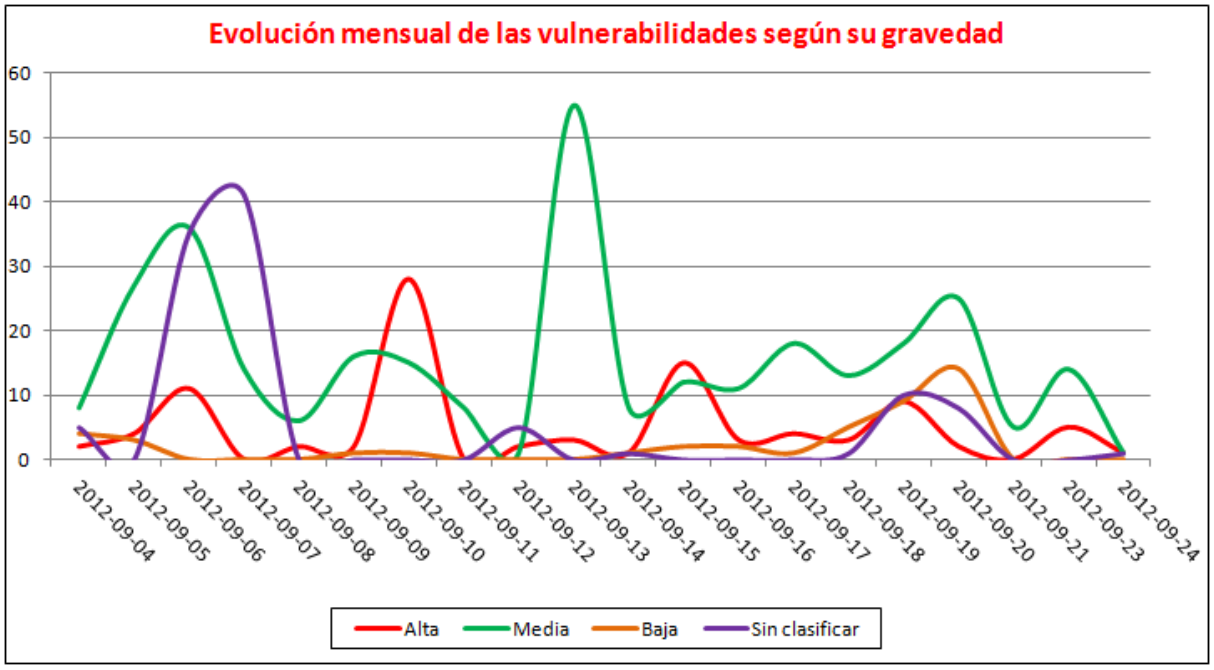

Figura 19: Vulnerabilidades emitidas por nivel de riesgo.

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.

