II INFORME SOBRE LA NECESIDAD LEGAL DE CIFRAR INFORMACIÓN Y DATOS PERSONALES

Presentado por el Despacho de Abogados con especialización en tecnología y protección de datos: ABANLEX

Incluye “Análisis de la Seguridad SSL Implementada en Ayuntamientos Españoles” realizado por Securizame

ABANLEX

SECURIZAME

SOPHOS

ÍNDICE

Informe Legal

1. Cifrar de forma legal es accesible, fácil y posible
2. Cifrar es el medio técnico correcto
3. Quién está obligado a cifrar en España
4. Requisitos que debe cumplir un cifrado legal
5. La importancia de cifrar de forma legal
   - 5.1. Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD).
   - 5.2. Reglamento de Desarrollo de la LOPD (RLOPD).
   - 5.3. Ley de Autonomía del Paciente (Ley 41/2002).
   - 5.4. Código Deontológico de la Abogacía Española
   - 5.5. Ley 9/2014, General de Telecomunicaciones (LGT) y Reglamento (UE) nº 611/2013
   - 5.6 El secreto profesional periodístico
   - 5.7 Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (LPBC)
   - 5.8. Esquema Nacional de Seguridad (ENS)
   - 5.9. Próximamente: el Reglamento Europeo de Protección de Datos.
6. Cifra el contenido que subes a Dropbox
7. Más motivos para cifrar
   - 7.1. Protección de la propiedad intelectual
   - 7.2 Protección de los secretos comerciales
   - 7.3. Protección contra el espionaje industrial
   - 7.4. Protección para aceptar BYOD (Bring Your Own Device)
   - 7.5 Protección adicional para generar seguridad
8. Libertades y precauciones sobre el cifrado
   - 8.1. Cifrado selectivo
   - 8.2 Otorga o restringe acceso a los distintos empleados

Informe Ayuntamientos

1. Alcance y Objetivos
2. Las necesidades de cifrado
3. Sobre los protocolos SSL y TLS
4. SSL/TLS a día de hoy
5. Implementación de SSL/TLS en los Ayuntamientos Españoles
6. Análisis de los resultados
7. Conclusiones y reflexiones

Esta obra está bajo una licencia de
Creative Commons Reconocimiento-SinObraDerivada 4.0 Internacional.

PARTE 1 - Informe Legal

1 Cifrar de forma legal es accesible, fácil y posible

Cifrar datos de forma correcta es una de las obligaciones que impone la normativa española para una inmensa cantidad de empresas. Muchas de ellas no cifran por miedo o desconocimiento. Cifrar no es complicado, el coste es asequible y los beneficios se muestran desde el inicio.

2 Cifrar es el medio técnico correcto

El Gabinete Jurídico de la Agencia Española de Protección de Datos recuerda, en su Informe 494/2009**, cuál es la importancia del cifrado correcto**, de manera que sea legal y suficiente:

"*La seguridad en el intercambio de información de carácter personal en la que hay que adoptar medidas de seguridad de nivel alto, en particular los requisitos de cifrado de datos, no es un tema baladí, ni un mero trámite administrativo, ni una cuestión de comodidad.* ***Es el medio técnico por el cual se garantiza la protección de un derecho fundamental y al que hay que dedicar el tiempo y los recursos que sean necesarios para su correcta implementación***".

3 Quién está obligado a cifrar en España

Deben cifrar datos los siguientes tipos sujetos y empresas:

- Los sujetos que tengan los siguientes ficheros de datos personales o realicen los tratamientos de datos de carácter personal que se indican: (art. 81.3 RLPOD):

  - Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

  - Los que contengan o se refieran a datos recabados para fines policiales . sin consentimiento de las personas afectadas

  - Aquéllos que contengan datos derivados de actos de violencia de género.

- Los sujetos obligados al cumplimiento de la normativa de prevención del blanqueo de capitales y de la financiación del terrorismo (art. 2 Ley 10/201), respecto de determinados ficheros que están obligados a crear (art. 15 y 32 Ley 10/2010)

- Sujetos que gestionan ficheros de whistleblowers, respecto del conjunto ordenado de datos de carácter personal de alertadores y potenciales incumplidores (Informe AEPD)

- Abogados en el ejercicio de su profesión, respecto del fichero de clientes (arts. 18 y 24 CE y art. 5 Código Deontológico)

- Las Administraciones públicas en cumplimiento del Esquema Nacional de Seguridad (Anexos RD 3/2010)

- Empresas que adheridas a un Código Tipo que obligue al cifrado (art. 72 RLOPD)

- Empresas que aceptan el BYOD (CCN-CERT IA-21/13)

- Empresas que deseen proteger sus creaciones (art 1 LPI)

- Empresas que deseen proteger sus secretos comerciales (art. 13 LCD)

- Empresas que deseen proteger minimizar el espionaje industrial (art. 278, 279 y 280 CP)

- Empresas que deseen adoptar medidas de seguridad que superen el mínimo exigido (art. 81.7 RLPOD)

4 Requisitos que debe cumplir un cifrado legal

Cuando la normativa española exige cifrado, otorga a las empresas dos posibilidades (art. 104 RLOPD): Un sistemas de cifrado o cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

Artículo 104 del Reglamento de la LOPD

"***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*".**

Únicamente son válidos los sistemas de cifrado que garantizan que la información no sea inteligible ni manipulada por terceros. Cualquier sistema no es suficiente. ¿Pero cuáles son estos? ¿Quién los ha auditado? ¿Hay alguna lista de los que permiten cumplir la ley y los que no?

