Expediente Nº: E/02699/2015

Con fecha 30/04/2015, el Director de la Agencia Española de Protección de Datos dictó Resolución, R/01031/2015, en la que se acuerda iniciar de ***oficio*** las presentes actuaciones de inspección, E/2699/2015, respecto del funcionamiento de la seguridad de los datos del sistema D.I.F.O de la Dirección General de la Policía**,**

CONCLUSIONES GENERALES

La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación y, con fecha 14/07/2015, la Comisaria General de la Policía Judicial de la Dirección General de la Policía, remitió a esta Agencia la siguiente información respecto del funcionamiento de seguridad de los datos del sistema D.I.F.O.:

1. Respecto al procedimiento de difusión de los formularios de solicitud de difusión (D.I.F.O.), la transmisión desde el Grupo Investigador hacia su Unidad Territorial de Inteligencia (UTI), se realiza mediante la cuenta oficial de correo electrónico a través de la red de la Dirección General de la Policía (DGP).

2. A continuación la UTI reenvía el formulario, también por correo electrónico, a la Unidad Central de Inteligencia Criminal –UCIC- a fin de evaluar si procede su difusión a nivel nacional, dependiendo de la relevancia de los hechos y del nivel de calidad de las imágenes a difundir.

3. Respecto al ámbito de difusión de los formularios a nivel nacional, es la UCIC la que lo realiza una vez registrada, difundiéndolo a todas las Unidades de Inteligencia y a determinadas Unidades Centrales de Investigación en función de la tipología delictiva del hecho, todo ello por el correo electrónico oficial. A nivel provincial o regional, es la propia UTI la que decide la extensión de la DIFO. En este sentido, no hay unos criterios reglados ya que las UTIs disponen de autonomía para tomar la decisión que proceda. En algunas plantillas, es el Grupo Investigador el que ya indica a su UTI la extensión y, en otros, es la propia UTI la decisora. En esa decisión se valora la entidad del hecho delictivo, peligrosidad y la posibilidad de que el autor pueda actuar en varias localidades. La lista de distribución del correo oficial es fija para determinados delitos aunque también cabe la posibilidad de elaborar dicha lista ex profeso, según las circunstancias de los hechos y, como regla general, siempre son grupos de investigación del CNP.
En ocasiones, si el grupo investigador lo decide o la propia UTI, la DIFO se hace extensiva a la Policía Local, Policía Autonómica y Guardia Civil, a las direcciones de correo oficial preestablecidas de antemano por acuerdos de colaboración.

4. En relación a las medidas de seguridad establecidas para dar cumplimiento a lo dispuesto en los artículos 85, 97, 103 y 104 del RLOPD, en el envío y recepción de los correos electrónicos en los que se transmiten los formularios:
a) Las comunicaciones entre servidores de la red del CNP se realizan utilizando una red privada de servidores protegida por sistemas de seguridad perimetral (firewall,

IDS, IPS.) a la que no tienen acceso los usuarios.

b) En todos los casos, para el envío/recepción de mensajes de correo, los servidores utilizan TLS para el cifrado del canal de comunicación, siempre que el cliente/servidor remotos lo admitan.

c) Actualmente el CNP dispone de tres dominios de correo (dgp.mir.es; policía.es y oficial.dgp.mir.es). Los dominios dgp.mir.es y policia.es no disponen de un sistema de encriptado del contenido de los mensajes automático. Para garantizar el cumplimiento de los requisitos de seguridad requeridos por la legislación vigente, se ha dotado a todos los miembros del CNP de certificados de autentificación, firma y cifrado en tarjeta criptográfica que permiten, entre otros, el cifrado y la firma digital de los mensajes de correo, de forma que cada usuario pueda garantizar el nivel de seguridad exigido para el tipo de información transmitida. El dominio oficial.dgp.mir.es sí que dispone de un sistema de cifrado automático, de forma que se cifran todos los mensajes de correo entre dicho dominio.

d) Sobre el sistema de registro de entrada de soportes a nivel central de UCIC, se lleva un registro de entrada, (fichero Excel), de todas las difusiones que recibe de la estructura territorial de inteligencia en donde constan los siguientes campos: fecha de entrada del correo; número de difusión; unidad de inteligencia remitente; el hecho delictivo; si hay detenidos o identificados; si es difusión de modus operandí nuevo y diferentes campos para calificar el hecho delictivo. estos últimos a efectos estadísticos. A nivel territorial, de UTIs, también llevan su registro de entrada (fichero Excel) pero al disponer de autonomía, como ya se ha indicado, no hay un formato estándar establecido, con lo cual la estructura de sus campos y del contenido de los datos dependen de cada UTI.

e) Las personas autorizadas para la distribución de la D.I.F.O son el personal destinado en las Unidades de Inteligencia, tanto a nivel central como territorial. Cada UTI estructura su sistema de archivo de carpetas con los correos electrónicos recibidos y enviados de las DIFO realizadas.

f) Los destinatarios finales de la DIFO son los que figuran en la lista de distribución de las distintas unidades de inteligencia.

g) Los ficheros de los logs de todas las transacciones de correo se almacenan, al menos, dos años y se puede seguir la trazabilidad de todos los datos del correo salvo el contenido que no se almacena, aunque dicha trazabilidad no es automática.

