Interrelación entre las FF. y CC. de Seguridad del Estado y la US.

Gustavo A. Rodríguez
Servicio de Informática y Comunicaciones (S.I.C.)

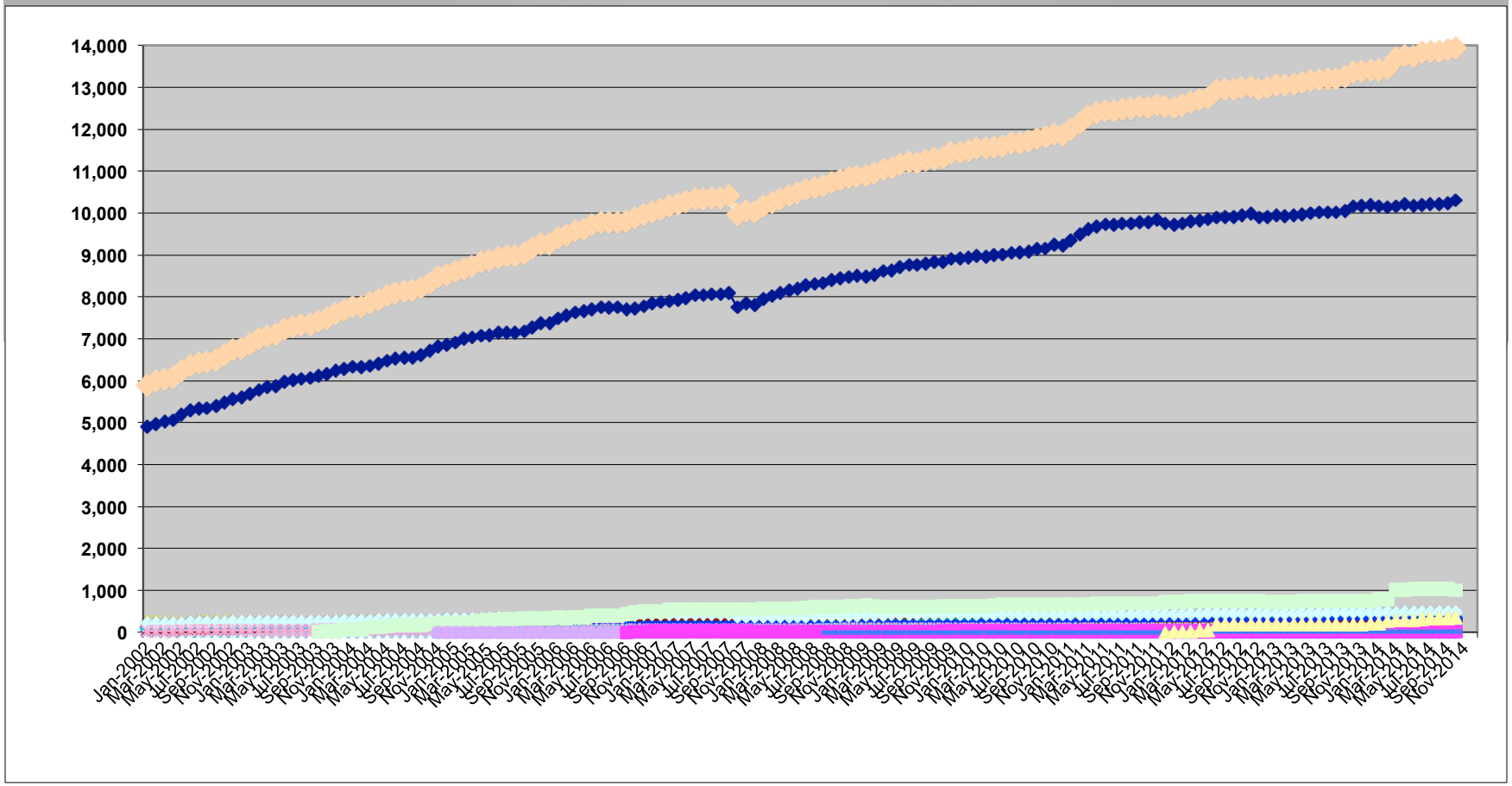
Contenido.

