INFORME MENSUAL

RED DE SENSORES DE INTECO

Red de Sensores de Inteco

Firmado digitalmente por Red de Sensores de Inteco
Nombre de reconocimiento (DN): c=es, st=León, l=León, o=Inteco, ou=eConfianza, cn=Red de Sensores de Inteco, email=gestion.sensores@cert.inteco.es
Fecha: 2012.09.07 16:19:34 +02'00'

Agosto 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 **112 entidades** que albergan al menos un sensor y que están ubicados en diferentes sectores con el porcentaje de distribución que aparece en la figura.

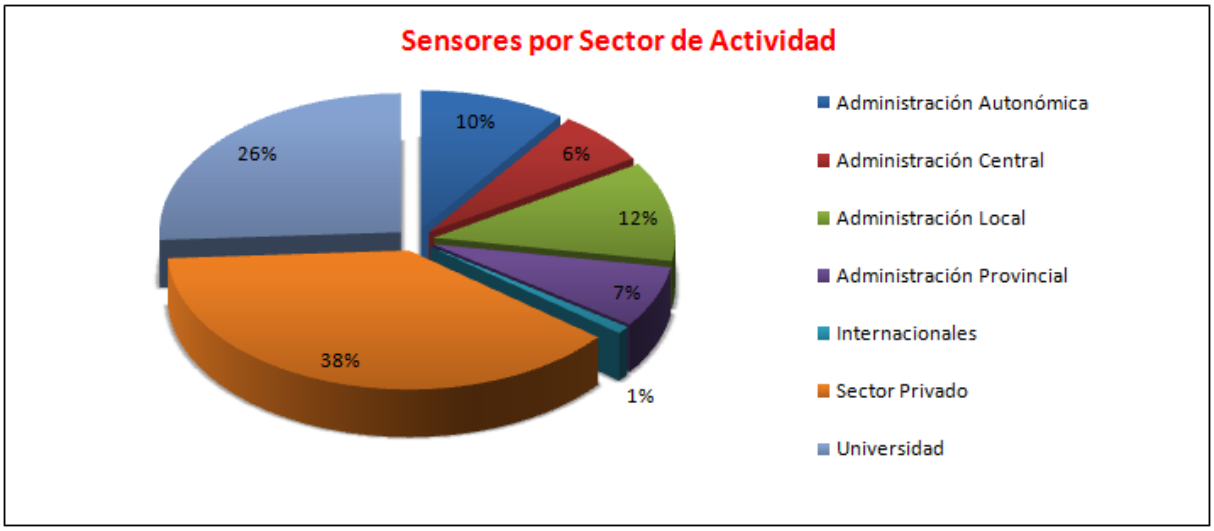

Figura 1: Distribución de los sensores por sector de actividad.

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.

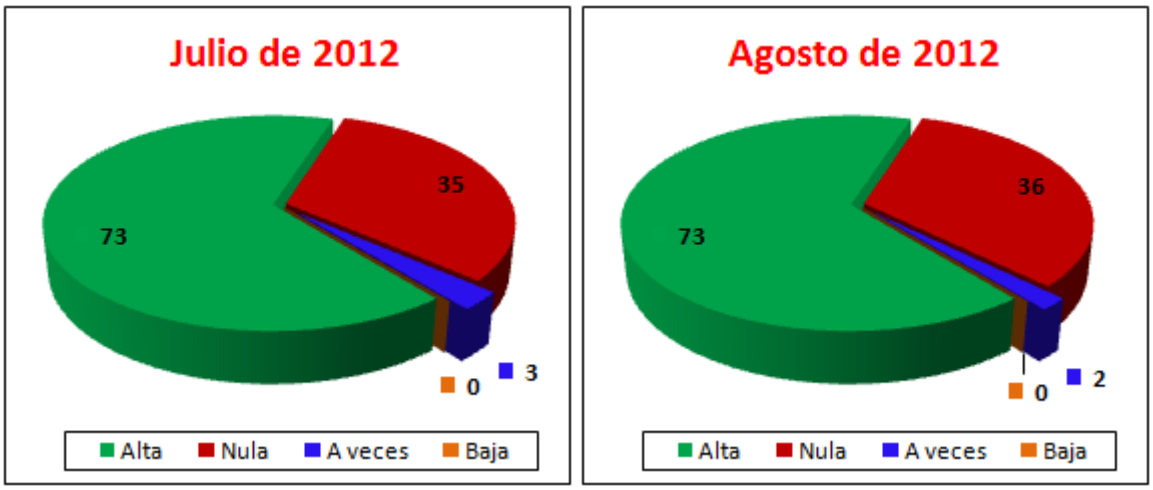

Figura 2: Distribución de sensores según frecuencia en el envío del informe.

A lo largo del mes de **Agosto** no se ha dado de alta ni de baja ningún sensor en la Red de Sensores de INTECO.

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.

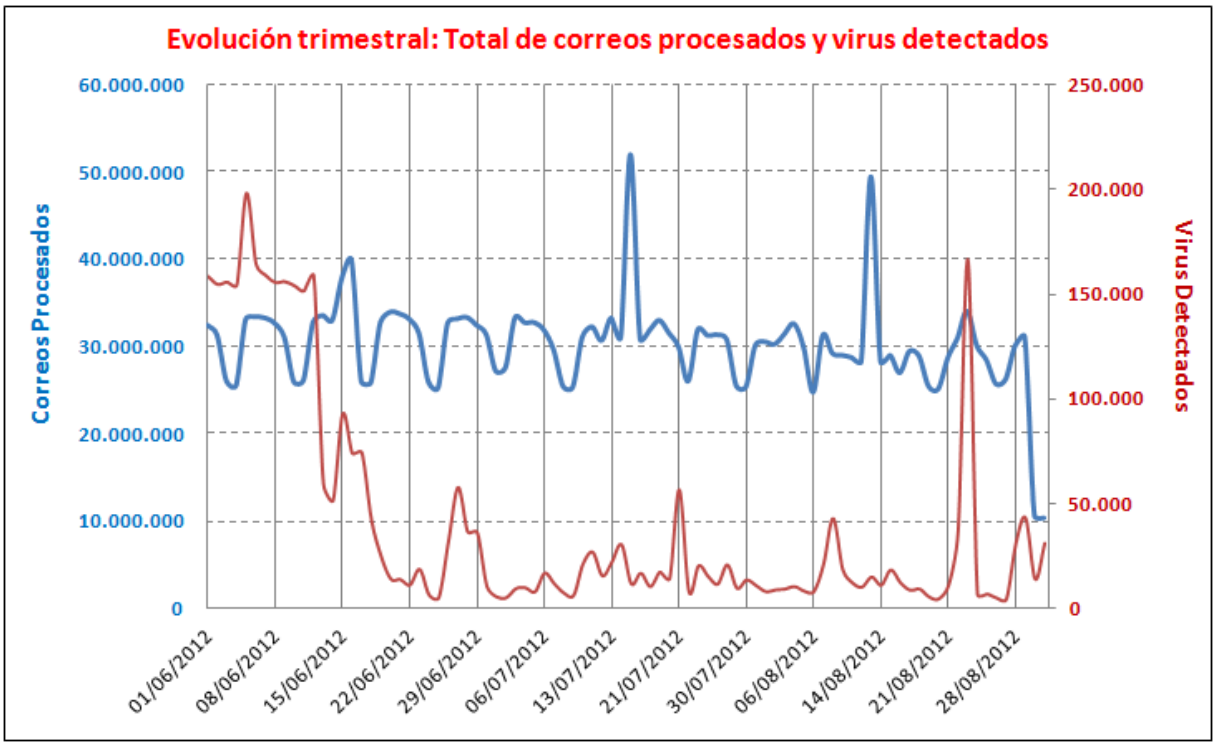

Figura 3: Evolución trimestral de correos procesados y virus detectados.

Como se puede ver desde hasta el 12 de Junio, el número de infecciones diarias encontradas por los sensores de la RSI era 10 veces superior. La razón era aparentemente un ataque dirigido contra algunos de los colaboradores de la Red de Sensores. Dichos colaboradores fueron debidamente informados de este hecho y tomaron las medidas que consideraron oportunas.