A la Agencia Española de Protección de Datos se le consultó si los sistemas de cifrados de ciertas herramientas, como las de compresión de archivos (ZIP) y los sistemas de claves de los PDF eran suficientes para cumplir la normativa. El Gabinete Jurídico de la Agencia Española de Protección de Datos, en su Informe 0494/2009, respondió: no son suficientes.

Los productos que generan archivos PDF o el realizado por WinZip tienen vulnerabilidades conocidas y se disponen de herramientas de libre distribución que aprovechan dichas vulnerabilidades. Más concretamente, no sólo se pueden obtener en Internet fácilmente utilidades que rompen las protecciones de los archivos PDF o ZIP, sino que el propio algoritmo en el que descansa la cifra de documentos PDF, el algoritmo RC4, es manifiestamente vulnerable".

La Agencia concluye lo siguiente:

- Para un uso particular, los sistemas generales de cifrado (ZIP, PDF, etc.) podrían considerarse adecuados, según el caso.
- Para un uso profesional, los sistemas generales de cifrado son insuficientes para el intercambio de información con las garantías que se precisan en el Reglamento.

La respuesta para cumplir la normativa se encuentra en las herramientas profesionales pensadas, diseñadas y probadas para cumplir al detalle la normativa vigente en España en materia de cifrado.

5 La importancia de cifrar de forma legal

5.1 Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD).

El objeto de la LOPD es "*garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas*" (art. 1 LOPD).

Las medidas de seguridad que marca la normativa de protección de datos se dividen en tres niveles: bajo, medio y alto. El que más interesa a los efectos de cifrado es el alto, que obliga a cifrar datos, sin desmerecer a los dos anteriores, que también podrán incorporar el cifrado de manera voluntaria.

El incumplimiento de estos deberes de secreto y custodia adecuada se considera una infracción grave. Las sanciones se califican como leves, graves o muy graves, siendo grave la vulneración del deber de guardar secreto, lo cual se sanciona con una multa de 40.001 a 300.000 euros.

Cuando la norma obliga a cifrar datos, el cifrado se debe realizar. Hay que dedicar el tiempo y los recursos que sean necesarios para su correcta implementación, como nos recuerda la Agencia en su Informe 494/2009 y como nos indica la propia LOPD en su articulado.

5.2 Reglamento de Desarrollo de la LOPD (RLOPD).

El objeto del Reglamento es desarrollar la LOPD. Es decir, fortalecer los mecanismos por los que se garantiza y protege, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

La primera referencia expresa a la obligación de cifrado la encontramos en el artículo 101 del RLOPD. El Reglamento obliga al cifrado de datos bajo las siguientes condiciones:

1. El cifrado de datos deberá garantizar que la información no sea accesible o manipulada.
2. Se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.
3. Se evitará el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado.

Cifrar fortalece la seguridad de la empresa y genera confianza en los trabajadores y en los clientes.

5.3 Ley de Autonomía del Paciente (Ley 41/2002).

El objeto de la Ley de Autonomía del Paciente es "*la regulación de los derechos y obligaciones de los pacientes, usuarios y profesionales, así como de los centros y servicios sanitarios, públicos y privados, en materia de autonomía del paciente y de información y documentación clínica*" (art. 1 Ley 41/2002).

El derecho a la intimidad de la persona es uno de los factores de mayor relevancia a la hora de llevar a cabo cifrados adecuados y conformes a la normativa.

Para preservar de forma correcta los derechos de los pacientes, con especial referencia a su intimidad, el artículo 16 de la Ley 41/2002 es claro al determinar que "*el acceso a los datos*" debe de realizarse, en todo caso, por un "*profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto*". De igual forma, "*el personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto*". Este deber de secreto unido a la salvaguarda efectiva del derecho fundamental hacen imprescindible el recurso al cifrado de datos, obligatorio, por otro lado, por el tipo de datos que van a ser tratados y la implantación debida de las medidas de seguridad de nivel alto.

El cifrado de datos es la medida técnica que permite a los centros sanitarios cumplir con su obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad.

El paciente tiene derecho a que los centros sanitarios establezcan un "*mecanismo de custodia activa y diligente de las historias clínicas*" (art. 19 Ley 41/2002). Por tanto, los centros sanitarios tienen la obligación de establecer e implementar dichos mecanismos.

5.4 Código Deontológico de la Abogacía Española

El Código Deontológico de la Abogacía Española establece unas normas deontológicas para la función social de la Abogacía, entre las que se encuentra el deber de secreto, que exige el cifrado de datos.

El cliente espera del abogado que guarde secreto profesional sobre todos los datos que le aporte. En algunos casos los datos están relacionados con la real comisión de delitos, de los que salen impunes o por los que se les condena. El cliente deposita su confianza en el abogado sabiendo que este está obligado a no defraudar su confianza, a guardar secreto sobre todos los datos de su vida personal e íntima que le revele y a que esta información permanezca secreta y confidencial para siempre, durante la relación contractual de asesoramiento jurídico y después de esta. Todo el contenido que el cliente revele al abogado tiene que permanecer a resguardo bajo las más altas y estrictas medidas de seguridad, lo que exige el establecimiento de medidas de nivel alto y, por tanto, del cifrado de todos los datos que se encuentren recogidos en formato digital, así como de las comunicaciones que el abogado mantenga con su cliente.