- Algunos números previos para situarnos en el entorno.
- Incidencias registradas en la US (periodo 2005-2014).
- Análisis previo de los datos.
- ¿Cómo llega a nosotros la petición?
- ¿Qué se pide en ellas?
- Procedimiento de actuación.
- Resumen y conclusión.

Gustavo A. Rodríguez
Servicio de Informática y Comunicaciones (S.I.C.)

Algunos números previos.

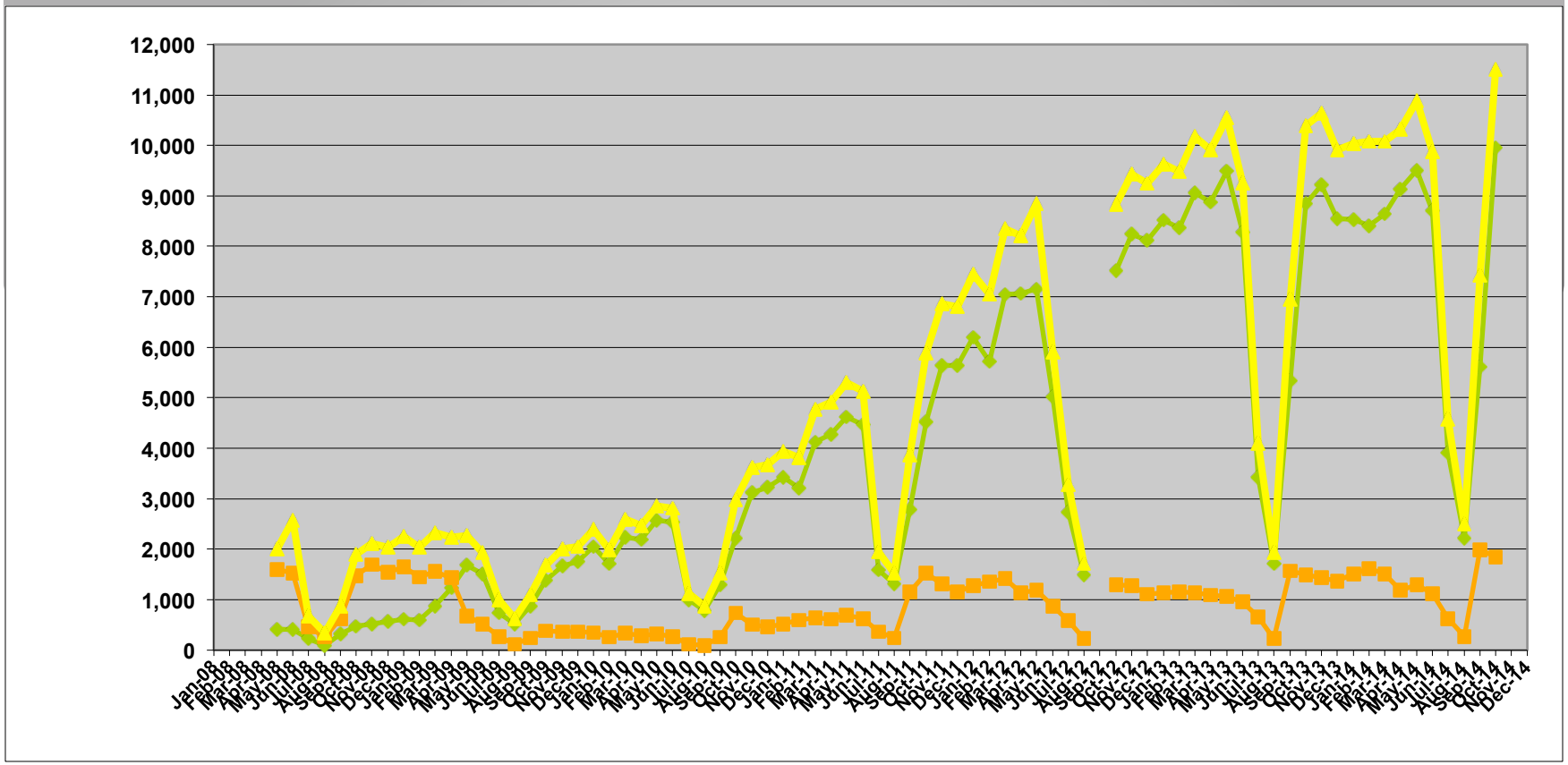
Total de equipos conectados a la red cableada:13.936 (992 equipos de acceso)
Evolución del número estos equipos:



Gustavo A. Rodríguez
Servicio de Informática y
Comunicaciones (S.I.C.)

