I. DISPOSICIONES GENERALES

MINISTERIO DE ASUNTOS EXTERIORES Y DE COOPERACIÓN

6725 *Memorando de Entendimiento sobre el establecimiento de una conexión segura entre Eurojust y España, hecho en Madrid y La Haya el 24 de marzo y 7 de abril de 2015.*

MEMORANDO DE ENTENDIMIENTO RELATIVO AL ESTABLECIMIENTO DE UNA CONEXIÓN SEGURA ENTRE EUROJUST Y ESPAÑA

El Ministerio de Justicia de España, representados a efectos del presente Memorando de Entendimiento por Javier Herrera García-Canturri, Director General de Cooperación Jurídica Internacional y Relaciones con las Confesiones (en lo sucesivo, «España»), y

Eurojust, representada a efectos del presente Memorando de Entendimiento por su Director Administrativo, Klaus Rackwitz,

En lo sucesivo denominados colectivamente las «Partes» o individualmente la «Parte»,

Teniendo presente la Decisión del Consejo, de 28 de febrero de 2002, por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia, cuya última modificación la constituye la Decisión 2009/426/JAI del Consejo, de 16 de diciembre de 2008, por la que se refuerza Eurojust (en lo sucesivo, la «Decisión Eurojust»)[1],

[1] DO L 138 de 4.6.2009, p. 14/32.

Considerando que los Servicios transeuropeos seguros de telemática entre administraciones (la «red s-TESTA») es un proyecto desarrollado en forma de una red telemática como servicio de infraestructura que se sustenta en el artículo 5 de la Decisión 2004/387/CE del Parlamento Europeo y del Consejo, de 21 de abril de 2004, relativa a la prestación interoperable de servicios paneuropeos de administración electrónica al sector público, las empresas y los ciudadanos (IDABC) para apoyar el desarrollo de Proyectos de Interés Común en el marco de la Decisión n.º 2004/387/CE y para proporcionar una plataforma de comunicación segura y fiable para el intercambio de datos entre administraciones públicas[2];

[2] DO L 144, 30.4.2004 y corrección en DO L 181, 18.5.2004, pág. 25.

Considerando que el programa se reemplazó por un programa de la Comunidad para las soluciones de interoperabilidad para las administraciones públicas europeas (el « programa ISA») mediante la Decisión n.º 922/2009/CE del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009 (la «Decisión ISA»)[3],

[3] DO L 260, 3.10.2009, pág. 20.

Teniendo presente que el considerando 17 de la Decisión ISA declara que el programa garantizará ademas el funcionamiento y la mejora de los servicios comunes existentes, creados en el marco del IDABC desde el 1 de enero de 2010, y, por tanto, la conexión s-TESTA está comprendida en el programa ISA.

Considerando que tanto Eurojust como España, han firmado con la Comisión Europea un Memorando de Entendimiento sobre los requisitos de calidad y seguridad relacionados con la conexión a la red s-TESTA facilitada en el marco del programa ISA o de cualquier otro programa que reemplace al mismo (en lo sucesivo mencionado colectivamente como los «Memorandos de Entendimiento s-TESTA»),

cve: BOE-A-2018-6725
Verificable en http://www.boe.es

Considerando que la transmisión de información entre las Partes basada en sus respectivos marcos jurídicos y, en concreto, en la Decisión Eurojust, requiere el establecimiento de una conexión segura entre las mismas,

Han convenido en lo siguiente:

ARTÍCULO 1

Objeto

1. El objeto del presente Memorando de Entendimiento es regular la creación, puesta en marcha y operación de una conexión segura entre Eurojust y España, que haga posible la transmisión de información entre las Partes tal como se expone en la Decisión Eurojust y especialmente en los artículos 12, 13 y 13a de la misma (en lo sucesivo denominada la «Red segura Eurojust-España»)[4]. Esta conexión segura se creará sobre la red s-TESTA ya existente, a la que ya están conectadas España y Eurojust.

---

[4] Más concretamente:

– El artículo 12(5)(a) de la Decisión Eurojust especifica que el sistema de coordinación nacional de Eurojust (en lo sucesivo denominado el «ENCS», por sus siglas en inglés) garantizará que el Sistema de Gestión de Casos de Eurojust (en lo sucesivo denominado el «CMS», por sus siglas en inglés) reciba de forma eficaz y fiable la información sobre el Estado miembro interesado.

– El artículo 12(6) especifica que algunos miembros del ENCS deberán conectarse al sistema de gestión de casos y otros podrán hacerlo con arreglo al artículo 12 y a los artículos 16, 16 bis, 16 ter y 17 y el Reglamento interno de Eurojust.