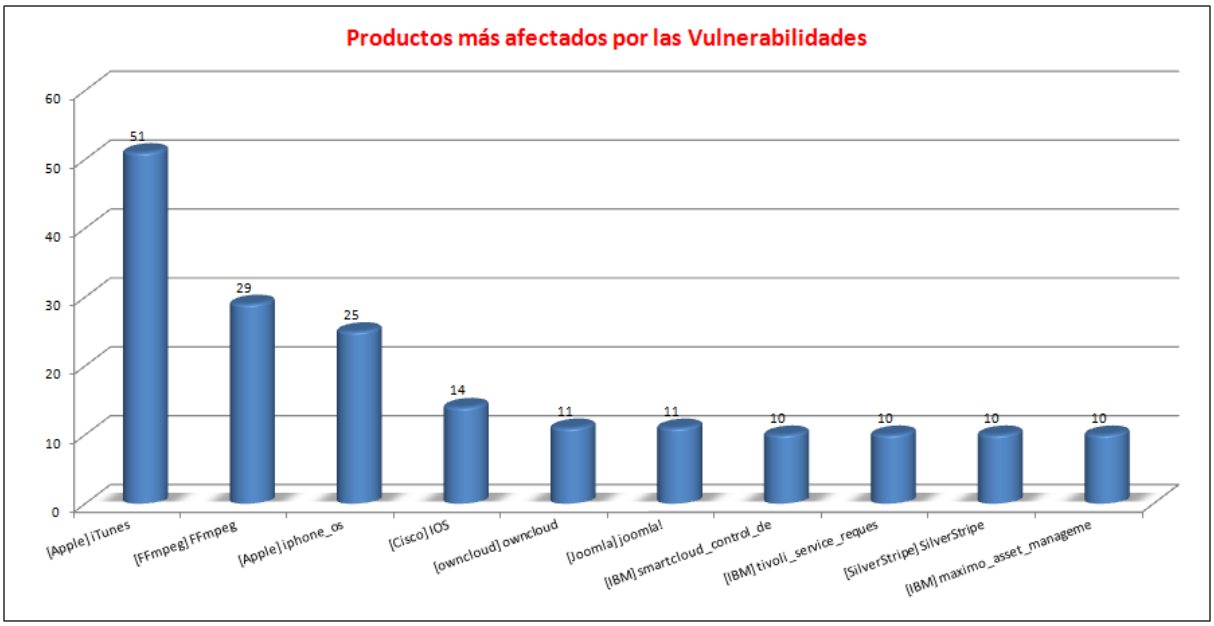

Figura 20: Productos más afectados por las últimas vulnerabilidades.

4.1.3. Fabricantes más afectados

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

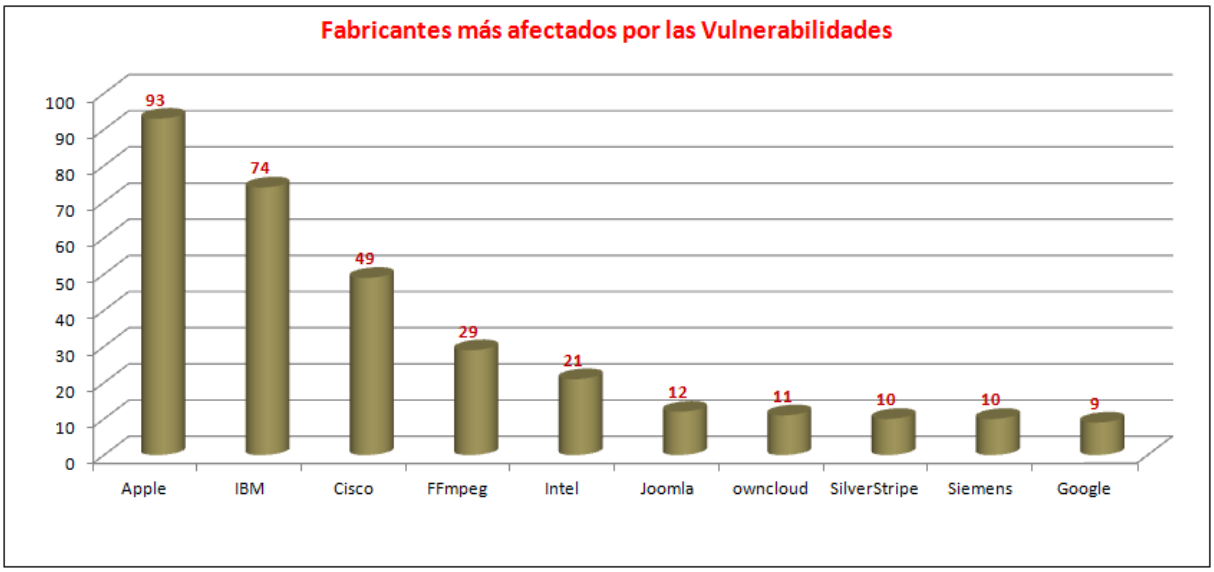

Figura 21: Fabricantes más afectados por las últimas vulnerabilidades.