Los derechos con los que trata un abogado son fundamentales y cuentan con la máxima protección constitucional. El de mayor relevancia es el derecho de los clientes "*a no declarar contra sí mismos, a no confesarse culpables y a la presunción de inocencia*" (art. 4 CDAE).

El secreto profesional es un derecho y deber primordial de la Abogacía que merece el mayor de los respetos y que obliga a la implantación de medidas de nivel alto a los ficheros en los que se guarden datos de clientes. Por tanto, todo abogado está obligado al cifrado de, al menos, las carpetas relativas a los casos que lleva, esto es, siempre que se cifren los datos tanto en origen como en destino y en la transmisión de los mismos.

5.5 Ley 9/2014, General de Telecomunicaciones (LGT) y Reglamento (UE) nº 611/2013

Actualmente, la LGT y el Reglamento (UE) nº 611/2013 obligan a las empresas del sector de las comunicaciones electrónicas a notificar las brechas de seguridad que pongan en peligro información personal. En concreto, vincula a los operadores que explotan redes públicas de comunicaciones electrónicas y a los prestadores de acceso a Internet o ISP (Internet Service Providers). Todas ellas han de notificar tales brechas (i) a la AEPD y (ii) a los sujetos interesados cuya información personal se haya visto comprometida, además de (iii) anotar la incidencia en su Documento de Seguridad.

El cumplimiento de esta obligación tiene una consecuencia clara: el sufrimiento de una grave pérdida reputacional entre los clientes de la compañía, ya que se estará poniendo en su conocimiento que las medidas de seguridad implantadas para proteger sus datos son deficientes.

Sin embargo, la normativa excepciona el deber de notificación a los interesados cuando la compañía haya aplicado a los datos personales afectados por la brecha medidas de seguridad que los hayan hecho incomprensibles. Es decir, medidas de seguridad que, como el cifrado, garanticen que quienes obtengan la información de forma ilícita no sean capaces de entenderla. El propio Reglamento europeo 611/2013 menciona expresamente el cifrado seguro como la medida idónea para convertir la información en incomprensible.

5.6 El secreto profesional periodístico

El secreto profesional periodístico es la base sobre la que se sustentan los pilares de la investigación periodística. El artículo 20.1.d) CE reconoce el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de la actividad de los periodistas. El secreto profesional periodístico no sólo implica el derecho a la no publicación de los datos que se quieren proteger, sino también a ocultar la fuente de la información dentro del mismo medio de comunicación, incluso ante superiores jerárquicos, en cuyo caso el cifrado se erige como la mejor herramienta a la mano del periodista para guardar a salvo la información.

Los periodistas deberán atenerse a la Ley 15/1999, de 13 de diciembre, de Protección de Datos, adoptando medidas de seguridad de nivel alto, es decir, cifrando, cuando así lo establezca la ley. En el caso de que se desee publicar datos de carácter personal que requieren un nivel de seguridad alto (datos de ideología, afiliación sindical, religión, creencias, origen racial, salud…) se deberá ponderar siempre la naturaleza de la información de que se trate, el carácter sensible de esta información para la vida privada del individuo, el interés público en disponer de dicha información y el papel que dicha persona desempeñe en la vida pública. Si, una vez aplicado el anterior criterio, los datos no se quisieren o pudieren publicar, el periodista o, en su caso, el medio de comunicación correspondiente, estarán obligados a cifrar la información anterior.

Los periodistas fundamentan la relación con sus fuentes en la confianza, lo cual exige de éste una conducta profesional íntegra y honrada, y, por ende, el periodista está obligado a cifrar todos los ficheros que guarden información conseguida a raíz de una relación periodística basada en el secreto profesional periodístico.

5.7 Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (LPBC)

El objeto de la LPBC es proteger "la integridad del sistema financiero y de otros sectores de actividad económica mediante el establecimiento de obligaciones de prevención del blanqueo de capitales y de la financiación del terrorismo" (art. 1 LPBC). Esta norma exige la implantación de medidas de seguridad de nivel alto sobre ciertos ficheros que almacenan datos de carácter personal y, en consecuencia, el cifrado de estos.

Esta norma es la que, de forma más directa, muestra qué colectivos de sujetos, tanto personas físicas como jurídicas, están obligados a cifrar datos. La lista está contenida en el artículo 2 LPBC y alcanza a abogados, profesionales del arte, joyerías, promotores inmobiliarios, servicios postales, entidades de crédito, notarios, y sociedades de garantía recíproca, entre otros muchos.

El deber de secreto, exige el cifrado de datos.

5.8 Esquema Nacional de Seguridad (ENS)

La finalidad del Esquema Nacional de Seguridad o ENS es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios. Este ENS fue aprobado por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

El ENS hace referencia en varias secciones a la conveniencia o necesidad de cifrar tanto la información como las comunicaciones. Además especifica medidas concretas de seguimiento obligatorio tanto para el uso de criptografía en las comunicaciones, como para el uso de criptografía en los soportes de información.