– El artículo 13(1) especifica que las autoridades competentes de los Estados miembros intercambiarán con Eurojust cualquier información necesaria con miras al cumplimiento de las funciones de esta última de conformidad con lo dispuesto en los artículos 4 y 5, ateniéndose a las normas de protección de datos establecidas en la presente Decisión.

– El artículo 13 bis especifica que Eurojust facilitará a las autoridades nacionales competentes información y reacciones conexión con los resultados del tratamiento de la información en el CMS.

ARTÍCULO 2

Uso de la conexión segura Eurojust-España

1. La conexión segura Eurojust-España se utilizará únicamente para la transmisión de información entre las Partes de conformidad con sus respectivos marcos jurídicos y,en concreto, con las normas sobre protección de datos aplicables a Eurojust.

2. El objetivo es el uso de la conexión segura Eurojust-España para la transmisión de información RESTREINT UE/EU RESTRICTED. A estos efectos, se aplicará una solución integral, basada en varios niveles de cifrado, de conformidad con la legislación nacional aplicable y el artículo 39 bis de la Decisión Eurojust. Hasta que se complete el proceso de acreditación, el uso de la conexión se limitará a la transmisión de información NO CLASIFICADA.

ARTÍCULO 3

Código de conexión

1. Las Partes respetarán el código de conexión para la conexión segura Eurojust-España, tal como se prevé en el anexo 1.

2. Ninguna otra interconexión futura que las Partes establezcan con cualquier otra red afectará a la conexión segura Eurojust-España y su funcionamiento deberá ajustarse, en todo lo posible, al código de conexión previsto en el anexo 1.

3. Las Partes llevarán a cabo las acciones necesarias para informar a sus respectivas Administraciones de sus responsabilidades en el contexto del presente Memorando de Entendimiento.

cve: BOE-A-2018-6725
Verificable en http://www.boe.es

4. En caso de que tenga lugar un incidente de seguridad, como por ejemplo los enumerados en la Parte C del anexo 1, la Parte afectada por el mismo se desconectará de la otra, para evitar todo riesgo para los sistemas de esta última.

5. Las Partes serán responsables de la seguridad de sus propios sistemas y redes, entre otros por los riesgos que se generen en la conexión segura Eurojust-España, desde el punto de demarcación hacia el interior, como se determina en el diseño de la conexión segura Eurojust-España que se señala en el anexo 3 (en lo sucesivo mencionado como el «diseño de la conexión segura»).

6. Las Partes no realizarán ninguna prueba, exploración de vulnerabilidades o acto de intrusión en los sistemas y redes de la otra Parte sin previa autorización por escrito de esta última.

7. Cada Parte compartirá la información sobre amenazas y vulnerabilidades que puedan afectar a los sistemas y redes de la otra.

ARTÍCULO 4

Diseño de la conexión segura Eurojust-España

1. La conexión segura Eurojust-España consiste en una conexión de red establecida entre Eurojust y España sobre la red s-TESTA.

2. Las Partes habrán establecido y configurado la conexión segura Eurojust-España y los sistemas de conexión relacionados previamente a su uso, de conformidad con el código de conexión y el diseño de la conexión segura, y de conformidad con sus respectivos Memorandos de Entendimiento de s-TESTA, en concreto en relación con el anexo III del mismo.

3. Las Partes habrán establecido y configurado un servicio seguro de encaminamiento de correo electrónico, que permite un intercambio seguro de correo electrónico entre ellos mediante el uso de la conexión segura Eurojust-España, de conformidad con el código de conexión y el diseño de la conexión segura.

ARTÍCULO 5

Control y mantenimiento de la conexión segura Eurojust-España

1. Las Partes serán responsables del control y mantenimiento de la conexión segura Eurojust-España, de conformidad con el código de conexión y el diseño de la conexión segura.

2. Las Partes garantizarán que sus respectivos sistemas y redes interconectados trabajan adecuadamente desde el punto de demarcación hacia el interior y, en caso de mal funcionamiento, harán todos los esfuerzos necesarios para restablecer la conexión segura Eurojust-España y los servicios que dependan de ella.

3. Las Partes garantizarán que el servicio seguro de encaminamiento de correo electrónico funcione de forma adecuada y harán todos los esfuerzos necesarios para restablecerlo en caso de mal funcionamiento.

4. En caso de que una Parte necesite realizar cualquier modificación de sistemas en red que puedan tener repercusiones en las redes de la otra Parte o en la conexión segura Eurojust-España, solicitará autorización previa por escrito (p. ej., mediante correo electrónico) a través del punto de contacto de la otra Parte que se indica en el artículo 6 del presente Memorando de Entendimiento.