4.1.4. Vulnerabilidades más comunes según su tipo

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

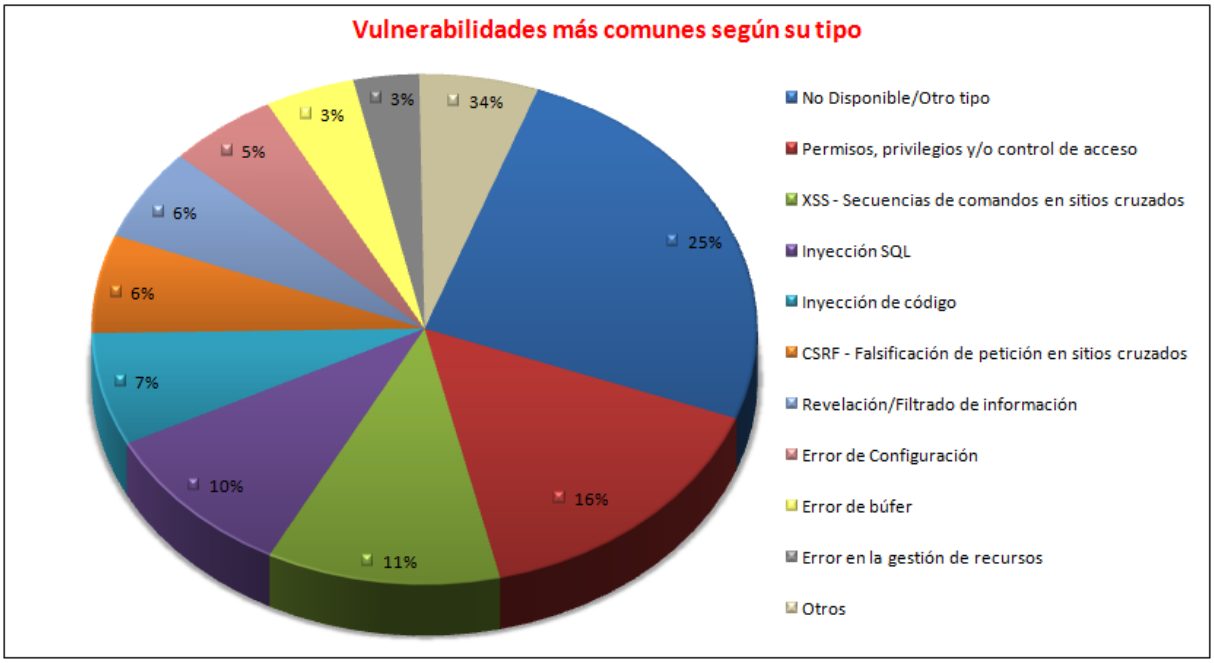

Figura 22: Vulnerabilidades más comunes por tipo.

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
Octubre 2011	822	**Abril 2012**	618
Noviembre 2011	1069	**Mayo 2012**	723
Diciembre 2011	768	**Junio 2012**	1002
Enero 2012	744	**Julio 2012**	723