5.9 Próximamente: el Reglamento Europeo de Protección de Datos

Desde hace varios años, la UE está inmersa en el proceso de tramitación del Reglamento Europeo de Protección de datos, concebido para generar un marco normativo más sólido y coherente en la materia. Se pretende que finalice con las pequeñas diferencias existentes entre los Estados Miembros y que lidie con asuntos relacionados con los nuevos avances

tecnológicos, tales como el cloud computing o la ciberdelincuencia.

Por el momento, este reglamento no es más que una Propuesta que aún debe aprobarse de forma definitiva. Sin embargo, el texto actual ya ha sido aprobado por la Comisión Europea, por lo que nos permite hacernos una idea bastante aproximada de cómo será su redacción final.

Obliga al responsable y al encargado del tratamiento a utilizar medidas técnicas y organizativas adecuadas para garantizar que la seguridad de los datos personales sea adecuada al riesgo existente. Se deben tener en cuenta:

- La tecnología disponible y los costes de aplicación
- La naturaleza, el alcance, el contexto y los fines del tratamiento.
- La probabilidad y gravedad de los riesgos del tratamiento de la información para los interesados. Para ello, se atiende a las consecuencias que se derivarían de la destrucción accidental o ilícita, la pérdida, la alteración, la comunicación o el acceso no autorizado a estos datos.

En relación con la seguridad de la información, el Reglamento Europeo de Protección de datos introduce una gran novedad: implanta la obligación de que el responsable que sufra una brecha de seguridad que afecte a información personal deba ponerlo en conocimiento (i) de la AEPD y (ii) de los afectados. Esta obligación ya existe actualmente, pero se limita a las compañías del sector de las comunicaciones electrónicas. En cambio, el Reglamento no sólo vincula a éstas, sino a cualquier entidad que trate datos personales, sin importar su sector de actividad.

Ahora bien, cualquier empresa puede evitar las nefastas consecuencias reputacionales que tendría esta comunicación a los interesados de una forma sencilla: utilizando un sistema de cifrado que impida a cualquier tercero no autorizado comprender el contenido obtenido. El Reglamento establece, expresamente (artículo 32.3), que cifrar la información personal excluye la obligación de notificar a los afectados que se ha producido una brecha de seguridad en la que se han visto comprometidos sus datos personales.

6 Cifra el contenido que subes a Dropbox

Siempre que vaya a hacer uso de un sistema de cloud computing, el cifrado de los datos personales es "una medida que debe valorarse positivamente", según la Agencia Española de Protección de Datos, como respuesta a la pregunta "¿Cómo puedo garantizar o asegurarme de que se cumplen las medidas de seguridad?", en la 'Guía para clientes que contraten servicios de Cloud Computing'. La AEPD sugiere que se solicite información al proveedor de cloud sobre el cifrado de los datos en todos los casos, no solo en los que haya que cumplir con las medidas de seguridad de nivel alto.

Para la AEPD, en la Guía para clientes que contraten servicios de Cloud Computing, ante la pregunta, un elemento de la seguridad cobra especial relevancia en un entorno 'cloud' es la "*aplicación de técnicas robustas de cifrado tanto a los datos en tránsito como a los datos almacenados*", ya que constituye una medida necesaria para garantizar su confidencialidad.

En relación con las profesiones que exigen secreto profesional y siempre que las medidas de seguridad a aplicar en materia de protección de datos sean de nivel alto, "*el cifrado de datos almacenados es una necesaria medida de seguridad*", según se apunta en el Informe 'Utilización del Cloud Computing por los despachos de abogados y el derecho a la protección de datos de carácter personal. El proveedor ha de dar a conocer "*el nivel de seguridad ofrecido por las técnicas de cifrado de la información que aplique en sus sistemas*", si es que aplica alguno.

7 Más motivos para cifrar

Cifrar siempre es conveniente, aunque no haya ninguna ley que obligue a ello.

7.1 Protección de la propiedad intelectual

Los productores, los creativos, los publicistas y todos los autores en general deben velar por su trabajo en todo momento. Cuando la obra está inacabada o aún no está lista para su divulgación (art. 4 LPI) los autores pueden cifrar su contenido con el objetivo de que sean solo ellos quienes puedan acceder al mismo.

7.2 Protección de los secretos comerciales

Las meras ideas cuentan con una protección legal un tanto indefinida. El cifrado es la solución para que estos secretos, confidenciales, puedan permanecer a la vista de unos pocos privilegiados y ocultos para la sociedad en general.

7.3 Protección contra el espionaje industrial

La comisión de delitos relativos al mercado y los consumidores es, en la era de la tecnología, cada vez más frecuente. Con un mecanismo de cifrado adecuado se consiguen minimizar los ataques exitosos ya que todo lo que verá el intruso es un conjunto de información ininteligible que será incapaz de manipular.

7.4 Protección para aceptar BYOD (Bring Your Own Device)

La tendencia empresarial es el BYOD (Bring Your Own Device) o "Trae tu propio dispositivo". Esta práctica implica una cantidad ingente de riesgos en relación con la protección de la información en todos sus niveles: datos personales, creaciones, secretos comerciales...