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

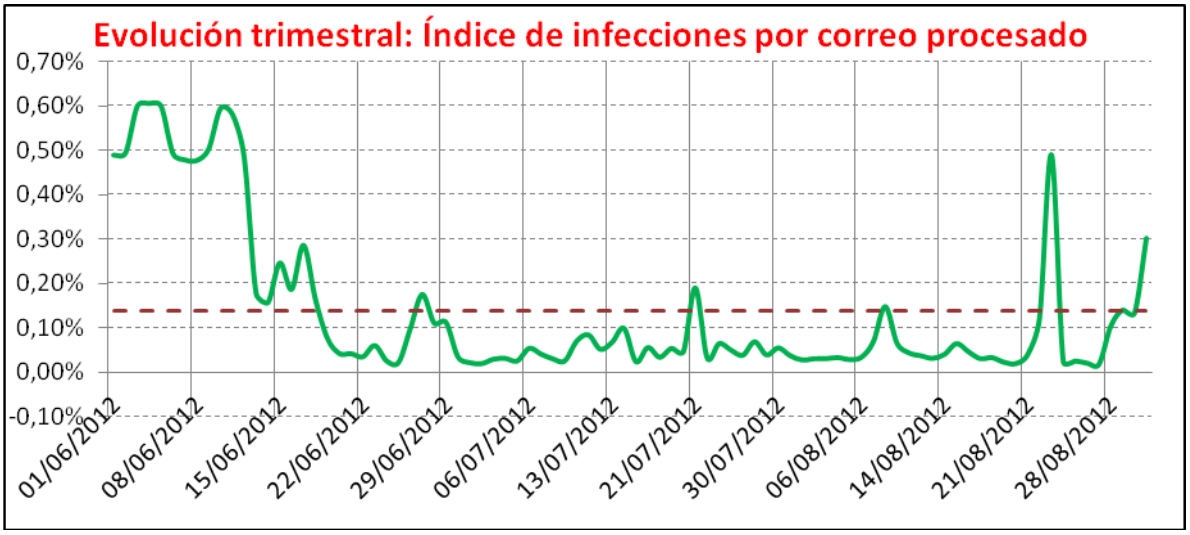

Figura 4: Evolución trimestral del índice de infecciones por correo procesado.

Como se puede ver, el porcentaje de correos infectados está en torno al **0,14%** de los correos recibidos (14 infecciones por cada 10000 correos).

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

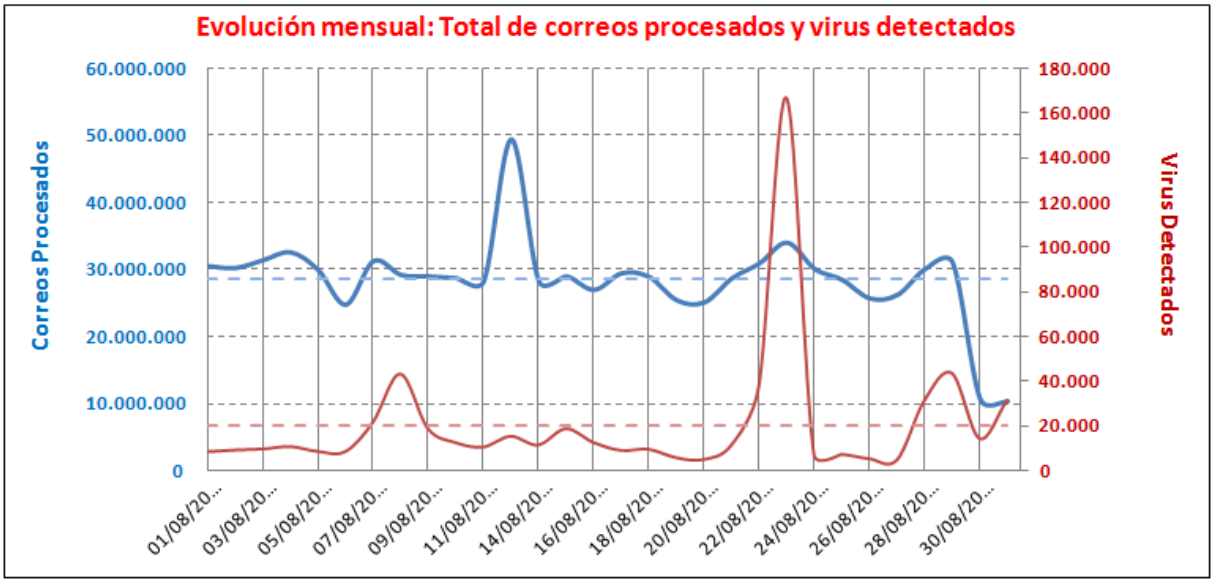

Figura 5: Evolución mensual de correos procesados y virus detectados.

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

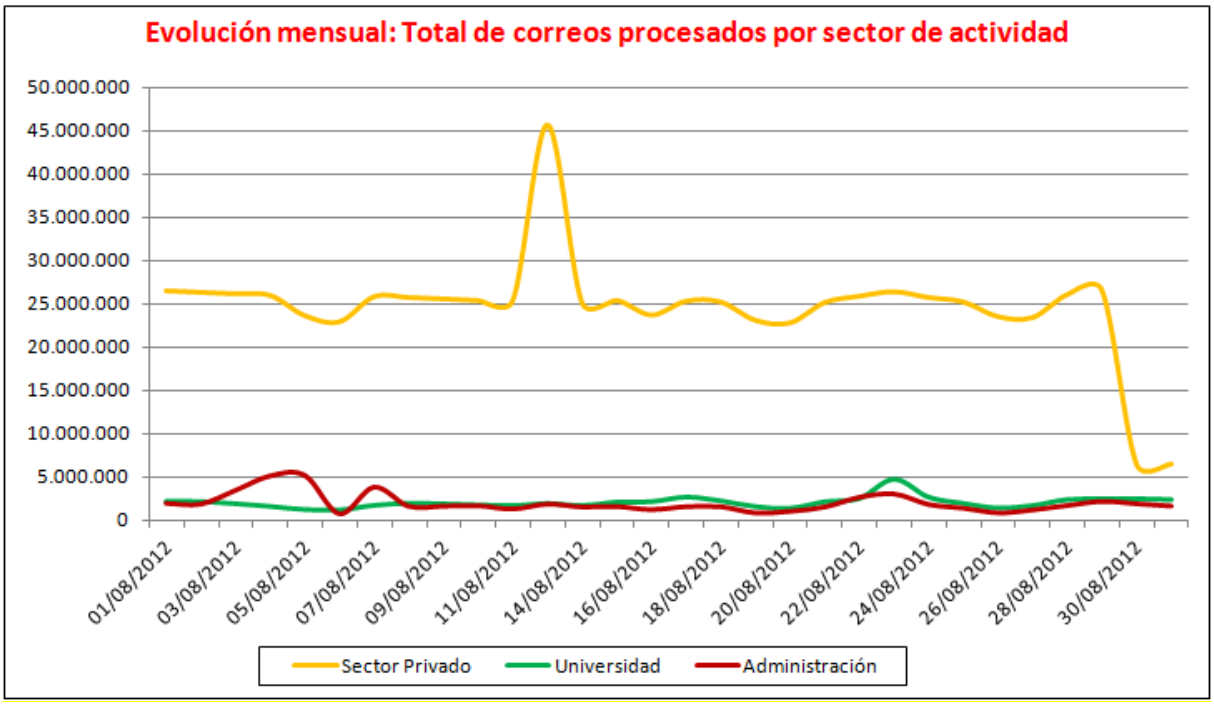

Figura 6: Evolución mensual de correos procesados por sector de actividad.

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 86% 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 **Agosto**.