MARCO LEGAL

La Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal -LOPD- en su artículo 3 define:

*"c) Tratamiento de datos: Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, **grabación**, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.*

La LOPD en su artículo 40 reconoce a la AEPD la *" potestad inspectora"* y en su apartado 1, recoge: *" Las autoridades de control podrán inspeccionar..."* El Reglamento de desarrollo de la LOPD -RLOPD- aprobado por R.D. 1720/2007, de 21/12, en su artículo 122 prevé: *" 1…., se podrán realizar actuaciones previas con objeto de determinar si concurren circunstancias que justifiquen tal iniciación..."* y el Reglamento del Procedimiento para el Ejercicio de la Potestad Sancionadora, aprobado por R.D 1398/1993, de 4/08, en su artículo 12 dispone lo siguiente: " *Con anterioridad a la iniciación del procedimiento, se podrán realizar actuaciones previas de investigación.."*

La LOPD en su artículo 9, recoge:

¡1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

La Inspección se centró en el análisis del cumplimiento de la LOPD y de las medidas de seguridad previstas en el RLOPD, resultando que la Comisaria General de Policía Judicial de la Dirección General de la Policía informó del procedimiento previsto en la difusión de los formularios de solicitud de difusión D.I.F.O. y correspondencia con la Guardia Civil y Policías locales, tal como se recoge en el Hecho Segundo, apartados 1, 2 y 3.

En concreto cuanto al cumplimiento de las medidas de seguridad del sistema D.I.F.O en el envío y recepción de los correos electrónicos en los que se transmiten los formularios, la inspección se centró en el grado de cumplimiento de los artículos 85, 97, 103 y 104 del RLOPD.

El RLOPD en el artículo 80, dispone:

"Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto."

Y su artículo 81, prevé:

"3. Además de las medidas de nivel básico, medio, las medidas de seguridad se aplicaran en los siguientes ficheros o tratamientos de datos de carácter personal: b) Los que contengan o se refieran a datos recabados para ***fines policiales*** *sin consentimiento de las personas afectadas".*

De acuerdo a lo expuesto, el sistema D.I.F.O como fichero con fines policiales

ha de cumplir con el nivel alto de medidas de seguridad.

Por su parte, el artículo 85, dispone:

"Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, conforme a los criterios establecidos en el artículo 80".

Respecto a ello, la Comisaría General de la Policía Judicial, a efectos de brevedad, informa en el Hecho Segundo, apartado 5, a), b) y c) sobre el modo de las comunicaciones entre servidores de la red del CNP que utiliza una red privada de servidores protegida m por sistemas de seguridad perimetral (firewall, IDS, IPS) y a la que no tienen acceso los usuarios. Y en todos los casos, para el envío y la recepción de mensajes de correo los servidores utilizan un TLS para el cifrado del canal de comunicación, siempre que el cliente/ servidor lo admita.

Asimismo, informa que el CNP dispone de tres dominios de correo (dgp.mir.es; policía.es y oficial.dgp.mir.es). Los dominios dgp.mir.es y policia.es no disponen de un sistema de encriptado del contenido de los mensajes automático y para garantizar el cumplimiento de los requisitos de seguridad requeridos por la legislación vigente, se ha dotado a todos los miembros del CNP de certificados de autentificación, firma y cifrado en tarjeta criptográfica que permiten, entre otros, el cifrado y la firma digital de los mensajes de correo, de forma que cada usuario pueda garantizar el nivel de seguridad exigido para el tipo de información transmitida. El dominio oficial.dgp.mir.es sí que dispone de un sistema de cifrado automático, de forma que se cifran todos los mensajes de correo entre dicho dominio.

Respecto a la gestión de soportes y documentos el artículo 97 del RLOPD, establece:

"1. Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

2. Igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada".

Tal y como se acredita en el punto 5, apartado d, e, f, g)) del Hecho segundo, el registro de entrada de soportes a nivel central de UCIC se lleva un registro de entrada en Excel con los campos que se recogen en el apartado d) y a nivel territorial de UTIs también se lleva registro de entrada sin un sistema establecido.

En lo concerniente al artículo 103 del RLOPD "registro de accesos", que prevé:

***"1.** De cada intento de acceso se guardarán, como mínimo, la identificación del*

usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.

4. El período mínimo de conservación de los datos registrados será de dos años.

5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:

a) Que el responsable del fichero o del tratamiento sea una persona física.

b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad" .

Las personas autorizadas para la distribución de la DIFO son el personal destinado en las unidades de inteligencia que figuran en las listas de distribución

Y los logs de todas las transacciones de correo se almacenan, al menos, dos años y se puede seguir la trazabilidad de todos los datos del correo salvo el contenido que no se almacena, aunque dicha trazabilidad no es automática.

En definitiva**,** se estima que es sistema DIFO cumple con las medidas de seguridad previamente referidas y contrastadas.

Respecto, al artículo 104 "Telecomunicaciones"**,** establece**:**

"Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros" .

RECOMENDACIONES

Dado que en ocasiones, si el grupo investigador lo decide o la propia UTI, la difusión DIFO se hace extensiva a la Policía Local, Policía Autonómica y Guardia Civil, a las direcciones de correo oficial preestablecidas de antemano por acuerdos de colaboración **que no garantiza el cifrado de la comunicación**, se estima necesario la aplicación del trascrito artículo 104 del RLOPD, ya que debido a la obligación de implementar medidas de seguridad de nivel alto por la naturaleza de los datos transmitidos en el sistema DIFO, se **RECOMIENDA** no transmitir dicha información por redes públicas sino por los sistemas de comunicaciones privativos de las Fuerzas y

Cuerpos de Seguridad que no tenga carácter de sistemas inalámbricos o bien implementar sistemas que garanticen que dicha información no sea inteligible ni manipulable por terceros, bien utilizando sistemas de cifrado punto a punto o bien remitiendo la información en contenedores o documentos que permitan el cifrado de su contenido.

Mar España Martí
Directora de la Agencia Española de Protección de Datos