Febrero 2012	518	**Agosto 2012**	874
Marzo 2012	732	**Septiembre 2012**	969

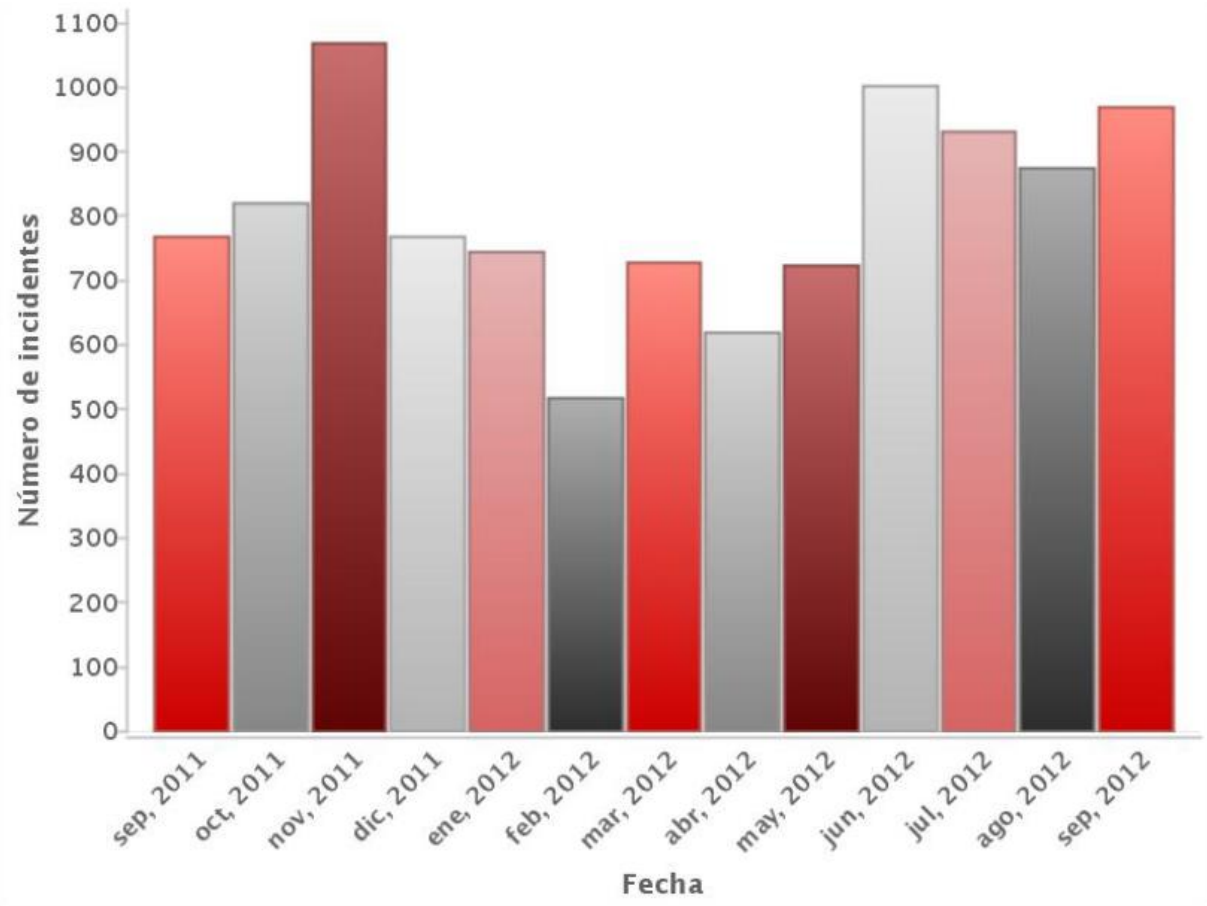

Figura 23: Evolución del número de incidentes de Fraude.

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.