5. Las Partes informarán al punto de contacto de la otra Parte de cualquier operación de mantenimiento prevista que pueda afectar a la disponibilidad de la conexión segura Eurojust-España o del servicio seguro de correo electrónico.

cve: BOE-A-2018-6725
Verificable en http://www.boe.es

ARTÍCULO 6

Punto de contacto

1. En el anexo 2 (Puntos de contacto técnico) se designa un punto de contacto de cada Parte. En el supuesto de cambio de su punto de contacto, la Parte correspondiente deberá informar a la otra por escrito (p. ej., mediante correo electrónico).

2. Cuando se den problemas técnicos en la conexión segura Eurojust-España o se precise una intervención de la otra Parte, se comunicará al punto de contacto, entre otros casos cuando una de las Partes descubra un problema en el otro extremo de la conexión.

3. Las modificaciones técnicas en las partes B y C del anexo 3 deberán acordarse por escrito entre los punto de contactos de las Partes, a condición de que dichas modificaciones no afecten a los derechos y obligaciones de las Partes que se establecen en el presente Memorando de Entendimiento.

4. En caso de que la cuestión afecte a la propia red s-TESTA la Parte que haya encontrado el problema se pondrá en contacto con el Centro de asistencia técnica de apoyo y operaciones de s-TESTA, como se concreta en el anexo V de los Memorandos de Entendimiento s-TESTA.

ARTÍCULO 7

Distribución de costes

1. La conexión segura Eurojust-España se crea utilizando la red s-TESTA existente, proporcionada por la Comisión Europea. A este respecto, ninguna de las Partes soporta coste extraordinario alguno de adquisición o instalación por el establecimiento de la conexión segura.

2. En caso de que una futura conexión de España al Sistema de gestión de asuntos de Eurojust exija la mejora de la conexión segura Eurojust-España, los costes de la misma deberán cargarse al presupuesto general de la Unión Europea con arreglo al artículo 12(6) de la Decisión Eurojust. En tal caso, el presente Memorando de Entendimiento deberá modificarse de conformidad con el artículo 9(2).

ARTÍCULO 8

Resolución de controversias y suspensión

1. Las Partes, a solicitud de cualquiera de ellas, se reunirán sin demora para resolver cualquier controversia relativa a la interpretación o aplicación del presente Memorando de Entendimiento o cualquier cuestión que afecte a su relación mutua.

2. Si no logra resolverse la controversia relativa a la interpretación o aplicación del presente Memorando de Entendimiento, las Partes podrán iniciar negociaciones sobre el asunto concreto.

3. En caso de que una de las Parte se aparte de las obligaciones estipuladas en el presente Memorando de Entendimiento o en sus anexos, la otra Parte podrá decidir suspender los servicios entre las dos redes hasta que se hayan resuelto las cuestiones.

ARTÍCULO 9

Revisiones y modificaciones

1. Las Partes revisarán el presente Memorando de Entendimiento, siempre que una de las Partes lo estime necesario.

2. No obstante lo dispuesto en los artículos 6(1) y 6(3), las modificaciones del presente Memorando de Entendimiento deberán acordarse por las Partes por escrito e incorporarse al mismo.

cve: BOE-A-2018-6725
Verificable en http://www.boe.es

ARTÍCULO 10

Terminación

El presente Memorando de Entendimiento podrá darse por terminado previa notificación por escrito, con tres (3) meses de antelación, por cualquiera de las Partes.

ARTÍCULO 11

Entrada en vigor y firma

El presente Memorando de Entendimiento entrará en vigor al día siguiente de su firma por la última de las Partes.

Firmado por duplicado:

Por España,	Por Eurojust,
Javier Herrera García-Canturri,	*Klaus Rackwitz,*
Director General de Cooperación Jurídica Internacional y Relaciones con las Confesiones, Ministerio de Justicia.	Director Administrativo.
Firma:	Firma:
Firmado en Madrid el 7 de abril de 2015.	Firmado en La Haya el 24 de marzo 2015.

Anexo 1: Código de conexión para la conexión segura Eurojust-España.
Anexo 2: Puntos de contacto técnico.
Anexo 3: Diseño de la conexión segura.

ANEXO 1

Código de conexión para la conexión segura Eurojust-España

1.1 Parte A: Introducción.

El objeto del presente código es garantizar que la conexión segura Eurojust-España y las otras redes y sistemas respectivos de las Partes interconectados con ella se encuentran adecuadamente protegidos contra las amenazas a su confidencialidad, integridad y disponibilidad. Un incidente de seguridad en una de las redes o sistemas de una de las Partes podría potencialmente afectar a la conexión segura Eurojust-España o a las otras redes y sistemas de la otra Parte.