Algunos números previos.

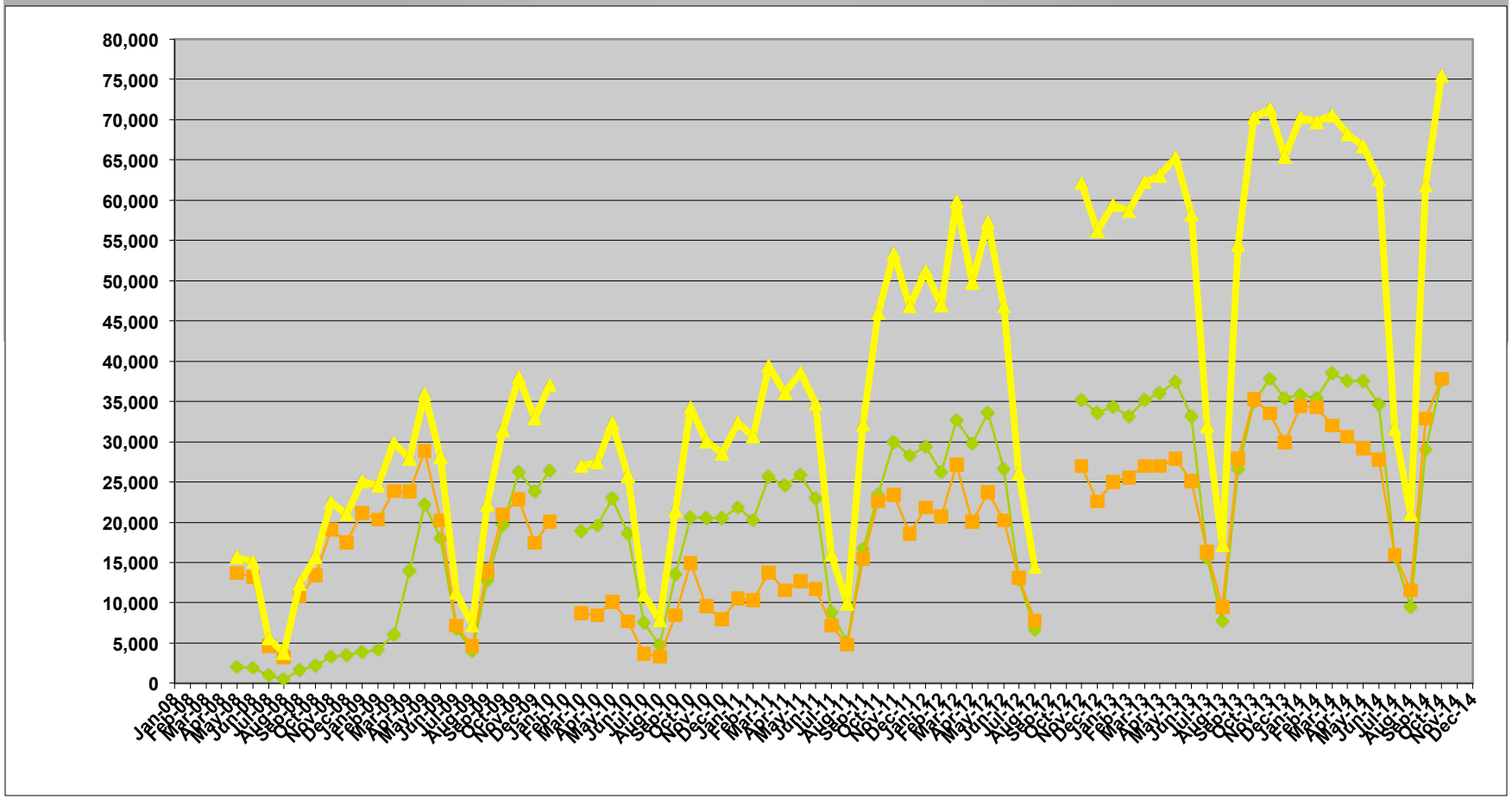
Total de equipos que acceden vía ReInUS: 40.000
Número máximo de usuarios concurrente que acceden vía ReInUS: 11.504
Evolución de éstos:



Gustavo A. Rodríguez
Servicio de Informática y
Comunicaciones (S.I.C.)

Algunos números previos.

Total de usuarios distintos que acceden por medio de ReInUS: 75.419
Evolución de éstos:



Gustavo A. Rodríguez
Servicio de Informática y
Comunicaciones (S.I.C.)

Algunos números previos.

- Total de Personal de la Universidad de Sevilla: 6.631 (PDI y PAS, todos con acceso a las redes).

- Total de Estudiantes matriculados: 76.405 (todos con acceso a las redes, tanto desde aulas de docencia, como de aulas informáticas, como desde aulas de libre acceso y por medio de la red inalámbrica de la US (ReInUS))

- Total de integrantes de la Comunidad Universitaria: 83.036.

- Potencialmente hay una gran cantidad de posibles infractores y victimas, incluido un servidor.

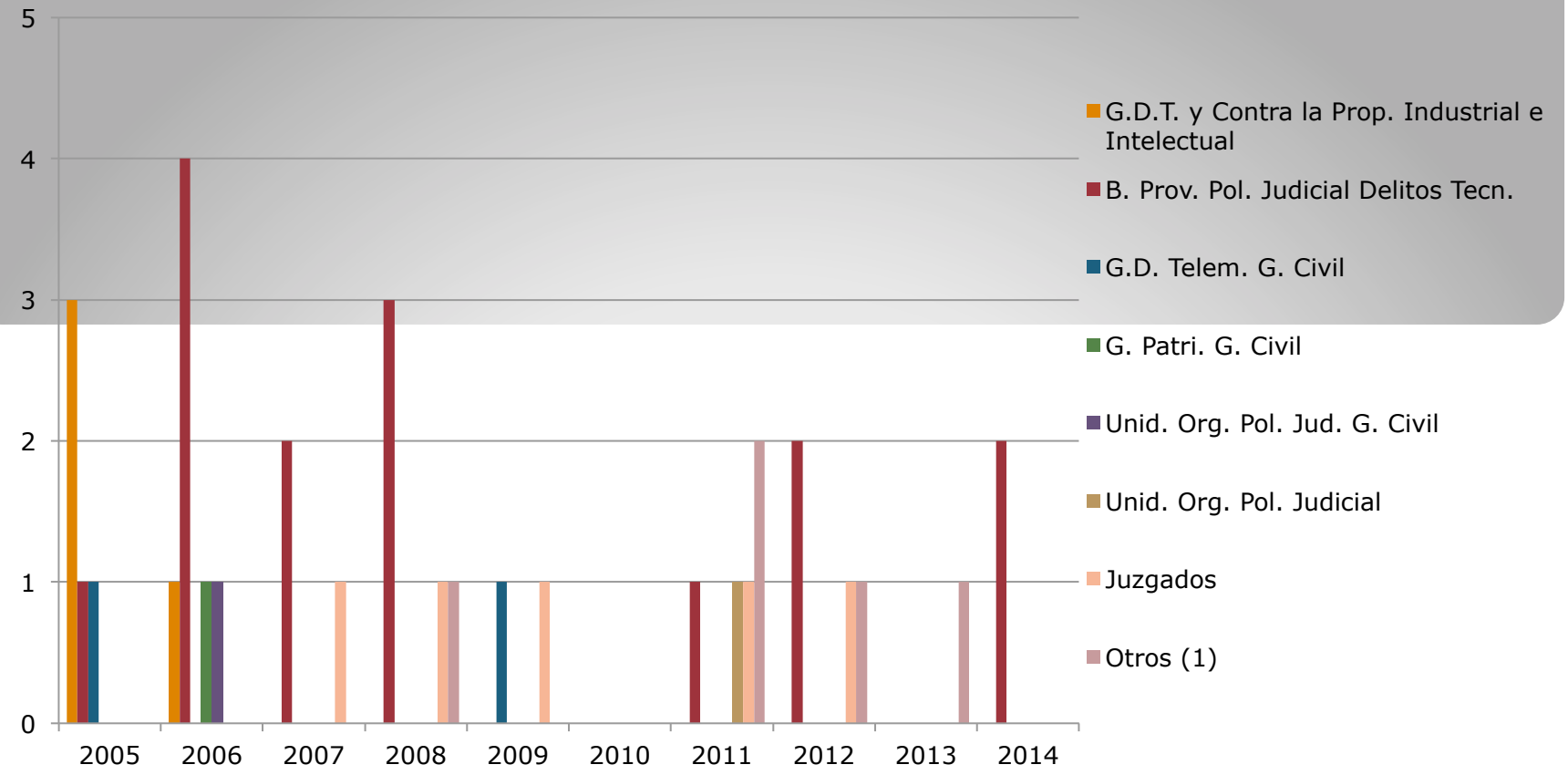
- Hay que recordar aquí que hay 10 capitales de provincia con menos habitantes que el total de la Comunidad Universitaria y solo en una de ellas, se incoaron 21 procesos durante 2011.