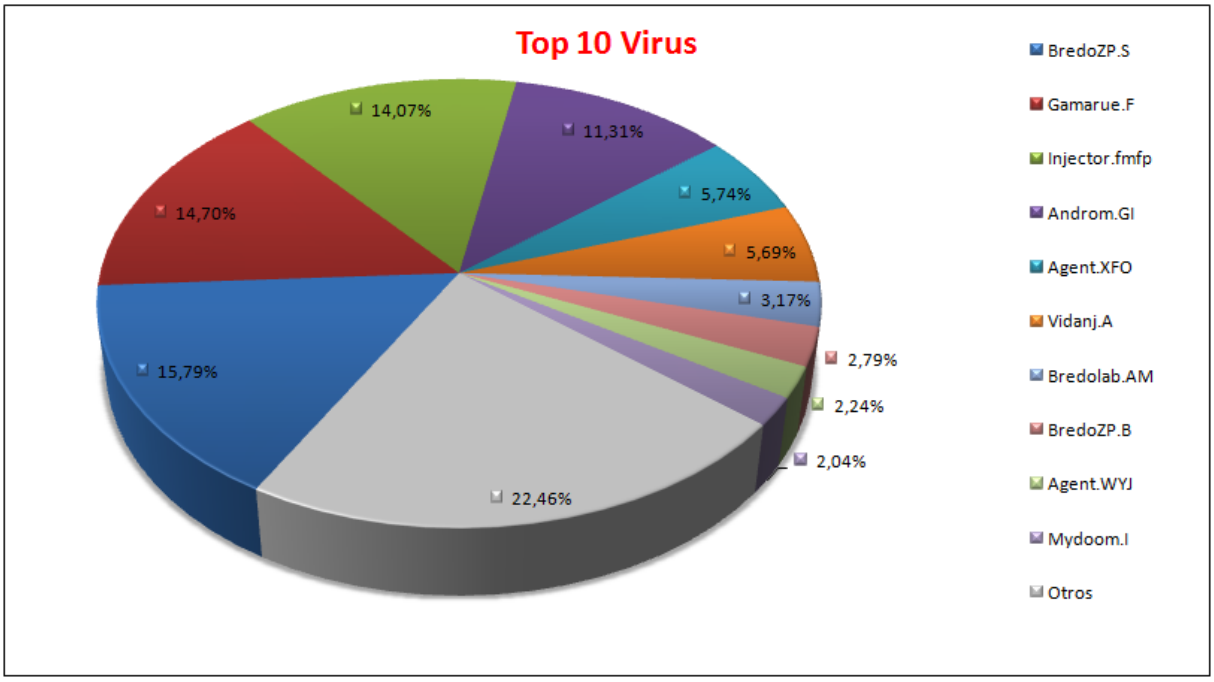

Figura 7: Virus más activos en la red de sensores durante el mes.

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.S* con un 15,79% del total de virus detectados en la Red de Sensores. Le sigue *Gamarue.F*, con un 14,70% y *Injector.FMFP* con un 14,07%.

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.

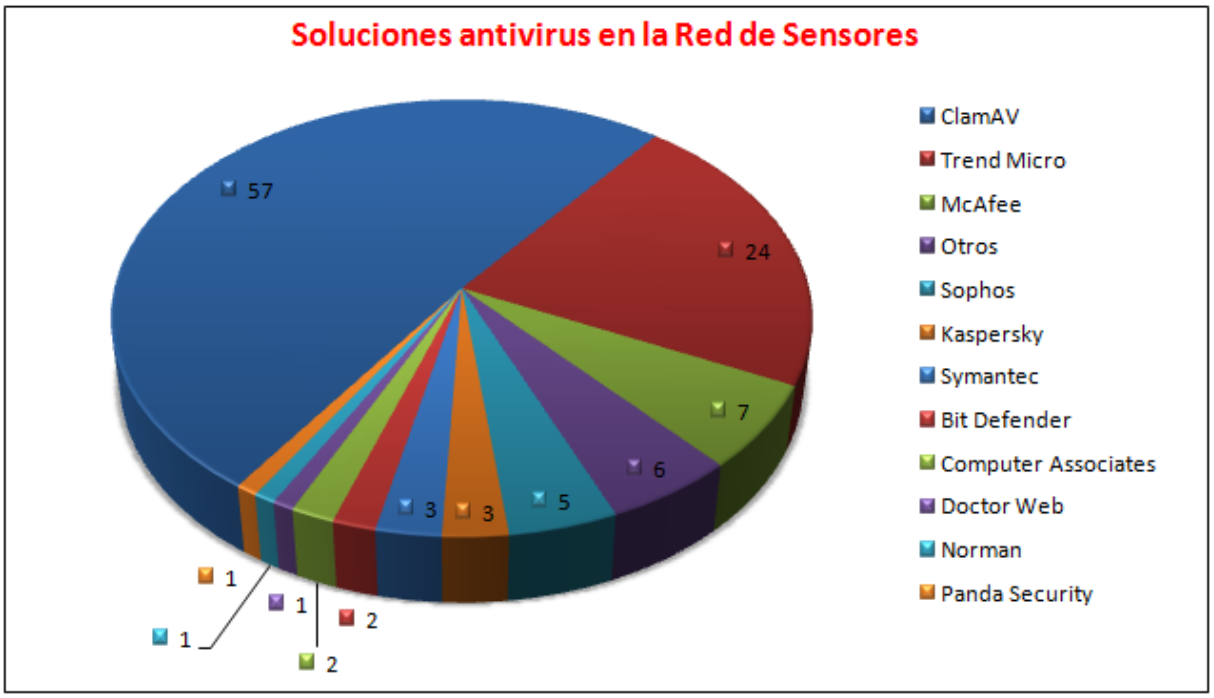

Figura 8: Antivirus utilizados en los sensores.

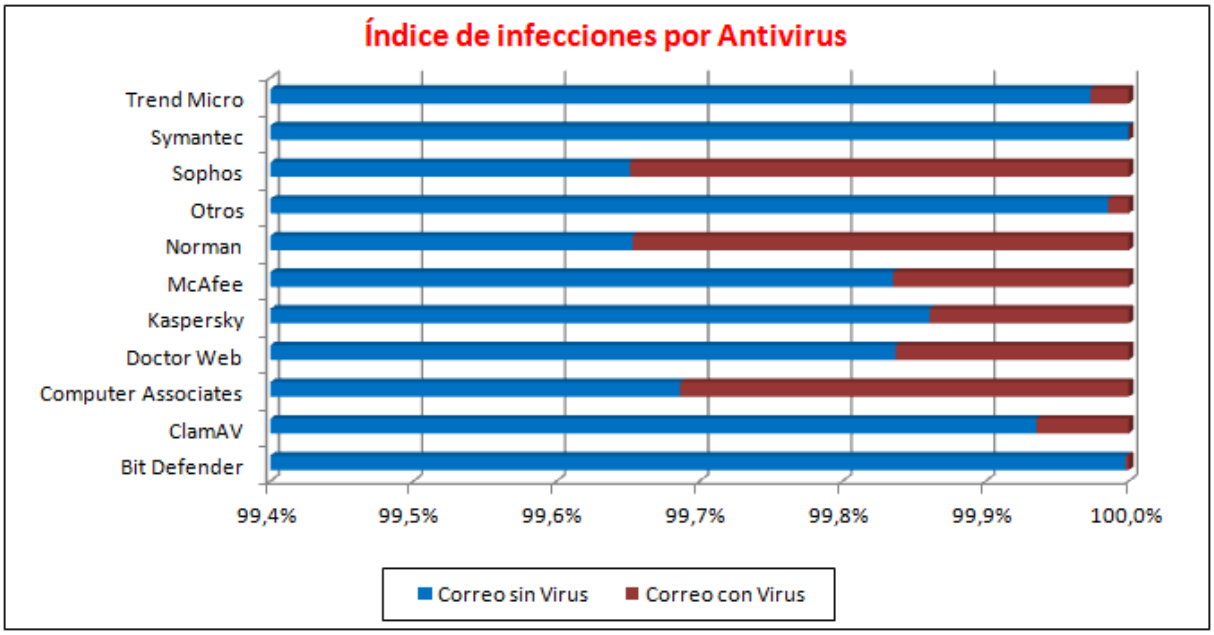

Figura 9: Relación correos analizados sin virus/correos con virus detectado por antivirus.

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 gran 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.

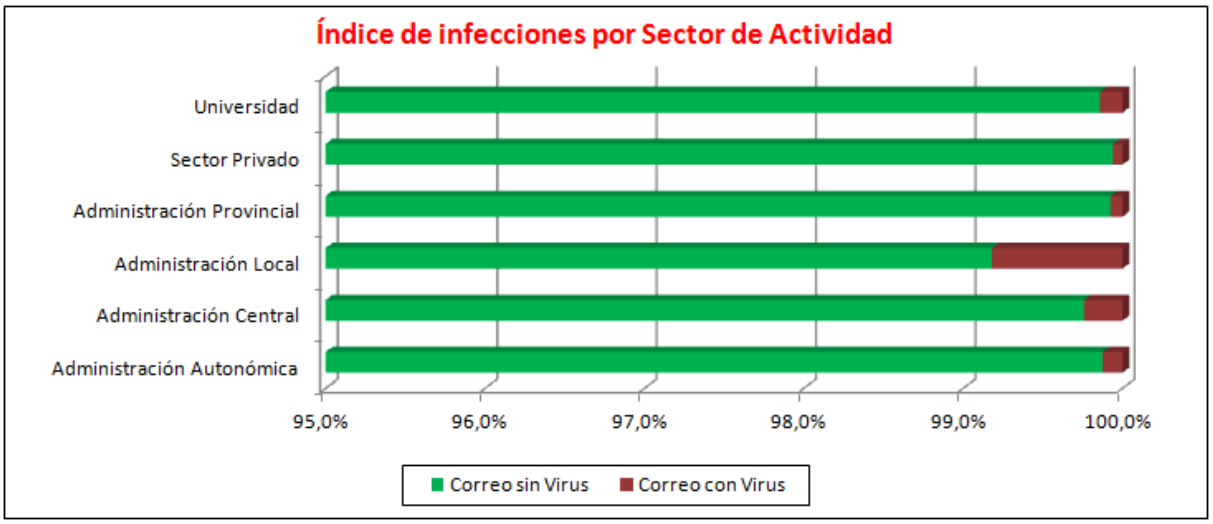

Figura 10: Porcentaje de correos sin virus frente a correos con virus detectados por sectores de actividad.