El código de conexión dispone que las Partes aplicarán un conjunto mínimo de requisitos de seguridad y de requisitos de seguridad específicos del sistema a todas las redes y sistemas conectados con la conexión segura Eurojust-España (en lo sucesivo mencionados respectivamente como los «requisitos mínimos de seguridad» y los «requisitos de seguridad específicos del sistema»). El objetivo de unos y otros es reducir a un nivel aceptable el riesgo de que los incidentes de seguridad que ocurran en cualquier punto de las redes o sistemas de una Parte afecten a la seguridad de la conexión segura Eurojust-España o las redes y sistemas de la otra Parte.

Las Partes serán por tanto responsables de la seguridad de la conexión segura Eurojust-España y de sus otras redes y sistemas respectivos desde el punto de demarcación de la conexión segura Eurojust-España hacia su interior.

cve: BOE-A-2018-6725
Verificable en http://www.boe.es

1.2 Parte B: Controles de seguridad.

1.2.1 Requisitos de seguridad específicos del sistema.

Las Partes definirán y establecerán sus propios requisitos de seguridad de la infraestructura de redes y sistemas bajo la forma de requisitos de seguridad específicos del sistema.

Dichos requisitos deberán basarse en la propia evaluación de riesgos de las Partes y cumplir con los requisitos mínimos de seguridad que se definen a continuación. Las Partes llevarán a cabo una evaluación de riesgo previamente a la puesta en marcha de la conexión segura Eurojust-España. Posteriormente, las Partes realizarán periódicamente nuevas evaluaciones de riesgo durante la vida de la conexión segura Eurojust-España y, en caso necesario y basándose en los resultados de las mismas, las Partes modificarán sus respectivos requisitos de seguridad específicos del sistema en cumplimiento de los requisitos mínimos de seguridad.

Todos los sistemas y flujos de información que constituyen la interfaz de la conexión segura entre Eurojust y España deberán estar incluidos en el ámbito de aplicación de los requisitos de seguridad específicos del sistema.

Los requisitos de seguridad específicos del sistema determinarán las medidas que deberán aplicar las Partes en el nivel de gestión organizativa en forma de políticas, procedimientos y directrices y los controles que deberán aplicarse en el interior de los sistemas que sustentan la conexión segura Eurojust-España.

Se considera que la conexión segura Eurojust-España será un canal de comunicación seguro de transmisión de datos entre los sistemas de tecnología de la información instalados en Eurojust y en los organismos competentes españoles, en el que todos los datos transmitidos estarán cifrados mediante productos criptográficos.

Los requisitos de seguridad específicos del sistema para la conexión segura Eurojust-España concretarán y complementarán los requisitos mínimos de seguridad que deben aplicar ambas Partes para proteger la conexión segura Eurojust-España. Estos últimos afectan a los controles procedimentales, técnicos y materiales, tal como se determina a continuación.

1.2.2 Requisitos mínimos de seguridad.

Las Partes podrán aplicar las medidas que consideren adecuadas en relación con sus propios requisitos de seguridad, políticas de seguridad locales y normativa, a condición de que, con anterioridad a la puesta en marcha de la conexión segura Eurojust-España y durante la vida de la misma, se cumplan los requisitos mínimos de seguridad que se determinan en los apartados 1.2.2.1, 1.2.2.2 y 1.2.2.3.

1.2.2.1 Controles procedimentales.

Cada Parte deberá aplicar los siguientes controles procedimentales, como mínimo:

– Los usuarios de los sistemas y todas las demás personas que intervengan en el ciclo vital de las redes y los sistemas (esto es, las personas que lleven a cabo su gestión y mantenimiento) habrán de tener la debida habilitación de seguridad del nivel oportuno.

– Al otorgarse permisos de acceso debe seguirse el principio de reducción al mínimo y del menor privilegio.

– Las Partes aplicarán políticas y procedimientos de autenticación; esto es, pautas básicas para la creación y gestión de contraseñas.

– Se proporcionará capacitación y concienciación en cuanto a la información a los usuarios y a todas las personas que intervengan en el ciclo vital de las redes y los sistemas de la conexión segura Eurojust-España.

– Se establecerá un procedimiento de evaluación y homologación de los productos incorporados a los sistemas que constituyen la interfaz de la conexión segura entre Eurojust y España.

cve: BOE-A-2018-6725
Verificable en http://www.boe.es

– Deberá designarse un organismo responsable de la garantía de la información, la certificación criptológica, la acreditación de seguridad, la distribución criptológica y la gestión de la clave criptográfica.

– Se establecerán y se ejecutarán de forma periódica normas de contabilidad y auditoría para los sistemas de conexión.

– La información relacionada con incidentes de seguridad que puedan interferir potencialmente con la seguridad de las otras redes y sistemas de una de las Partes de la conexión segura Eurojust-España deberá trasladarse de inmediato a la otra Parte. En la Parte C de este anexo se incluye una lista no exhaustiva de lista de los incidentes de seguridad mencionados.

