ASPECTOS DE SEGURIDAD SOBRE LA TRANSMISIÓN DE DOCUMENTOS JUDICIALES A TRAVÉS DEL CORREO ELECTRÓNICO CONVENCIONAL, SU PROCEDENCIA, BUENAS PRÁCTICAS Y ERRORES A EVITAR

VASSILEIOS KARAGIORGOS
Director de DGE Bruxelles

En el entorno de la administración de la Justicia en el que se desarrolla la procura, proliferan durante los últimos tiempos iniciativas de comunicación telemática, expresadas fundamentalmente mediante el lanzamiento del LexNet como manifestación de 'e-justicia'. Dentro de este proceso, todas las partes implicadas: abogados, procuradores y sus representados; y en menor grado los propios juzgados; están realizando un uso de correo electrónico cada vez más extensivo. En este punto, debemos recordar, que la propia LEC (artículo 152.3.2ª) incluye, entre los actos de comunicación, el correo y otros medios electrónicos que dejen constancia de su recepción, su fecha y hora, y su contenido. Mediante esta definición de la ley se descarta cualquier duda sobre la validez del email como acto de comunicación válido salvo la primera comunicación a la parte demandada que todavía se debe realizar mediante correo certificado (ver al respecto, la sentencia 47/2019 del Tribunal Constitucional, de 8 de abril de 2019).

No obstante, nunca tenemos que olvidar que un uso indebido de estas herramientas podría provocar serios daños sobre los intereses, tanto propios como de nuestros representados. Entre los riesgos derivados podríamos contemplar: riesgos legales (riesgo de sanción por incumplimiento de la normativa de protección de datos, secretos profesionales, etc.), riesgos reputacionales y, por supuesto, riesgos operacionales (por ejemplo, bloqueo de todo nuestro sistema de información a causa de la infección por un malware introducido mediante un correo electrónico, etc.).

A continuación, expondremos unas breves pautas sobre el uso responsable del correo electrónico como herramienta de comunicación de nuestro despacho. Para más información al respecto, el lector puede consultar el 'Decálogo de medidas de seguridad en el correo electrónico' del Instituto Nacional de Ciberseguridad (INCIBE)[1]:

Ante cualquier duda con respecto a la identidad del remitente, no debemos abrir el correo electrónico recibido, o, al menos, no hacer clic en enlaces incluidos en correos electrónicos de remitentes desconocidos.

Tener instalada, y permanentemente actualizada, una aplicación antivirus incluyendo antimalware y activando los filtros antispam.

Usar siempre contraseñas seguras (como mínimo, 8 o más caracteres e incluir mayúsculas, minúsculas y letras o caracteres especiales). Dichas contraseñas deben cambiarse periódicamente, y al menos, una vez al año.

Evitar utilizar el correo electrónico desde conexiones públicas, como puede ser, por ejemplo, desde la wifi de una cafetería, el ordenador de un hotel, etc. Es mucho más seguro si utilizamos las redes de telefonía móvil, como el 3G o el 4G.

Cifrar el correo electrónico al enviar información confidencial. Esta particularidad no es solamente por un tema de seguridad informática, sino por un deber de cumplimiento legal, ya que la ley en materia de protección de datos nos obliga a cifrar cualquier comunicación efectuada a través de las redes que incluya datos sensibles, que, en el caso de procura, pueden ser datos o ficheros incluidos en expedientes jurídicos que recogen datos de infracciones penales, datos de salud, etc.). El cifrado puede aplicar en todo el correo electrónico, incluyendo el cuerpo y sus ficheros adjuntos, o únicamente los adjuntos del email. Sin ninguna duda, la opción más segura es cifrar la totalidad del correo electrónico enviado, de esta manera nadie que no fuera el remitente y el destinatario del mensaje podrían acceder a su contenido. Para ello se pueden utilizar varias herramientas como por ejemplo; Enigmail, GPG o la extensión de Google Chrome Mailvelope[2].

Si lo que nos interesa proteger es el contenido de los ficheros adjuntos, entonces podemos enviar dichos adjuntos como documentos comprimidos y cifrados. Para ello, podríamos utilizar, por ejemplo, la opción de cifrado de aplicaciones de comprimido como WinRAR, 7-Zip o WinZip o el servicio de cifrado de ADOBE Acrobat. En cualquier caso, cuando utilizamos opciones de cifrado basadas en contraseñas nunca debemos enviar dicha contraseña, no solamente en el mismo correo del adjunto si no, ni siquiera mediante el mismo medio, es decir, por correo electrónico. Al contrario, deberíamos

enviar la contraseña mediante otro medio como puede ser un WhatsApp, SMS o incluso, quizás la opción más segura, verbalmente por teléfono.

No publicar direcciones de correo electrónico, salvo quizás una genérica, en la web de la empresa ni en sus redes sociales. Los ciberdelincuentes rastrean todas las páginas web y redes sociales con el objeto de localizar direcciones de correo electrónico dentro de las mismas. Asimismo, nunca debemos responder al correo basura si no bloquearlo directamente mediante las opciones del 'correo no deseado' de nuestro programa de correo electrónico. En caso de proceder de otra forma lo que conseguiremos es simplemente confirmar a los spammers la existencia de nuestra cuenta.

Utilizar la copia oculta (BCC o CCO) cuando se envíen direcciones a múltiples destinatarios. Igual que en el tema de cifrado del contenido del correo, este punto no responde solamente a una medida lógica de seguridad sino a una exigencia legal una vez que si emitimos a todos los destinatarios en copia visible entonces revelaríamos su identidad al resto de destinatarios habiendo acometido, conforme al nuevo Reglamento de Protección de Datos, una brecha de seguridad con respecto a la confidencialidad de los datos. **Además, según incidencia ocurrida, la ley nos exige evaluar la necesidad de comunicar dicha brecha a la Agencia de Protección de Datos o, incluso, también a las propias personas afectadas.**

Como conclusión a esta breve reseña, podríamos afirmar que la solución a la práctica totalidad de los problemas vinculados al uso del correo electrónico la podemos encontrar en la formación y concienciación de sus usuarios. Según indica el propio INCIBE, "una formación en ciberseguridad a los empleados supone una gran inversión que traerá consigo un enorme beneficio en términos de evitar ataques, fraudes, sustos y mejorar la imagen de la compañía".

Para acceder al documento integro del INCIBE:

Para ver como instalar las herramientas **GPG** y **Google Chrome Mailvelope** pueden consultar está guía de la Oficina de Seguridad de Internauta (OSI):

ILUSTRE COLEGIO DE
PROCURADORES
DE MADRID

Revista nº 52
1er semestre 2020
www.icpm.es

Profesionales: servicio público en primera línea

Tribuna del decano del ICPM, Gabriel M.ª de Diego

Los procuradores: pieza fundamental para agilizar la administración de Justicia.

Entrevista al ministro de Justicia, Juan Carlos Campo