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.

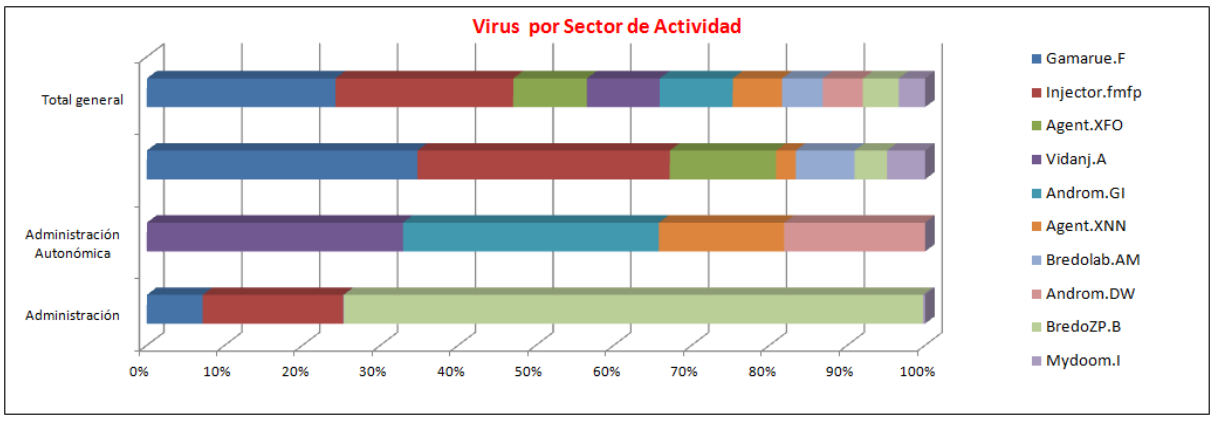

Figura 11: Top virus por sectores de actividad.

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

Virus	Administración	Sector Privado	Universidad	Total general
Gamarue.F	5,25%,	0%,	30,52%,	21,42%,
Injector.fmfp	13,22%,	0%,	28,47%,	20,21%,
Agent.XFO	0%,	0%,	12%,	8,36%,
Vidanj.A	0%,	30,15%,	0%,	8,29%,
Androm.GI	0%,	30,13%,	0%,	8,28%,
Agent.XNN	0%,	14,75%,	2,23%,	5,61%,
Bredolab.AM	0,04%,	0%,	6,63%,	4,62%,
Androm.DW	0%,	16,59%,	0%,	4,56%,
BredoZP.B	54,4%,	0%,	3,65%,	4,07%,
Mydoom.I	0,2%,	0%,	4,29%,	2,99%,
Otros	26,9%,	8,38%,	12,21%,	11,57%,

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 *BredoZP.B*, en el sector privado, los que más han afectado han sido *Vidanj.A y Androm.GI* 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 **Agosto**.

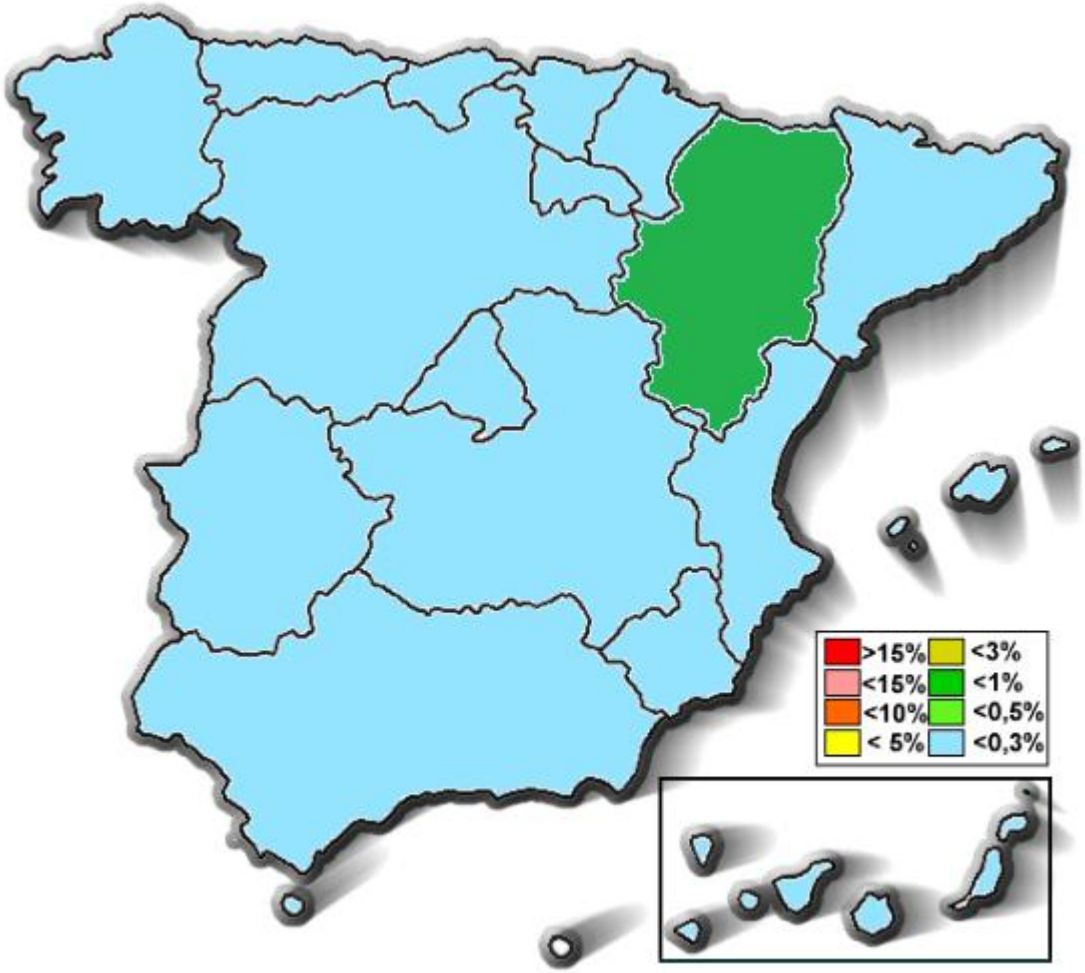

Figura 13: Mapa autonómico de detecciones de virus.

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	17.146.236	0,01%
Aragón	9.050.042	0,53%
Canarias	457.352	0,01%
Cantabria	558.138	0,0%
Castilla y León	1.080.845	0,0%
Castilla-La Mancha	28.210.201	0,01%
Catalunya / Cataluña	33.472.008	0,05%
Ciudad Autónoma de Ceuta	0	0,0%
Ciudad Autónoma de Melilla	0	0,0%
Comunidad Foral de Navarra	1.822.919	0,12%
Comunidad de Madrid	9.142.739	0,02%
Comunitat Valenciana / Comunidad Valenciana	12.197.481	0,1%
Euskadi / País Vasco	865.221	0,02%
Extremadura	14.908	0,21%
Galicia / Galicia	28.580.277	0,1%
Illes Balears / Islas Baleares	87.893	0,18%
La Rioja	0	0,0%
Principado de Asturias	16.035.622	0,0%
Región de Murcia	2.074.454	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 **Catalunya** la comunidad que más muestras aporta a la red de Sensores, mientras que **Aragón** es la comunidad que más infecciones reporta en porcentaje (0,53%) y en número total de infecciones (Unas 180.000).

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 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/

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.