INCIBE, el Instituto Nacional de Ciberseguridad, recomienda a las compañías que apuesten por el BYOD que concienciencien al empleado, "*para que en caso de que este lo use para temas de trabajo, incorpore las mismas medidas de seguridad que los dispositivos utilizados dentro de la compañía*". Asimismo, ofrece una recomendación clara en cuanto al cifrado de datos en su artículo 'Móviles personales y otros « wearables » en la empresa: los riesgos del BYOD': "*No permitir el almacenamiento de información sensible dentro del dispositivo. Y en caso de que se produzca recomendar el uso de cifrado.*"

El riesgo de del BYOD es extremo en materia de seguridad. El empleado puede: extraviar el dispositivo, permitir que lo utilicen familiares o amigos, olvidar cambiar la contraseña de acceso, conectarse a través de una red 2G permitiendo la extracción de datos, enchufar su equipo a un cargador USB falso en un bar, instalar malware que envía archivos al exterior o, simplemente, anclar su dispositivo a una red 4G ajena a la propia de la compañía para realizar a través de ella lo que a través de la red de la compañía no podría.

El CERT Gubernamental español (CNN-CERT), que forma parte del Centro Nacional de Inteligencia (CNI), realizó una encuesta a empleados BYOD. Según el CERT, *"el dato más preocupante es que cerca de la mitad de los encuestados no manejan la información corporativa de forma cifrada en su dispositivo personal, incluso el 15,6% dice no saber cómo se debe manejar dicha información"* ('Riesgos y amenazas del Bring Your Own Device (BYOD)'). El CERT señala que este tipo de trabajadores puede conectarse a redes que desconocen que son inseguras, posibilitando "*ciberataques de tipo man-in-the-middle, que podrían interceptar e incluso modificar los datos en tránsito*". Para evitar esta consecuencia, la primera medida de seguridad que recomienda que el CERT adoptar es "usar mecanismos de cifrado fuerte", tales como el uso de redes privadas virtuales VPN con el refuerzo de un sistema propio y eficaz de cifrado de datos.

7.5 Protección adicional para generar seguridad

Las empresas pueden elegir cumplir los "*mínimos exigibles*" (art. 81.7 RLOPD) que marca la normativa de protección de datos o pueden dotar a sus procesos de mayor seguridad y confidencialidad. Cuando una corporación usa datos y realiza tratamientos de nivel bajo y medio puede optar por asegurar la información por medio del cifrado.

8 Libertades y precauciones sobre el cifrado

Es posible llevar a cabo un cifrado selectivo de datos, así como otorgar permisos de acceso a determinados usuarios individualizados o a grupos de trabajadores, de manera que la empresa tenga una capacidad completa de control sobre la información a la que cada usuario tiene acceso.

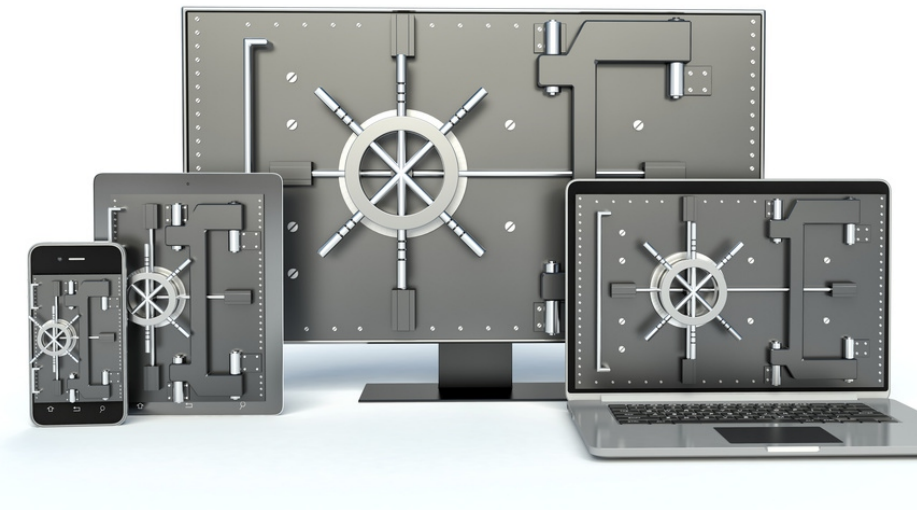
8.1 Cifrado selectivo

Las empresas pueden decidir aplicar el sistema de cifrado solo a una sección de los datos que alberga en un mismo fichero.

8.2 Otorga o restringe el acceso a los distintos empleados

Un sistema de cifrado adecuado que se quiera aplicar a un conjunto de datos que vaya a ser accedido por una pluralidad de personas debe permitir al administrador dotar de derechos de descifrado a algunos usuarios o a determinados grupos de usuarios (por ejemplo, al departamento de recursos humanos o al de marketing) y negar el acceso al resto.

El cifrado de los datos se puede realizar sin excesiva dificultad, con un coste razonable y con la seguridad de que se cumple la ley de forma adecuada. La mayoría de las herramientas de cifrado profesional son modulares o permiten la gestión completa a través de un panel de control específico.



Ahora, generar un búnker legal de uso sencillo aplicando tecnologías completas de cifrado es posible.

Resulta extremadamente recomendable llevar a cabo un cifrado completo de todos los dispositivos del empleado que vayan a ser utilizados también para el trabajo, además de configurar medidas que le permitan abrir determinados archivos, le impidan enviar otros o le bloqueen el borrado o la edición del resto.

PARTE 2 - Informe Ayuntamientos.

1 Alcance y objetivos

El presente documento se concibe como el resultado del análisis de seguridad de diferentes páginas web de contacto del ciudadano, fundamentalmente de la implementación SSL de los servidores web de varios Ayuntamientos españoles.