1.2.2.2 Controles técnicos.

Cada Parte aplicará los siguientes controles técnicos adecuadamente configurados:

– Dispositivos de seguridad fronteriza (perimetral), como cortafuegos o filtros de routers.

– Tecnologías contra los programas maliciosos apoyadas en políticas y estrategias contra dichos programas.

– No podrá conectarse a la conexión segura Eurojust-España, ni utilizarse para acceder al punto de demarcación de la misma, ningún puesto de trabajo directamente conectado a una red informática pública (como Internet) o a una red sin protección.

– Los sistemas que estén conectados a una red informática pública, como Internet, o a una red sin protección, deberán configurarse adecuadamente para proteger la conexión segura Eurojust-España de las amenazas que se generen en la red pública o en la red sin protección.

– El cifrado del tráfico de datos deberá ser del nivel adecuado a la clasificación/sensibilidad de la información intercambiada.

– Las evaluaciones de la seguridad de la información, las identificaciones de vulnerabilidades y las pruebas deberán realizarse de forma periódica, para garantizar que las vulnerabilidades se detectan y remedian.

– La administración de parches y los procedimientos de mantenimiento del sistema deberán realizarse de forma periódica y con arreglo a los calendarios acordados.

– Deberían establecerse medidas técnicas que impidan el intercambio de mensajes de correo electrónico entre las Partes a través de líneas de comunicación no seguras.

– El tráfico de correo electrónico debe controlarse de forma periódica para garantizar que los mensajes de correo electrónico intercambiados entre las Partes se encaminan únicamente a través de canales de comunicación seguros y no de redes públicas o sin protección.

– Deberán tomarse medidas técnicas para proteger las claves de cifrado y evitar su divulgación.

1.2.2.3 Controles físicos.

Cada Parte deberá aplicar los siguientes controles físicos:

– Los sistemas de conexión deberá estar adecuadamente situados en un lugar seguro.

– Los equipos sensibles, como consolas, el equipo del servidor, cortafuegos, interruptores de red, routers y dispositivos de cifrado emplearán controles de acceso físicos.

– El acceso a los puestos de trabajo, terminales, etc., en los que exista la posibilidad de acceso a la conexión segura Eurojust-España, deberá estar limitado físicamente. En el caso de que, por razones organizativas u operativas, los puestos de trabajo deban estar situados en áreas de acceso público o trasladarse a través de las mismas, los equipos se protegerán físicamente en todo momento del acceso no autorizado, el robo o la pérdida.

cve: BOE-A-2018-6725
Verificable en http://www.boe.es

1.3 Parte C: Ejemplos de incidentes de seguridad.

La siguiente es una lista no exhaustiva de incidentes que pueden generar una alerta de seguridad. Estos incidentes, como mínimo, se investigarán y, cuando sea procedente, se notificarán a la otra Parte para garantizar que la información no se ve comprometida.

«Comprometida» significa que, como resultado de una infracción de la seguridad, se ha revelado información, total o parcialmente, a personas no autorizadas.

– Detección de malware.

– Pérdida o robo de equipamiento que contenga información de una Parte o se utilice para procesarla o información relativa a los usuarios, acreditaciones, configuración de la herramienta de cifrado o configuración del sistema.

– Toda actividad inusual detectada por los sistemas o al analizar los archivos de registros, como la autorización a un usuario fuera del horario laboral, trasmitir información a un destino sospechoso o no autorizado, etc.

– Se han dado varios ataques sostenidos a puertos IP de las redes de las Partes.

– Un sistema no responde como se espera.

– Cualquier otro incidente que plantee una amenaza real o potencial al entorno informático y a la información de las Partes.

ANEXO 2

Puntos de contacto técnico

2.1 Eurojust.

En el caso de Eurojust, el punto de contacto técnico será:

Nombre/Cargo: ICT Operations Sector/User Support.
Dirección: Maanweg 174. 2516 AB La Haya. Países Bajos.
Correo electrónico: usersupport@eurojust.europa.eu
Teléfono: 0031 70 412 5677.
Fax: 0031 70 412 5675.

2.2 España.

En el caso de España, el punto de contacto técnico será:

Nombre/Cargo: División de Tecnologías de la Información y las Comunicaciones, Subsecretaria, Ministerio de Justicia.
Dirección: C/ Bolsa, 8 28071 Madrid (España).
Correo electrónico: secretaria.dtic@mjusticia.es
Teléfono: 918388882.
Fax:

ANEXO 3

Diseño de la conexión segura Eurojust-España

3.1 Parte A: Introducción

El objeto del presente anexo es garantizar que la conexión segura Eurojust-España, así como el servicio seguro de encaminamiento de correo electrónico que se proporciona sobre esta red, está establecida y configurada por cada Parte de conformidad con las especificaciones del diseño acordadas.