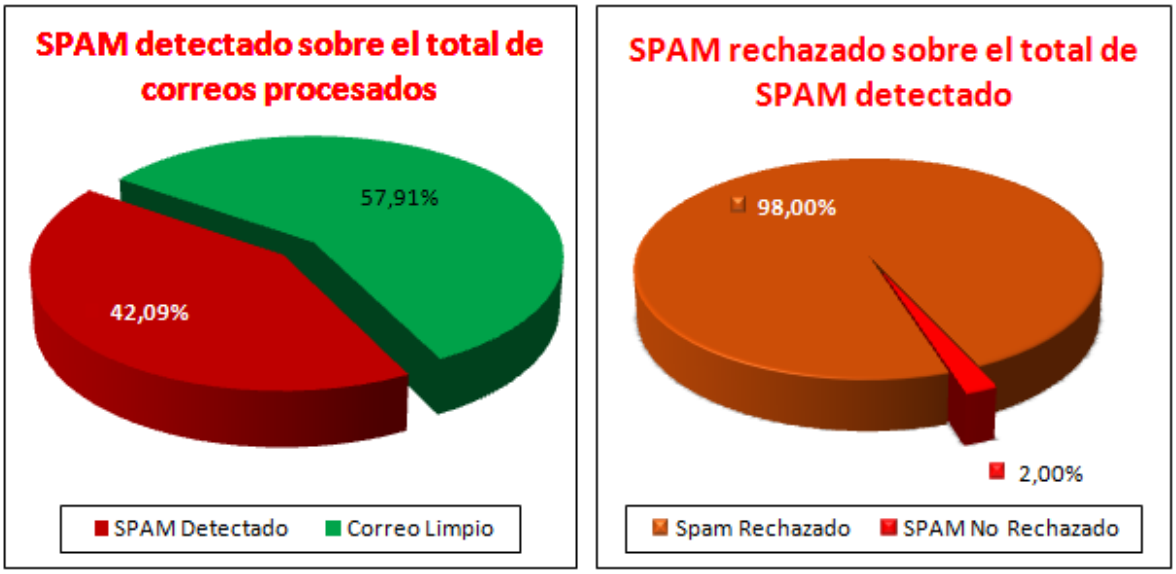

Figura 15: Nivel de SPAM detectado por la red de sensores.

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 este mes el nivel de SPAM en correo es de un **42,09%** 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 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.

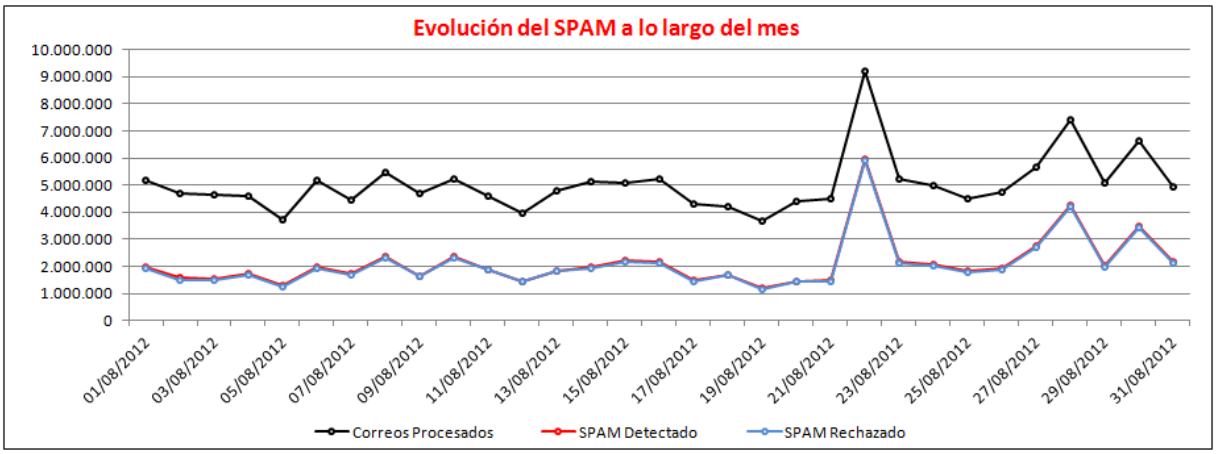

Figura 16: Evolución temporal del SPAM detectado por la red de sensores.

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.

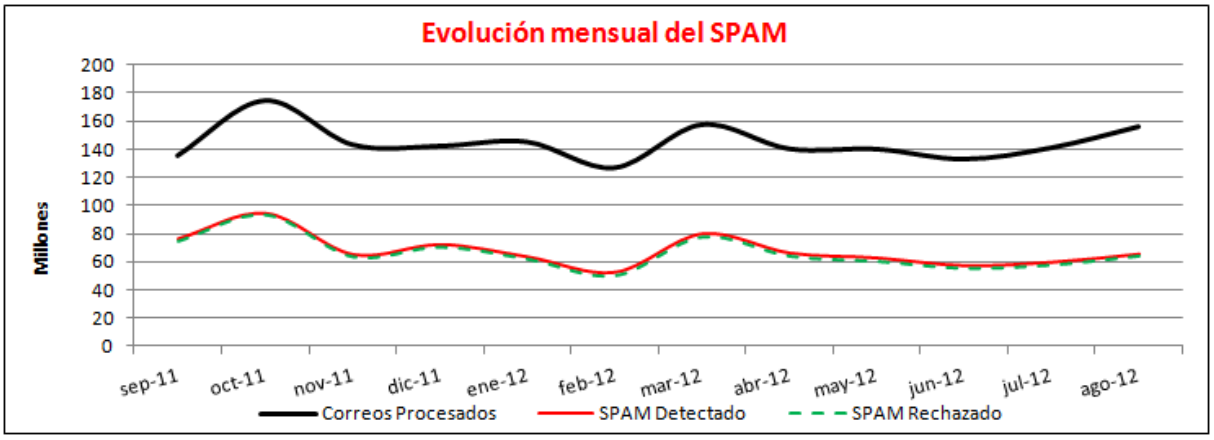

Figura 17: Evolución mensual del SPAM a lo largo del año.

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.

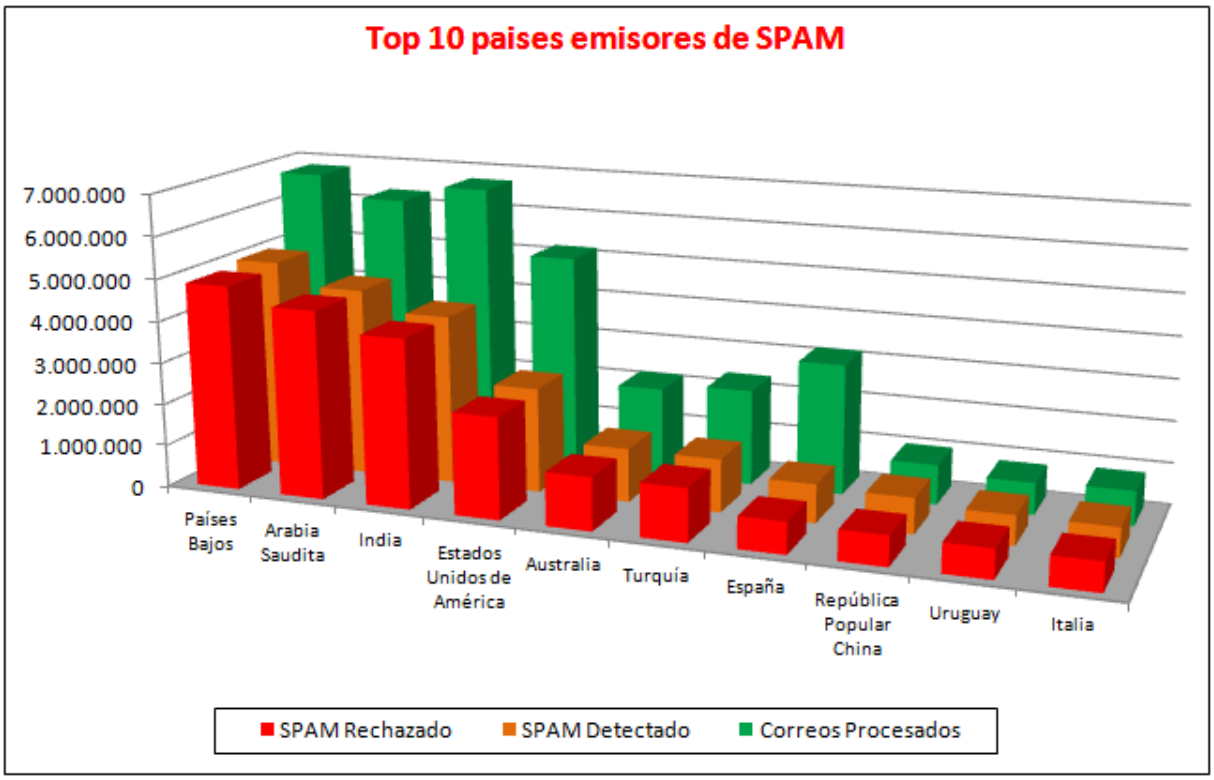

Figura 18: Top 10 países emisores de SPAM según datos recogidos por la RSI.

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

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 **Agosto**.