- Según datos del Ministerio del Interior, en 2013 se produjeron 42.437 infracciones penales relacionadas con el uso de ordenadores.

Gustavo A. Rodríguez
Servicio de Informática y Comunicaciones (S.I.C.)

Incidencias registradas en la US.

Total de incidentes registrados en el periodo comprendido entre 2005 y 2014 (10 años): 34 (Incluyendo uno informativo y mi declaración en el Juzgado).
Evolución de éstos y su procedencia:



(1) Operación Mariposa, UI Esplugas, Ertzaintza
Declaración como testigo en Juzgado por causa abierta

Gustavo A. Rodríguez
Servicio de Informática y Comunicaciones (S.I.C.)

Análisis previo de los datos.

- Se constata que el número de incidencias entre 2005 y 2007 (15) afectó al 1,5 % de los equipos que tenían acceso a la red cableada existen en el momento.

-Siendo este porcentaje entre 2008 y 2014 (19 incidencias) del 0,14 % de los equipos con acceso cableado.

- Este último porcentaje baja al 0,06 % si se incluyen los equipos de acceso inalámbrico (ReInUS) que se empezaron a usar de manera masiva a partir de 2008.

-Es evidente la disminución del número de incidencias en el periodo 2008-2014, se pasa de 15 en tres años, un 14,7 % por año, a 19 en este periodo, un 7,98 % por año, de media en ambos casos.

- El porcentaje de usuarios involucrados sería del 0,04 % del total de la Comunidad Universitaria.

- Se constata también la disparidad de fuentes desde las que llegan las peticiones.

Gustavo A. Rodríguez
Servicio de Informática y Comunicaciones (S.I.C.)

¿Cómo llega a nosotros la petición?

- Por lo general se recibe directamente en la US, un fax dirigido a mí como responsable de Comunicaciones aunque con “titulación” dispar.

- También se han solicitado por correo electrónico, igualmente dirigido a mí.

- En dos ocasiones se remitió la petición al CICA que me la reenvió y una vez se dirigieron a la Junta de Andalucía, que también lo reenvió a su destino.

- En una ocasión la G. Civil se presentó en mi despacho y me lo entregó en mano.

- En otra ocasión se dirigieron a la Gerencia de la US, pero era solo informando (Operación Mariposa), que me lo remitió.

Gustavo A. Rodríguez
Servicio de Informática y Comunicaciones (S.I.C.)

¿Qué se pide en ellas?

- Solicitudes variopintas, por lo general sobre una dirección IP y el usuario o los usuarios asociados, ubicación del equipo, uso que se le dio, “titularidad de la línea telefónica asociada a la IP” (sic), etc.