Este documento facilita una pormenorizada descripción del establecimiento de la conexión segura Eurojust-España, que incluye el establecimiento de la conexión de la red como tal y una solución para encaminar los correos electrónicos intercambiados entre las dos Partes a través de esta conexión.

cve: BOE-A-2018-6725
Verificable en http://www.boe.es

Las disposiciones sobre el diseño y control establecidas en este artículo son vinculantes para Eurojust y España. Deberán cumplirse y respetarse las especificaciones del diseño y los parámetros de la conexión, así como los procedimientos de control y las obligaciones contenidas en el mismo.

3.2 Parte B: Parámetros de conexión.

La conexión segura Eurojust-España trabaja sobre la conexión s-TESTA ya existente. Los cortafuegos en s-STESTA, Eurojust y España se configurarán para permitir los siguientes tráficos.

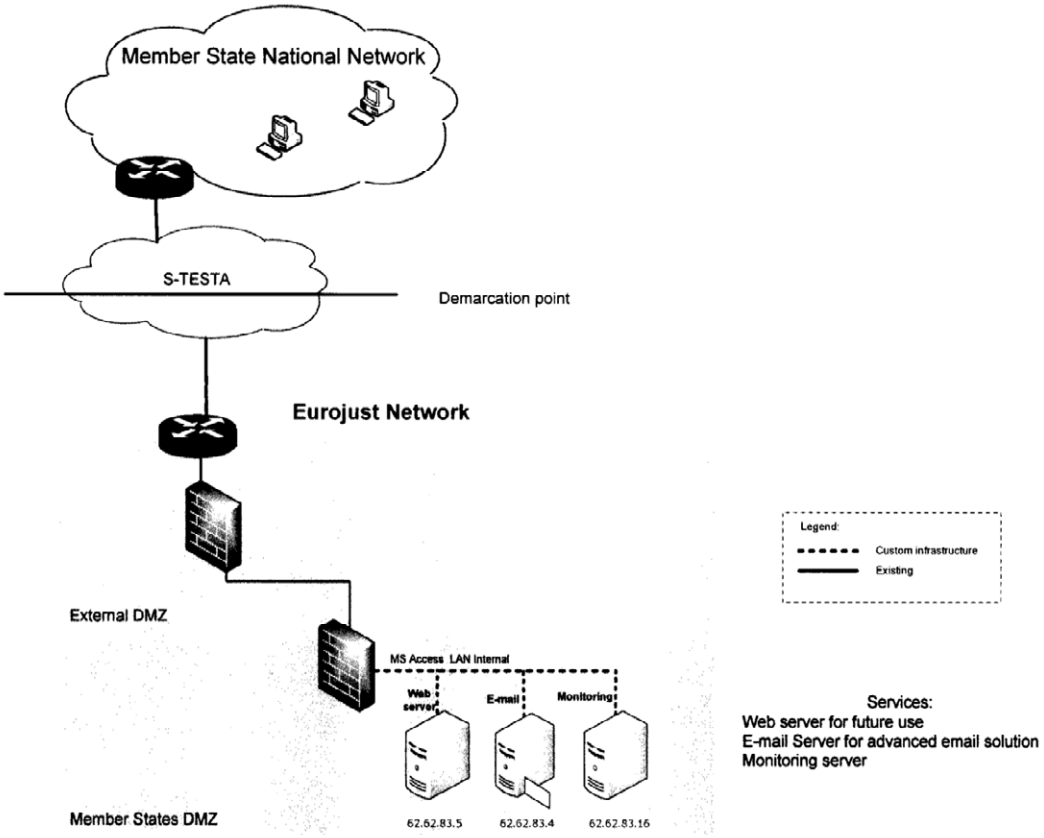
Definiciones:

EJ-SMTP: 62.62.83.4
EJ-MON: 62.62.83.16
MS-OUT-SMTP: 62.62.6.143
MS-IN-SMTP: 62.62.6.143
MS-MON: 62.62.6.143

Normas de acceso a la red:

– Permit MS-OUT-SMTP -> EJ-SMTP TCP 25
– Permit EJ-SMTP -> MS-IN-SMTP TCP 25
– Permit EJ-MON -> MS-IN-SMTP ICMP
– Permit MS-MON -> EJ-SMTP ICMP

Se ruega tomar nota de que en algunos casos, por ejemplo, si existe una NAT interna, puede ser necesario adaptar estas normas.



cve: BOE-A-2018-6725
Verificable en http://www.boe.es

3.3 Parte C: Encaminamiento seguro de correo electrónico

El sistema de correo electrónico se configurará para encaminar los correos electrónicos a través de la línea segura establecida entre Eurojust y España.

España:

Los correos electrónicos para @*.euroiust.europa.eu: se enviarán a 62.62.83.4.