A lo largo del pasado mes se emitieron un total de **741** 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.

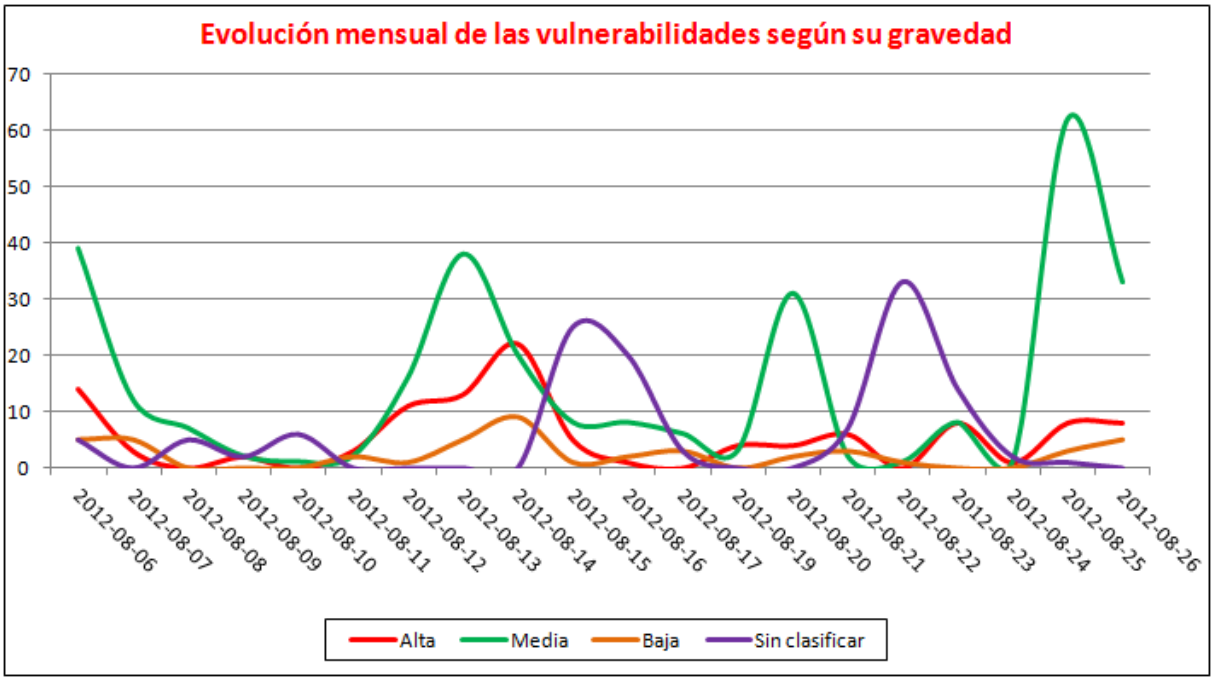

Figura 19: Vulnerabilidades emitidas por nivel de riesgo.

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.

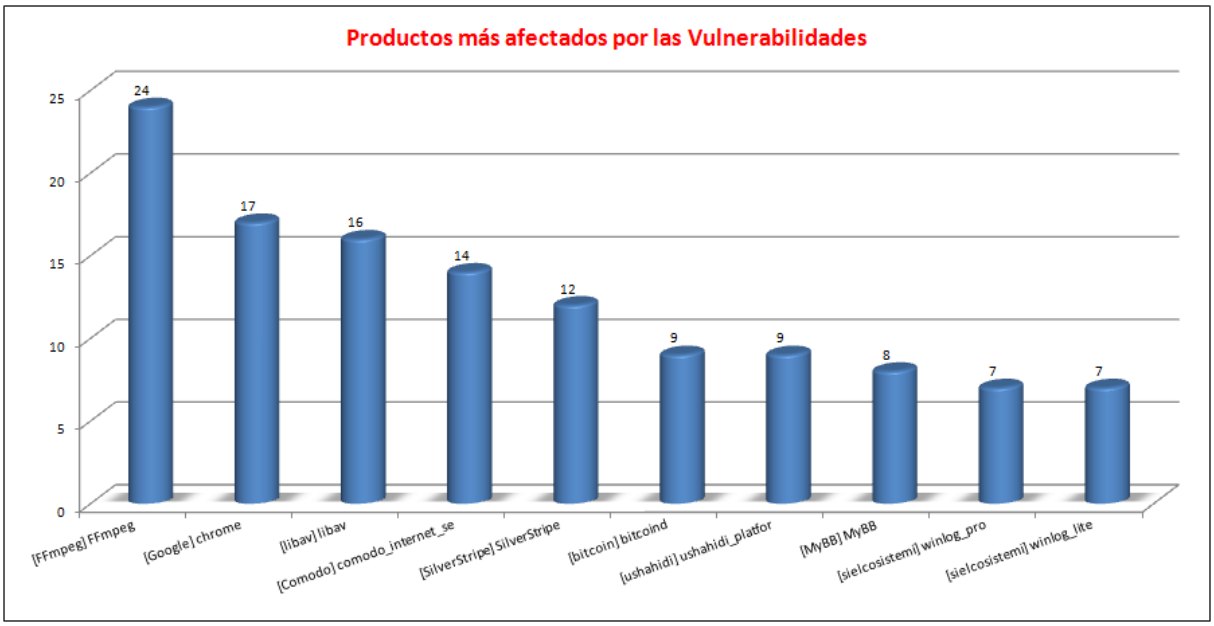

Figura 20: Productos más afectados por las últimas vulnerabilidades.

4.1.3. Fabricantes más afectados

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

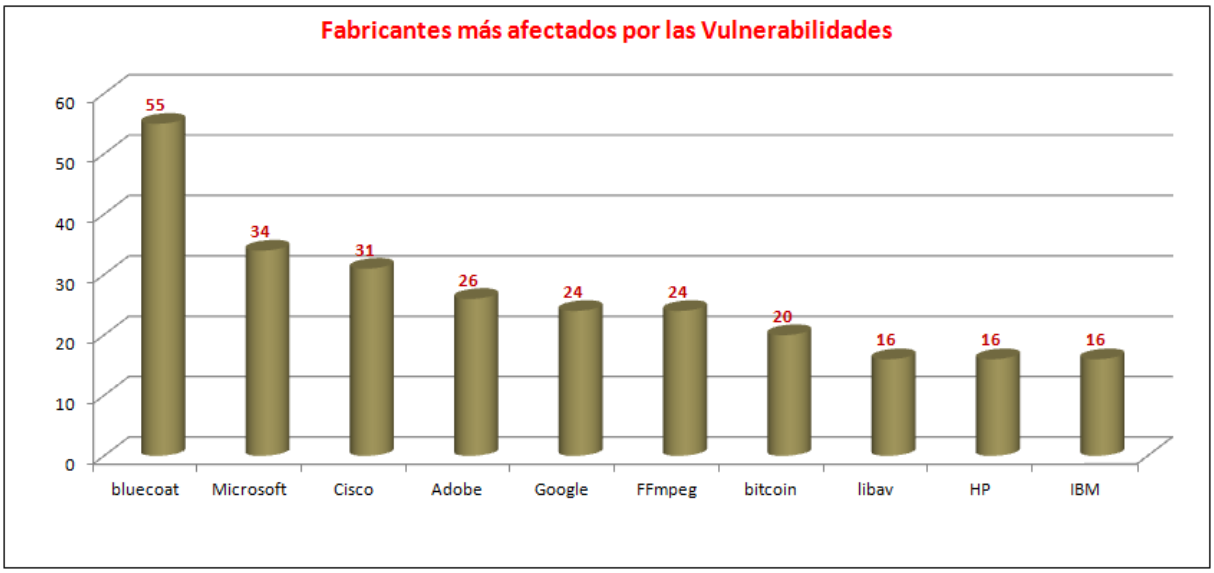

Figura 21: Fabricantes más afectados por las últimas vulnerabilidades.