- Una muy completa, de la que más, creo, la envió la B.P.P.J. de Badajoz, solicitando (literalmente):

  - Ubicación
  - Usuario o usuarios
  - Si el equipo es de libre acceso o está en un despacho y en este caso si tiene llave el despacho
  - Si el ordenador ha tenido alguna incidencia (malware especifican) en la fecha indicada.
  - Y trazas de acceso a una página web determinada.

Procedimiento de actuación.

- Recibida la petición, lo primero que se hace, nosotros al menos, es ponernos en contacto con el peticionario ya sea por teléfono o por correo electrónico.

- Si no ha llegado con mandamiento judicial, se solicita, aceptándose que lo remitan por fax, se consultó con el Servicio Jurídico que no puso obstáculos.

- El mandamiento es **indispensable** para poder dar la información sobre personas, así nos ha informado siempre el Servicio Jurídico.

- En este primer contacto y dependiendo del tiempo que hace desde que se cometió la presunta infracción, se les dice si es posible por nuestra parte recabar los datos solicitados o si no lo es.

- Recuérdese que nosotros no somos proveedores de servicio por pago directo y no tenemos obligación de guardar datos.

Gustavo A. Rodríguez
Servicio de Informática y Comunicaciones (S.I.C.)

Procedimiento de actuación.

- No obstante se guardan datos de los equipos de las redes de aulas de libre acceso, de los proxy (aunque éstos por la gran cantidad, por un plazo muy limitado) y de la red inalámbrica ReInUS desde que se puso en marcha en 2007.

- Si hay mandamiento, se les envía **toda** la información de la que disponemos.

- Si no lo hay, y no es complicado o supone un retraso grande el obtenerlo, se espera al mandamiento, si hay posibilidad de recabar datos, si no, se les dice y ellos deciden si se pide y envían o no.

- Se les adelanta toda la información posible a la espera del mandamiento, por ejemplo confirmando que la IP es nuestra y que está en tal o cual Facultad o, todo lo más Dpto., pero sin dar más detalles.

- Vía mensajería o teléfono.

Gustavo A. Rodríguez
Servicio de Informática y Comunicaciones (S.I.C.)

Procedimiento de actuación.

- Mantenemos al tanto de las actuaciones al Servicio Jurídico.

- Dependiendo de la naturaleza del asunto y a quién involucre, de todas las actuaciones o del inicio o fin de ellas y de algún hecho relevante si procede.

- Salvo que se solicite explícitamente por el peticionario, **no se toca el equipo afectado para nada**, una vez lo hicimos, porque pedían algo que precisaba analizarlo, y nos quisieron poner “las orejas coloradas”.

- Independientemente de que se usen los diferentes medios electrónicos para comunicarse con los peticionarios y que se les envíe la información por éstos, **siempre se envía una respuesta por escrito**, que se archiva especialmente.

Gustavo A. Rodríguez
Servicio de Informática y Comunicaciones (S.I.C.)

Resumen y conclusión.

- Procedencia de peticiones muy diversa.
- Solo 8 de las solicitudes se acompañaban del mandamiento judicial preceptivo desde el principio, incluyendo en ellas 5 peticiones directas del Juzgado.
- Mucha distancia en el tiempo entre la petición y el momento de la posible infracción.
- Confundirnos con proveedores de servicio de pago directo, obligados a guardar una información de la que nosotros no disponemos en muchos casos.

- **Si hay mandamiento hay que dar todo lo que se tenga, si no lo hay cuidado con lo que se da, no porque el receptor vaya a hacer mal uso de ellos, sino porque el afectado puede aplicarnos la LOPD, por ello máxima coordinación con los Servicio Jurídicos.**

Gustavo A. Rodríguez
Servicio de Informática y Comunicaciones (S.I.C.)

Gracias por su atención.

Atenderé gustoso cualquier pregunta.

Gustavo A. Rodríguez (gurodri@us.es)

Dtor. Técnico Área de Comunicaciones.

Servicio de Informática y Comunicaciones (S.I.C.)
Universidad de Sevilla.