Eurojust:

Los correos electrónicos para @*. mjusticia.es:se enviarán a 62.62.6.143.

cve: BOE-A-2018-6725
Verificable en http://www.boe.es

Lo siguiente es la cabecera de un correo electrónico enviado de España a Eurojust utilizando el Encaminamiento seguro de correo electrónico. La dirección resaltada muestra cómo se recibió el correo electrónico a través de s-TESTA.

```
Received: from EXTMS-EDGEl.eurojust.europa.eu (10.103.27.4) by
HV1-CASHT2.eurojust.eu.int (10.200.52.134) with Microsoft SMTP Server (TLS)
id 14.3.210.2; Tue, 13 Jan 2015 11:21:15 +0100
Received: from vifexch02.minjus.es (62.62.6.143) by
EXTMS-EDGEl.eurojust.europa.eu (10.103.27.4) with Microsoft SMTP Server id
14.3.210.2; Tue, 13 Jan 2015 11:21:14 +0100
Received: from OCEXCH02.minjus.es ([fe8O::40e0:5f6a:67fe:1550]) by
vifexch02.minjus.es ([::1]) with mapi id 14.03.0181.006; Tue, 13 Jan 2015
11:21:14 +0100
From: "GARCIA CORPAS, JOSE MANUEL" <josemanuel.garciac@externos.mjusticia.es>
To: SER-TEST <SER-TEST@eurojust.local>
CC: ComSeg <ComSeg@mjusticia.es >, EJD IT Projects Team
                  <EJD-IT@eurojust.europa.eu>
Subject: RE: Test email. Test 5
Thread-Topic: Test email. Test 5
Thread-Index:
AdAUWHNFOLhS2391QgirIHgrA/xd8gAAM/agBb7hEMAAAC9ZOAAAHApgAAAhnEAAJvj8OACUk5+QADVz
7yA=
Date: Tue, 13 Jan 2015 10:21:13 +0000
Message-ID: <FF58FD63189FD5489D5DBD8E3BDAC463475345DF@ocexch02.minjus.es>
References: <5E74C52619797344BC735EOBE9229CA5475EFO39@ocexch02.minjus.es>
<FF58FD63189FD5489D5DBD8E3BDAC46347530679@ocexch02.minjus.es>
<798242E932715047B5982AF30D6AE9599F310C66@HV1-MBX2.eurojust.eu.int>
<FF58FD63189FD5489D5DBD8E3BDAC46347533F22@ocexch02.minjus.es>
<798242E932715047B5982AF30D6AE9599F310C74@HV1-MBX2.eurojust.eu.int>
<798242E932715047B5982AF30D6AE9599F31OC92@HVl-MBX2.eurojust.eu.int>
<FF58FD63189FD5489D5DBD8E3BDAC4634753405F@ocexchO2.minjus.es>
<798242E932715047B5982AF30D6AE9599F327D8C@HVl-MBX2.eurojust.eu.int>
In-Reply-To: <798242E932715047B5982AF30D6AE9599F327D8C@HV1-MBX2.eurojust.eu.int>
Accept-Language: es-ES, en-US
Content-Language: es-ES
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator:
x-originating-ip: [192.168.73.136]
Content-Type: multipart/mixed;
              boundary="_006_FF58FD63189FD5489D5DBD8E3BDAC463475345DFocexchO 2m
injuse_"
MIME-Version: 1 .0
Return-Path: josemanuel.garciac@externos.miusticia.es
X-MS-Exchange-Organization-AuthSource: HV1-CASHT2.eurojust.eu.int
X-MS-Exchange-Organization-AuthAs: Anonymous
X-MS-Exchange-Organization-AVStamp-Mailbox: SYMANTEC;539754624;0;info
```