4.1.4. Vulnerabilidades más comunes según su tipo

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

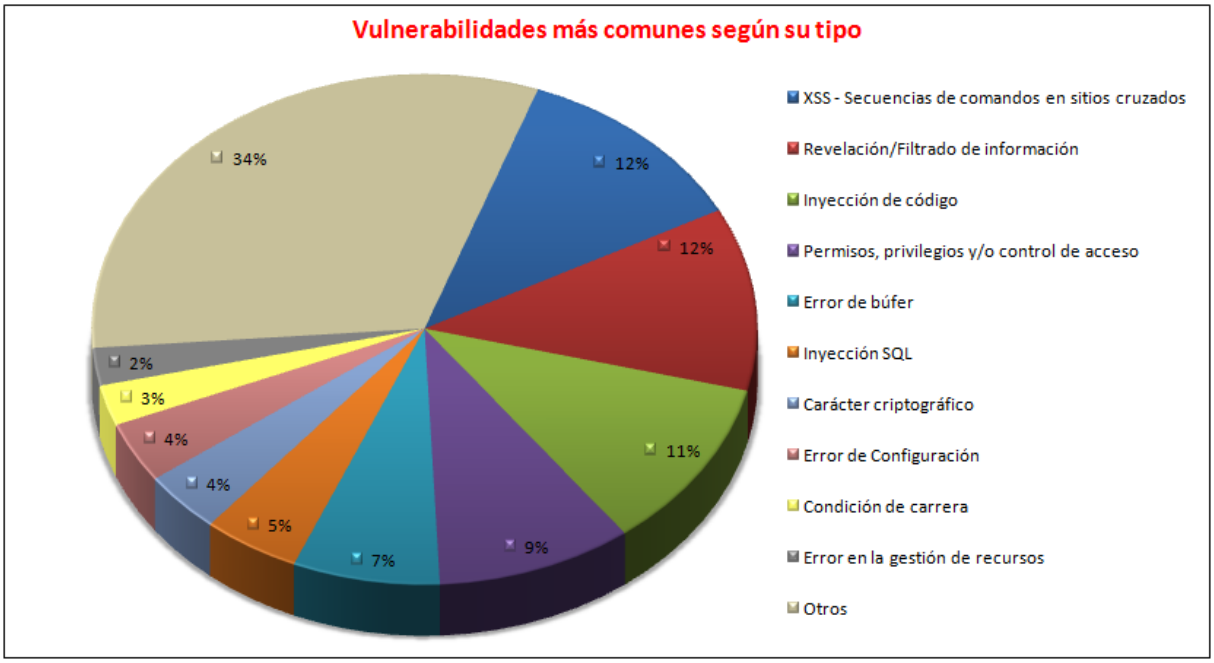

Figura 22: Vulnerabilidades más comunes por tipo.

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
Septiembre 2011	769	**Marzo 2012**	732
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

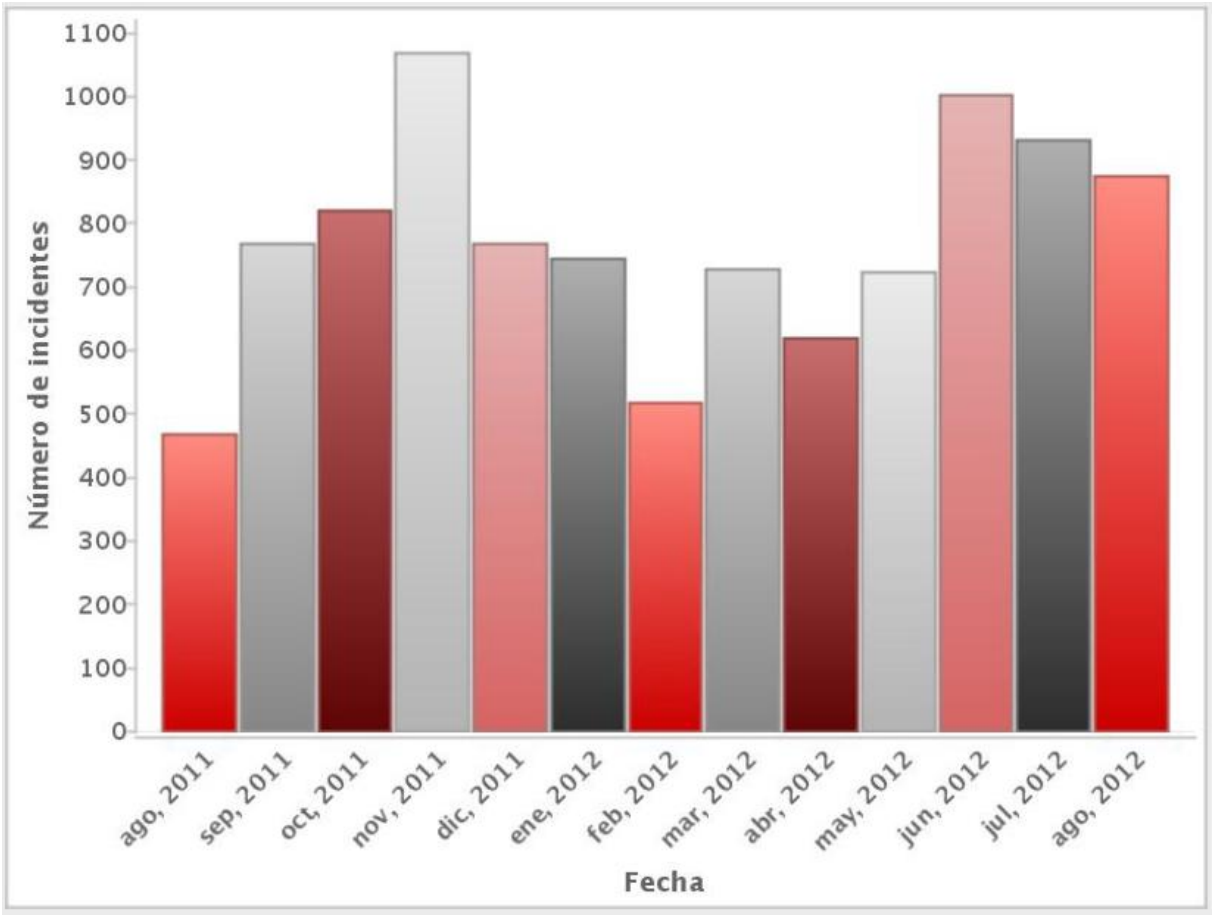

Figura 23: Evolución del número de incidentes de Fraude.

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.

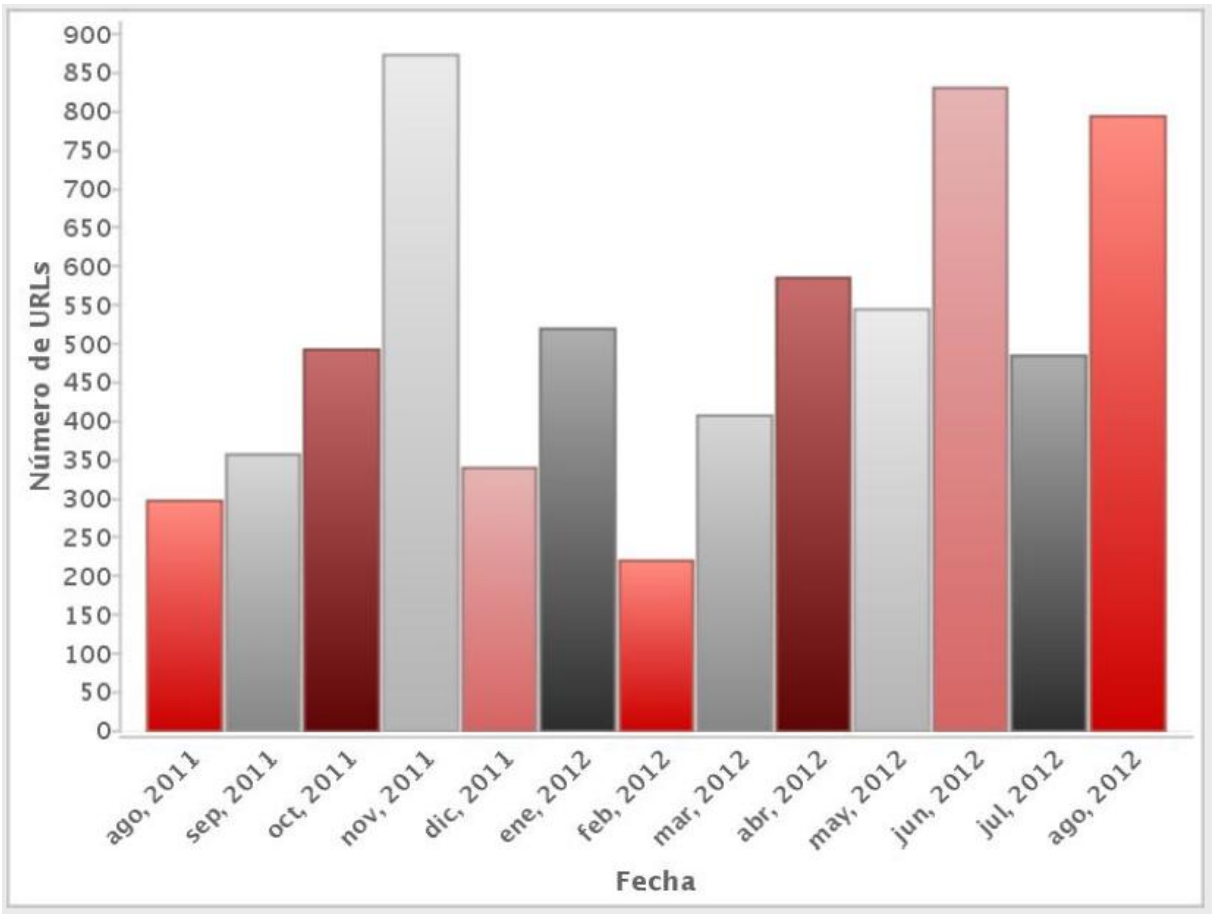

Figura 24: Evolución del número de URLs fraudulentas.