Para la elaboración del mismo se ha hecho uso de herramientas de uso público, a los que cualquier persona puede acceder.

Los objetivos del documento son presentar el estado actual (Julio de 2015) de varios Ayuntamientos, respecto a las diferentes medidas de seguridad implementadas en la configuración del cifrado SSL, en los servidores en los que los ciudadanos pueden introducir sus datos personales.

Para el estudio, se ha escogido una muestra de los 77 principales ayuntamientos españoles.

2 Las necesidades de cifrado

La Ley 11/2007, del 22 de Junio de Acceso Electrónico de los ciudadanos a los servicios públicos, tiene como objetivo reconocer el derecho a que los ciudadanos puedan relacionarse con las Administraciones Públicas mediante medios electrónicos.

Esto implica que el canal a utilizar para realizar diversos trámites que involucran el intercambio, envío o consulta de datos personales, será Internet. Fundamentalmente este tipo de comunicaciones se llevarán a cabo mediante el estándar HTTP.

Por ende, y por cumplir con la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD), las diferentes Administraciones Públicas tendrán obligatoriedad de aplicar diversas medidas de seguridad, según la clasificación de los datos personales intercambiados.

A partir de aquí, queda en manos de cada Administración, que de forma independiente, implemente dichas medidas de seguridad, de manera más o menos estricta.

3 Sobre los protocolos SSL y TLS

Para dotar de una capa de cifrado a las comunicaciones electrónicas que utilizan típicamente el protocolo HTTP, los dos protocolos más utilizados son SSL (Secure Sockets Layer) y TLS (Transport Layer Security).

Ambos, son protocolos criptográficos que utilizan criptografía de clave pública (o asimétrica) para autenticar a una de las partes (obligatoriamente al servidor) o ambas, siendo opcional la autenticación del cliente.

Para dicha autenticación se utilizan certificados X.509, emitidos y firmados mediante una estructura jerárquica, con diferentes capas basadas en Autoridades Certificadoras y de Registro.

Cada certificado X.509 lleva información que identifica unívocamente a un individuo o una entidad, como el identificador único del sujeto (CN o Common Name, organización, ciudad y país) información relativa al emisor, desde cuándo y hasta cuándo es válido el certificado, la propia clave pública del certificado y el algoritmo utilizado para generarla.

Tanto SSL como TLS, utilizan criptografía de clave pública para las fases de autenticación, intercambio de claves como de firma digital. Sin embargo, para el establecimiento de la comunicación y el intercambio de información entre las partes, se hace uso de criptografía de clave privada, o simétrica.

Un algoritmo se considera seguro, si el tiempo y el esfuerzo necesarios para romperlo y descifrar el contenido sin el conocimiento de la clave, es mayor que el valor del contenido de los datos en sí.

Cada implementación de SSL/TLS, va mejorando de una versión a otra, soportando cada vez algoritmos considerados

más seguros, ya sea por mayor longitud de clave, como por la complejidad criptográfica del algoritmo en sí.

4 SSL/TLS a día de hoy

Hablar de "el día de hoy", en un universo tan volátil y en el que cada mañana se hace pública una nueva vulnerabilidad, se hace complicado.

Un repaso al historial de vulnerabilidades de SSL/TLS

Ya desde el año 2011, desde la publicación de BEAST la industria del software e Internet sufrió un gran revuelo. En 2012, Thai Duong y Juliano Rizzo, publicaron CRIME, otra vulnerabilidad explotable bajo determinadas condiciones, que aprovechaba un fallo en la compresión en los protocolos HTTPS y SPDY.

Pero sin duda, ha sido 2014 el año en el que SSL se haya visto más afectado. Posiblemente, el que mayor repercusión mediática tuvo, fue Heartbleed, ya que permitía leer de forma remota bloques de memoria del servidor. Esto implicaba que un atacante, desde la otra punta del mundo, podía extraer información de uso reciente en el servidor, como credenciales, cookies, e incluso la clave privada SSL utilizada. De esta manera, un atacante sería capaz, bajo ciertas condiciones, de interceptar la comunicación entre cliente y servidor, descifrándola o incluso suplantar a éste.

A finales de 2014 apareció POODLE (Padding Oracle On Downgraded Legacy Encryption) afectando a software que utilizase la versión 3.0 de SSL y posteriormente, una variante que afectaba a TLS. Este tipo de ataque, sería aplicable en escenarios en los que es posible previamente interceptar las comunicaciones entre cliente y servidor, mediante un ataque de Man-in-The-Middle.

Las vulnerabilidades mencionadas afectaban fundamentalmente a las implementaciones SSL de OpenSSL, y por tanto todos aquellos dispositivos que se basasen en ella.

Pero en 2014 no sólo las implementaciones de OpenSSL se vieron afectadas, sino también se descubrieron vulnerabilidades en la implementación de otros fabricantes.

En Marzo de 2015, estrena el año FREAK (Factoring Attack on RSA-Export Keys). Esta vulnerabilidad, que afecta a ambos protocolos SSL y TLS, aprovechándose de un fallo en la negociación inicial, que permite forzar que se utilicen especificaciones de algoritmos RSA con longitudes de clave muy cortas, consideradas crackeables en un tiempo moderado.