cve: BOE-A-2018-6725
Verificable en http://www.boe.es

Lo siguiente es la cabecera de un correo electrónico enviado de España a Eurojust utilizando el Encaminamiento seguro de correo electrónico. La dirección resaltada muestra cómo se recibió el correo electrónico a través de s-TESTA.

```
Received: from mail.mjusticia.es (192 168.73.254) by OCFEXCH02.minjus.es
(192.168.73.182) with Microsoft SMTP Server id 14.3.181.6; Mon, 12 Jan 2015
09:56:07 +0100
X-IronPort-Anti-Spam-Filtered: true
X-IronPort-Anti-Spam-Result:
ArOEALCLs1TAgEmI/2dsb2JhbABbgkOBFVgEuGWNFYVxAoFTAQEBAQF9hAwBAQEEBRULAgYBGxsDAgEP
EAIBCAOEAwEBAQYBAgIPAQEFAQYHAgUQAQUCBwwUCQgCBA4EAQYCBogjCMsIAQEBAQEBAQEBAQEBAQEB
AQEBAQEBF48XDwECARgGBAICAwIJCQEOAwYBBAIDGgSCb4ETBYQ7hQAGgyGBFEuCCgFOhlcwgkKCL4gO
gzqEEG8BgQs5fgEBAQ
X-IronPort-AV: E=Sophos; i="5.07,742,1413237600";
d="gif'147?scan'147,208,217,147";a="5668032"
Received: from unknown (HELO EXTMS-EDGEl.eurojust.europa.eu)
([192.168.73.136]) by mail.mjusticia.es with ESMTP; 12 Jan 2015 09:52:27
+0100
Received: from HV1-CASHT2.eurojust.eu.int (10.200.52.134) by
EXTMS-EDGEl.eurojust.europa.eu (10.103.27.4) with Microsoft SMTP Server (TLS)
id 14.3.210.2; Mon, 12 Jan 2015 09:55:38 +0100
Received: from HV1-MBX2.eurojust.eu.int ([fe80::4d2b:b012:a8lb:648a]) by
HV1-CASHT2.eurojust.eu.int ([fe80::cca5:57fb:540a:bOOl%14]) with mapi id
14.03.0210.002; Mon, 12 Jan 2015 09:55:36 +0100
From: SER-TEST <SER-TEST@eurojust.local>
To: "'GARCIA CORPAS, JOSE MANUEL" <josemanuel.garciac@externos.mjusticia.es>
CC: ComSeg <ComSeg@mjusticia.es>, EJD IT Projects Team
<EJD-IT@eurojust.europa.eu>
Subject: RE: Test email. Test 5
Thread-Topic: Test email. Test 5
Thread-Index:
AdAUWHNFOLhS2391QgirIHgrA/xd8gAAM/agBb7hEMAAAC9ZOAAAHApgAAAhnEAAJvj8OACUk5+Q
Date: Mon, 12 Jan 2015 08:55:35 +0000
Message-ID: <798242E932715047B5982AF30D6AE9599F327D8C@HV1-MBX2.eurojust.eu.int>
References: <5E74C52619797344BC735EOBE9229CA5475EF039@ocexchO2.minjus.es>
<FF58FD63189FD5489D5DBD8E3BDAC46347530679@ocexch02.minjus.es>
<798242E932715047B5982AF30D6AE9599F310C66@HV1-MBX2.eurojust.eu.int>
<F F58FD63189FD5489D5DBD8E3BDAC46347533F22@ocexchO2.minjus.es>
<798242E932715047B5982AF30D6AE9599F310C74@HV1-MBX2.eurojust.eu.int>
<798242E932715047B5982AF30D6AE9599F310C92@HVl-MBX2.eurojust.eu.int>
<FF58FD63189FD5489D5DBD8E3BDAC4634753405F@ocexch02.minjus.es>
In-Reply-TO: <FF58FD63189FD5489D5DBD8E3BDAC4634753405F@ocexchO2.minjus.es>
Accept-Language: en-GB, nl-NL, en-US
Content-Language: en-US
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator:
x-originating-ip: [10.107.15.1]
Content-Type: multipart/related;
boundary="_004_798242E932715047B5982AF30D6AE9599F327D8CHV1MBX2eurojust_";
type="multipart/alternative"
MIME-Version: 1.0
Return-Path: SER-TEST@eurojust. local
X-MS-Exchange-Organization-AuthSource: ocfexch02.minjus.es
X-MS-Exchange-Organization-AuthAs: Anonymous
```

cve: BOE-A-2018-6725
Verificable en http://www.boe.es

3.4 Parte D: Control de la conexión segura.

3.4.1 Control de la conexión.

Cada Parte decidirá los pormenores técnicos específicos y las herramientas para el control de la conexión. El requisito mínimo es que se controle la disponibilidad de al menos un sistema en el otro extremo de la conexión. El control debe ser automático y repetido periódicamente, al menos cada 10 minutos. Cuando se detecte un problema, se emitirá un aviso, para que pueda examinarse el problema.

3.4.2 Control del encaminamiento seguro de correo electrónico.

A menos que se haya acordado previamente por las Partes, no debe modificarse la configuración previamente descrita del Encaminamiento seguro de correo electrónico. En caso de modificación este Anexo deberá actualizarse con arreglo a ello. Cada Parte debe asegurarse de que esta configuración no se ve afectada por ningún medio (actualizaciones de software, mejora del servicio de correo electrónico, parches, etc.). Por esta razón, cada Parte revisará periódicamente la configuración.

* * *

El presente Acuerdo Administrativo entró en vigor el 8 de abril de 2015, según se establece en su artículo 11.

Madrid, 16 de mayo de 2018.–El Secretario General Técnico, José María Muriel Palomino.

cve: BOE-A-2018-6725
Verificable en http://www.boe.es