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

Mes	URLs fraudulentas	Mes	URLs fraudulentas
Septiembre 2011	358	**Marzo 2012**	403
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

4.3. AVISOS TECNICOS Y NO TÉCNICOS PUBLICADOS

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

Aviso de Seguridad	Fecha
Actualización crítica de Oracle https://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/actualizacion_critica_oracle_20120831	31/08/2012
Vulnerabilidad 0-day en Java 7 https://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/vulnerabilidad_0day_java_7_20120827	27/08/2012
Nueva versión de Apache 2.4.3 soluciona problemas de seguridad https://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/nueva_version_apache_243_soluciona_problemas_seguridad_20120824	24/08/2012
Actualización de seguridad 11.4.402.265 de Flash Player https://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/actualizacion_seguridad_114402265_flash_player_20120822	22/08/2012
Autenticación MS-CHAP v2 podría permitir revelación de información https://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/autenticacion_mschap_v2_podria_permitir_revelacion_informacion_20120821	21/08/2012
Publicada actualización de seguridad 3.6.1 de Apple Remote Desktop https://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/publicada_actualizacion_seguridad_361_apple_remote_desktop_20120821	21/08/2012
Actualizaciones de seguridad disponibles para productos Adobe https://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/actualizaciones_seguridad_disponibles_adobe_reader_adobe_acrobat_adobe_shockwave_player_adobe_flash_player_20120815	15/08/2012
Boletines de seguridad de Microsoft de Agosto 2012 https://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/boletines_seguridad_microsoft_agosto_2012_20120815	15/08/2012

Actualización de seguridad para Oracle https://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/actualizacion_seguridad_oracle_20120812	12/08/2012

4.4. EVENTOS DEL MES (SEPTIEMBRE Y OCTUBRE)

4.4.1. Reunión Española sobre Criptología y Seguridad de la Información

La Reunión Española sobre Criptología y Seguridad de la Información (RECSI) es el congreso científico referente español en el tema de la Seguridad en las Tecnologías de la Información. En él se dan cita de forma bianual los principales investigadores españoles en el tema, así como invitados extranjeros de reconocido prestigio.

Los temas de interés principales que se tratarán serán Criptología y criptoanálisis, Autenticación y firma digital, Aplicaciones de la criptografía, Privacidad y anonimato, Marcas de agua y esteganografía, Control de accesos, Detección de intrusiones y máquinas trampa, Análisis de malware, Detección de SPAM, Seguridad en redes sociales, Seguridad en sistemas embebidos, Informática forense.

- Fecha: 04-07 de Septiembre de 2012
- Lugar: Palacio de Miramar. Paseo Miraconcha, 48, 20007 San Sebastián
- Precio: A consultar
- Más información: http://recsi2012.mondragon.edu

4.4.2. 5th International Conference on Computational Intelligence in Security for Information Systems

CISIS quiere ofrecer una oportunidad de encuentro para los investigadores del sector académico y de la industria que pertenezcan a cualquiera de las grandes comunidades relacionadas con la inteligencia artificial, seguridad de la información y data mining.

- Fecha: 05-08 de Septiembre de 2012
- Lugar: Ostrava, República Checa
- Precio: A consultar
- Más información: http://gicap.ubu.es/cisis2012/home/home.shtml

4.4.3. EuroCASC- Information Security and Risk Management Conference

EuroCACS / ISRM es un evento multidimensional centrado en la auditoría, la seguridad el gobierno y el análisis de riesgos, además de en los programa de seguridad y auditoría, herramientas y recursos que se necesitan para ser sensible a los cambios de la industria.

- Fecha: 10-12 de Septiembre de 2012

- Lugar: Munich, Alemania
- Precio: A consultar
- Más información: http://www.isaca.org/Education/Conferences/Pages/European-CACS-ISRM-Europe-2012.aspx

4.4.4. Seren2 - Security 6th Call Joint Parthering Event

SEREN2 Joint Partnering Event meetings permitirá presentarse personalmente, a la organización y las ideas de cooperación como un primer paso para preparar un proyecto de seguridad en R&D.

- Fecha: 11 de Septiembre de 2012
- Lugar: Bruselas
- Precio: A consultar
- Más información: http://www.b2match.eu/security-brussels2012

4.4.5. 7th International Workshop on Data Privacy Management

La séptima edición del International Workshop on Data Privacy Management DPM 2012, se celebra en colaboración con ESORICS 2012.

Las organizaciones se están preocupando cada vez más por la privacidad de la información que gestionan, así que el tratamiento de información privada sensible es muy crítico e importante para todas las organizaciones. Esto plantea muchos problemas de cambio, como el traducir los objetivos de negocio de alto nivel en políticas de privacidad a nivel sistema, administración de los datos privados sensibles, integración e ingeniería de la privacidad de la información, mecanismos de control de acceso a la privacidad, seguridad orientada a la información y ejecución de la consulta en privacidad de la información para respuestas parciales.

- Fecha: 12-13 de Septiembre de 2012
- Lugar: Pisa, Italia
- Precio: A consultar
- Más información: http://www-ma4.upc.edu/DPM2012/main.html

4.4.6. 7th International Workshop on Critical Information Infrastructures Security CRITIS 2012

El séptimo congreso de CRITIS se pone en marcha para continuar la tradición de presentar las investigaciones innovadoras y los nuevos retos para la protección de infraestructuras

críticas. Como en años anteriores, ponentes invitados y un panel de ponencias complementarán un programa de contribuciones originales.

- Fecha: 17-18 de Septiembre de 2012
- Lugar: Radisson Blu Lillehammer Hotel, Lillehammer, Noruega
- Precio: A consultar
- Más información: http://critis12.hig.no/

4.4.7. Community SANS - primera parte

El próximo mes de septiembre, tendrá lugar en Madrid un evento Community SANS con dos cursos de SANS: "SEC-503: Intrusion Detection In-Depth" y "SEC-560: Network Penetration Testing & Ethical Hacking".

- Fecha: 20-22 de Septiembre de 2012
- Lugar: Madrid
- Precio: A consultar
- Más información: http://www.pentester.es/2012/06/evento-community-sans-en-madrid.html

4.4.8. Privacidad en bases de datos estadísticas - PSD2012

El evento busca analizar las ventajas y desventajas de la tensión entre el incremento de la demanda de la sociedad y de la economía de información precisa y la obligación ética y legal de proteger la privacidad de las personas y de las empresas que son los que responden aportando datos estadísticos. En el caso de las bases de datos estadísticas, la motivación para la privacidad de los que responden es una de supervivencia: las agencias estadísticas y los institutos de estudios no pueden esperar recoger información precisa de las personas o de las entidades a no ser que sientan que la privacidad de sus respuestas está garantizada.

- Fecha: 26-28 de Septiembre de 2012
- Lugar: Palermo, Italia
- Precio: A consultar
- Más información: http://unescoprivacychair.urv.cat/psd2012/

4.4.9. Virus Bulletin 2012 Conference

Conferencia organizada por la revista de seguridad 'Virus Bulletin'. Se trata de un evento clave en el calendario de eventos anti-malware, con muchos de sus asistentes comentando que se trata del evento de año en este campo.

- Fecha: 26-28 de Septiembre de 2012
- Lugar: Dallas, EEUU
- Precio: De 1615 a 1895 Dólares
- Más información: http://www.virusbtn.com/conference/vb2012/index

4.4.10. Community SANS - segunda parte

El próximo mes de septiembre, tendrá lugar en Madrid un evento Community SANS con dos cursos de SANS: "SEC-503: Intrusion Detection In-Depth" y "SEC-560: Network Penetration Testing & Ethical Hacking".

- Fecha: 27-29 de Septiembre de 2012
- Lugar: Madrid
- Precio: A consultar
- Más información: http://www.pentester.es/2012/06/evento-community-sans-en-madrid.html

4.4.11. 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/

4.4.12. 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