Y ya en Mayo de 2015, el último hit a SSL ha sido Logjam. En este caso, el ataque se establece dentro del algoritmo Diffie-Hellman, cuando se usan de 512 a 1024 bits. Una vez más, en un entorno de Man-in-The-Middle, es posible para un atacante establecer un downgrade de la negociación para utilizar un algoritmo de Diffie-Hellman de longitud baja.

Han existido otros ataques a SSL/TLS que han tenido menos repercusión como Lucky13 o Bar Mitzvah, pero que permitían igualmente descifrar contenido parcial o totalmente de las comunicaciones.

Los algoritmos de hashing más populares, MD5 y SHA-1, también han sido reconocidos como no-confiables debido a que en ambos es posible establecer colisiones.

Tras ver la cantidad de vulnerabilidades existentes en diversas implementaciones de SSL/TLS, se considera que SSL está "muerto" y que la única implementación viable es TLS, actualmente en su versión 1.2.

"9 de cada 10 ayuntamientos españoles son vulnerables a los ciberataques

5 Implementación de SSL /TLS en Ayuntamientos

Para el estudio realizado, se ha escogido una muestra representativa de ayuntamientos españoles.

La prueba consiste en introducir el dominio de cada ayuntamiento en la que el protocolo a servir es HTTPS en la herramienta web pública utlizada. Se ha identificado para cada prueba, alguna dirección web a través de la que se envíen datos personales a cada Ayuntamiento.

Por cada prueba, la herramienta ofrece un resultado como el que se puede apreciar en la imagen. La valoración de la seguridad nos dará resultados comprendidos entre la F, el peor resultado, hasta el A+ que es el mejor.

Por confidencialidad, en este informe se establece un resumen de resultados, sin asociarlos a un Ayuntamiento concreto.

6 Análisis de los resultados

Tras la revisión de cada uno de los informes generados por el servicio online se extrae los siguientes:

- La nota más alta otorgada a un Ayuntamiento es la 'A', la más baja es la 'F'. Los resultados son:

  A - 1 Ayuntamiento

  B - 1 Ayuntamiento

  C - 10 Ayuntamientos

  F - 39 Ayuntamientos

  T* - 13 Ayuntamientos

  (*) T - No aplicable porque el certificado está en keystone

  (no se han encontrado datos de 25 de los ayuntamientos estudiados)

- El servidor muestra el nombre del fabricante y su versión y/o de mod_ssl -> 4 ayuntamientos. Sólo el fabricante del servidor, 4 ayuntamientos (la muestra se hizo en 10 ayuntamientos)
- El servidor de 24 de los ayuntamientos analizados soporta SSLv2, considerado inseguro desde hace varios años.
- El servidor es vulnerable a POODLE. Ya sea por soporte de SSLv3 como por TLS, al no soportar la extensión TLS_FALLBACK_SCSV, que mitigaría este problema. Se considera que SSLv3 es inseguro y se recomienda deshabilitarlo http://disablessl3.com/ (27 ayuntamientos)
- El servidor es vulnerable a FREAK: (23 ayuntamientos)
- El servidor es vulnerable a CRIME: Sólo 10 son vulnerables a CRIME por tener activo el soporte de compresión en TLS.
- El servidor soporta parámetros inseguros de intercambio de claves Diffie-Hellman: (15 ayuntamientos)
- El servidor utiliza primos comunes/ conocidos para algoritmo Diffie-Hellman (14 ayuntamientos)
- Sólo soportan TLS v1.2 el 60% de los ayuntamientos analizados, aunque en todos ellos, se soporta al menos TLS v1.0, siendo bastante común el tandem SSLv3 y TLSv1.0, sin dar soporte para TLS v1.1 ni v1.2
- Respecto al algoritmo de firma del certificado SSL presentado por el servidor, dos ayuntamientos utiliza clave privada con RSA de 1024 bits, considerada una longitud de clave insuficiente.

7 Conclusiones y Reflexiones

Tras haber desglosado los diferentes ataques de los que pueden ser víctimas, tanto los servidores, como sobre todo los clientes, que intercambian datos mediante una conexión SSL/TLS, se puede ver que mantener los servicios lo más seguro posible es una labor que requiere dedicación y mantenimiento.

No sólo se trata de actualizar los parches de seguridad, y tener todo el software a la última versión, sino que además, los servicios que hacen uso de SSL, deben estar configurados de forma segura, manteniendo unos niveles de compatibilidad con los algoritmos de cifrado soportados por los dispositivos y sistemas operativos más comunes del mercado.

Las debilidades de los algoritmos de cifrado empleados en las comunicaciones, permitirían el acceso a quien tuviera el conocimiento de la existencia de una vulnerabilidad. Sin embargo, una vez que los detalles de éstas se hacen públicas, es la propia comunidad quien se lanza a construir exploits y herramientas automatizadas que permitan su explotación a cualquiera con unos conocimientos mínimos. De ahí la importancia vital de que cualesquiera sean los sistemas, cuenten con las últimas versiones y parches de seguridad, sean configurados de la forma más exigente y segura posible, así como que formen parte de un programa frecuente de auditorías, con el fin de disminuir los riesgos al mínimo posible.

Se puede decir que prácticamente todos los Ayuntamientos, cumplen con que el tráfico intercambiado entre cliente y servidor "**no sea inteligible ni manipulada por terceros**". Sin embargo, y pese a estar al día con la normativa vigente, sigue habiendo una diferencia entre cumplir una ley y tener una conciencia real de seguridad de la información.