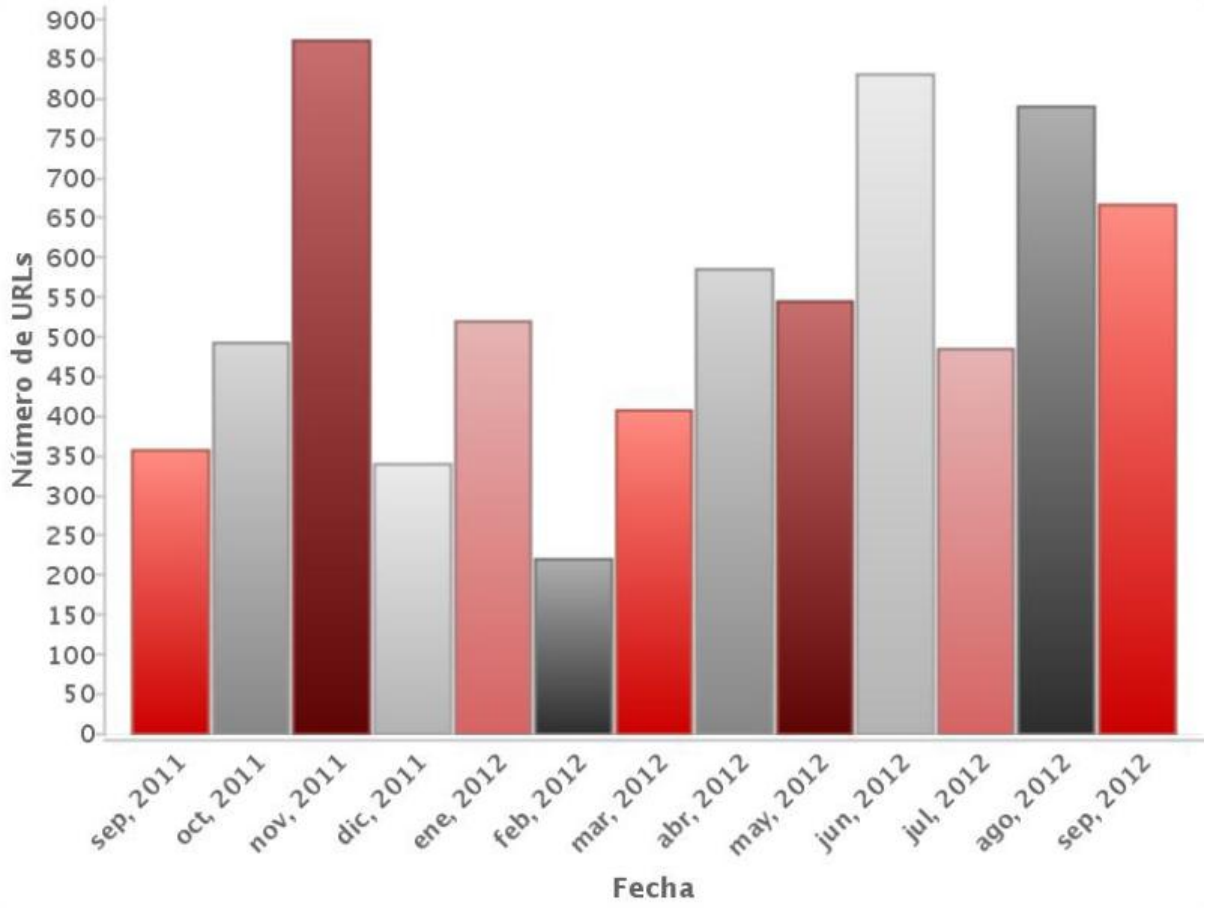

Figura 24: Evolución del número de URLs fraudulentas.

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

Mes	URLs fraudulentas	Mes	URLs fraudulentas
Octubre 2011	492	**Abril 2012**	585
Noviembre 2011	873	**Mayo 2012**	541
Diciembre 2011	339	**Junio 2012**	831
Enero 2012	519	**Julio 2012**	542
Febrero 2012	221	**Agosto 2012**	793
Marzo 2012	403	**Septiembre 2012**	666

4.3. AVISOS TECNICOS Y NO TÉCNICOS PUBLICADOS

A lo largo del mes de **Septiembre**, INTECO publicó los siguientes avisos técnicos:

Aviso de Seguridad	Fecha
Ataques USSD contra terminales móviles http://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/ataques_ussd_contra_terminales_moviles_20120927	27/09/2012
Alertan de una vulnerabilidad grave en Java http://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/alertan_vulnerabilidad_grave_java_20120926	26/09/2012
Microsoft publica la actualización de seguridad para la vulnerabilidad 0-day http://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/microsoft_publica_actualizacion_seguridad_vulnerabilidad_0day_20120922	22/09/2012
Apple publica IOS 6 https://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_no_tecnicos/apple_publica_ios_6_20120920	20/09/2012
Mensaje falso de advertencia de privacidad en Facebook https://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_no_tecnicos/mensaje_falso_advertencia_privacidad_facebook_20120917	17/09/2012
0day en Internet Explorer http://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/0day_internet_explorer_20120917	17/09/2012
Actualización de seguridad 2.5.7 de Joomla! https://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/actualizacion_seguridad_257_joomla_20120914	14/09/2012
Boletines de seguridad de Microsoft de Septiembre 2012 http://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/boletines_seguridad_microsoft_septiembre_2012_20120912	12/09/2012
Actualización de seguridad 3.4.2 de WordPress http://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/actualizacio	11/09/2012

n_seguridad_342_wordpress_20120911	
Actualización de Java 1.6.0_35 para Mac OS X https://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/actualizacion_java_160_35_mac_x_20120906	06/09/2012

4.4. EVENTOS DEL MES (SEPTIEMBRE Y OCTUBRE)

4.4.1. Cloud Day

"Cloud Day, un rayo de sol entre las nubes" pretende acercar a las empresas catalanas los pasos a seguir para enfocar su migración al cloud desde varios puntos de vista: estratégico o de negocio, técnico y legal. Todo ello con el objetivo de que los asistentes puedan orientarse a la hora de plantear el uso del cloud en sus empresas y beneficiarse de las ventajas competitivas que éste ofrece.

El evento tendrá lugar el 4 de octubre de 2012 en el Palacio de Congresos de Cataluña (Barcelona) a partir de las 9.30h.

- Fecha: 4 de Octubre de 2012
- Lugar: Barcelona
- Precio: Gratuito
- Más información: http://www.amiando.com/Cloud_day_barcelona.html?page=833507

4.4.2. Gestión de la Seguridad de la Información con acreditación de Lead Auditor ISO 27001 (Certificación IRCA)

Curso, de modalidad online y presencial, que pretende dar a conocer los conceptos, estándares, normativa, regulación y buenas prácticas de uso más extendido en la gestión de la seguridad de la información, así como permitir a los asistentes superar el curso Lead Auditor y obtener la certificación IRCA.

Dirigido a personas que ocupan cargos de alta responsabilidad en las Organizaciones, profesionales TIC y para todos aquellos que se planteen [re]orientar su actividad profesional hacia los sectores de Auditoría | Consultoría de la Seguridad de la Información (especialmente recomendable para personas con formación/conocimientos en TIC's, Derecho y Gestión Empresarial).

El curso cuenta con una parte online (del 15/10/2012 al 25/11/2012) y una presencial (del 26/11/2012 al 30/11/2012).

- Fecha: 15 de Octubre al 30 de Noviembre de 2012
- Lugar: Online salvo la semana 26-11 al 30-11 en Madrid
- Precio: 1300€
- Más información: https://srvoei.eui.upm.es/web/sgs/panele_curso_sgs.pdf

4.4.3. Respuestas SIC. Del SIEM al BIG DATA de seguridad

En este Respuestas SIC se tratará de fijar el estado del arte del big data orientado a la seguridad y la mejor forma para ir enfocándose hacia su creación, al tiempo que se expondrán algunas alternativas tecnológicas de mercado y las opiniones de expertos de corporaciones usuarias.

El contenido del evento se estructurará, como viene siendo habitual, en base a su formato de tres bloques. En el primero, un especialista en protección de la información tratada en sistemas tecnológicos ofrecerá su visión sobre este asunto. En el segundo, cuatro compañías con foco en la prestación de tecnologías, y soluciones y servicios de seguridad TIC explicarán sus orientaciones, ya sean acotadas para ámbitos específicos ya genéricas, en la materia. El tercer bloque contará con la participación de dos grandes organizaciones usuarias, quienes expondrán sus experiencias y valoración a futuro de esta tendencia emergente.

- Fecha: 16 de Octubre de 2012
- Lugar: Hotel Novotel Barcelona City. Barcelona
- Precio: A consultar
- Más información: http://www.revistasic.com/respuestassic

4.4.4. I Congreso Smart Grids

El I Congreso Smart Grids, será, por una parte, un foro de reflexión para analizar las redes inteligentes, su posible desarrollo y las estrategias para abordarlo. Por otra parte el Congreso servirá de intercambio de ideas y opiniones entre todos los agentes implicados, grupos de investigación y empresas, fomentando el debate entre los distintos expertos participantes en las conferencias magistrales, mesas redondas y sesiones de ponencias que ayudarán a conocer mejor los aspectos claves relativos a las Smart Grids (redes inteligentes).

- Fecha: 22-23 de Octubre de 2012
- Lugar: Madrid
- Precio: A consultar
- Más información: http://congreso-smartgrids.es/

4.4.5. 6ENISE

Un año más, INTECO pone en marcha ENISE, el Encuentro Internacional de Seguridad de la Información. Esta sexta edición se desarrolla bajo una coyuntura de cambios y oportunidades en los ambientes tecnológicos y de investigación. Cuando las TIC juegan un papel condicionante, dependiente y ya intrínseco a nuestra sociedad, se intuye necesario favorecer su evolución con todas las garantías, y por tanto, con seguridad. Por eso, este año entramos de lleno en la dimensión del ciberespacio y bajo el lema: «La Ciberseguridad: un elemento clave para el futuro de nuestra sociedad».

El desarrollo de las Tecnologías de la Información y las Comunicaciones (TIC) ha generado un nuevo espacio de relación en el que la rapidez y facilidad de los intercambios han eliminado las barreras de espacio y tiempo. El ciberespacio, como entorno global constituido por los sistemas de información, las redes, la información y los servicios, ha venido a difuminar fronteras, haciendo partícipes a sus usuarios de una globalización sin precedentes que propicia nuevas oportunidades, al tiempo que comporta nuevos riesgos, retos y amenazas. Una adecuada estrategia que de respuesta a estos riesgos y amenazas se constituye como elemento esencial de la seguridad nacional.

- Fecha: 23-24 de Octubre de 2012
- Lugar: León
- Precio: A consultar
- Más información: https://enise.inteco.es

4.4.6. No cON Name

Este evento de periodicidad anual reune tanto a nuevas promesas del sector y expertos, como a profesionales en el campo de la informática en general, redes telemáticas, programación o ingeniería de protección de software. La meta del congreso es el intercambio para la actualización del conocimiento con la finalidad de estimular una industria puntera en seguridad informática y de la información.

- Fecha: 02-03 de Noviembre de 2012
- Lugar: CosmoCaixa Barcelona
- Precio: 40-120€
- Más información: https://www.noconname.org/

4.4.7. ISF 23rd Annual World Congress

El 23er congreso annual del ISF se realizará en Chicago, EEUU, entre el 4 y el 6 de Noviembre de 2012 (con “Academy day” opcional el 3 de Noviembre). El congreso ofrece una perfecta oportunidad para los miembros para escuchar a expertos de reconocimiento mundial, encontrar solucionaes a los problemas actuales de Seguridad, aprenderfind solutions to current security problems, aprender de los actores claves de la industria, adquirir una visión interna de los últimos proyectos del ISF y compartir experiencias e interconectarse con todos los asistentes.

- Fecha: 04-06 de Noviembre de 2012
- Lugar: ISF - Information Security Forum
- Precio: Consultar
- Más información: https://www.securityforum.org/?page=publiccongress

4.4.8. 2012 Global Enterprise Mobility Forum: Experience a world where everything intelligently cooperate

Análisis de las tecnologías móviles en los procesos de negocio y en la potenciación de la productividad. Uno de los aspectos que se analizará será la mejora de la seguridad en la movilidad de la empresa.

- Fecha: 13-14 de Noviembre de 2012
- Lugar: Londres
- Precio: Consultar
- Más información: https://www.gem-forum.com

4.4.9. Jornada Técnica 2012 ISACA Madrid

Jornada Técnica organizada por ISACA Madrid, que se celebrará el 15 de noviembre en horario de 9 a 18.30.

- Fecha: 15 de Noviembre de 2012
- Lugar: Madrid
- Precio: Consultar
- Más información: https://www.isacamadrid.es

4.4.10. 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

4.4.11. e-Crime Europe 2012

El "e-Crime Mid Year Meeting Europe" está diseñado para suplir las necesidades de los directivos y tomadores de decisiones que son responsables de gestionar los riesgos del manejo de la información y la tecnología, protegiendo datos sensibles, securizando tecnología y asegurando el cumplimiento de múltiples marcos regulatorios.

- Fecha: 06 de Diciembre de 2012
- Lugar: Amsterdam
- Precio: Consultar
- Más información: http://www.e-crimecongress.org/forumeurope