"La mejor protección siempre es un buen cifrado.

LAS CONCLUSIONES DE SOPHOS

Sophos es un fabricante que apuesta por la protección de datos, así lo avalan los siete años consecutivos como líderes en el cuadrante mágico de Gartner de protección de datos.

Figure 1. Magic Quadrant for Mobile Data Protection Solutions

Una correcta política de protección de datos para evitar el 80% de las fugas o robos información más comunes puede ser desplegada en menos de 2 horas. Hoy en día la tecnología de cifrado, dada su baja complejidad, debería estar presente en todas aquellas empresas que deseen proteger su activo más importante: su información.

Con la implementación de las dos prácticas descritas a continuación, podrá asegurar que su empresa u organización:

- Cumple con la legislación descrita anteriormente por el despacho de abogados Abanlex y
- estará protegida ante las amenazas descritas por la empresa Securizame.

Solución SOPHOS para el perímetro

Es muy importante tener los servidores siempre actualizados y configurados de forma segura para disminuir los riesgos ante un posible ataque, sin embargo, esto provoca una sobrecarga administrativa que no siempre se puede asumir, lo que al final deja los servidores con lo que podríamos denominar "dia-1" (concepto opuesto al día-0, donde ya existe parche pero éste no ha sido aplicado).

Ante esta situación, Sophos propone securizar las aplicaciones web con un proxy inverso con reglas de seguridad (WAF, web application firewall), el cual estará focalizado en:

- Impedir la conexión directa entre cliente y servidor. Todo pasará a través del proxy.
- Prevenir ataques, revisando los formularios, evitando la adulteración de cookies, estableciendo permisos adicionales de acceso sobre la aplicación (muchas veces, las aplicaciones son desplegadas por personal ajeno a la seguridad de la corporación).
- Establecer mecanismos de autenticación securizados, adicionales a la propia aplicación.
- Análisis de ficheros subidos/bajados (si la aplicación lo permite) para evitar la propagación de malware.
- Proporcionar una versión siempre actualizada y bastionada de los paquetes SSL/TLS utilizados para securizar la conexión.

Sophos, con los UTM y la licencia de WebServer Protection permite realizar todos estos puntos vistos anteriormente, creando una capa extra de seguridad, la cual es mantenida de forma constante con nuevas reglas/patrones/módulos procedentes de SophosLabs (varias actualizaciones diarias).

La solución WebServer Protection hace las funciones de Proxy y Autenticación Reversas, así como de SSL/TLS "off-loading" (el propio equipo Sophos tendrá el certificado de la aplicación web para realizar la conexión cifrada). Gracias a las actualizaciones automáticas, pese a que nuestro servidor no esté al día con la última versión de sus módulos de cifrado, Sophos proporcionará la seguridad requerida y en las pruebas realizadas con el mismo sistema utilizado

para el análisis de los Ayuntamientos, las pruebas fueron satisfactorias, con la máxima puntuación sin alterar en absoluto la configuración del servidor web.

Sophos WebServer Protection proporcionará:

- Cortafuegos de aplicaciones web: interceptando el tráfico que llega a los servidores para protegerlos contra ataques y manipulaciones, con más de 400 patrones de ataques, incluidas técnicas de inyección de SQL, secuencias de comandos entre sitios y cruce de directorios.
- Antimalware de pasarela: Se podrá escanear todos los archivos de subida y bajada con doble motor antimalware para evitar la entrada de contenido infectado en la red.
- Bastionado de Servidores: Solventa vulnerabilidades en aplicaciones web sin la ayuda de desarrolladores. Se dispone de “hardening” de URL impidiendo que los ciberdelincuentes creen de forma manual "enlaces profundos”. El refuerzo de formularios impide la introducción comandos y códigos maliciosos para aprovechar vulnerabilidades de la base de datos. Y la protección de cookies garantiza que están firmadas para evitar manipulaciones.
- Servidor Proxy Inverso: ofrece autenticación persistente para sus aplicaciones web añadiendo una capa extra de seguridad a servicios como Outlook Web Access para Exchange permitiendo a los usuarios autenticarse contra nuestro proxy inverso exento de vulnerabilidades.

Sophos SafeGuard Encryption: El cifrado es el medio técnico correcto para la protección de datos.

Todas las vulnerabilidades de las que se hablan en este informe tienen el mismo objetivo, interceptar las comunicaciones y sacar toda la información posible, no importa si se llama FREAK, POODLE o CRIME, si afecta a SSL o TLS, si funciona de una manera o de otra, o incluso si se conocen o no dicha vulnerabilidad, nuestros atacantes tienen un objetivo claro, introducirse en nuestro sistema y poder obtener nuestra información.

El problema surge cuando no estamos protegidos contra esas vulnerabilidades, tal vez nuestos servidores están desactualizados, o tienen una versión afectada por un zero-day para la cual actualmente no hay solución ¿Cómo nos enfrentamos a estas dificultades?

El cifrado: un aliado

No importa que alguien acceda a nuestra red y nos robe información, si todo está cifrado, estaremos tranquilos, tendremos una barrera más de seguridad. Incluso si nos roban ficheros y se publican en internet o se venden a terceros, podemos estar tranquilos, sin las claves de cifrado no será posible abrirlos.

Si nos interceptan correos electrónicos nuestra información se mantendrá segura, ya que con **Sophos File Encryption** y con **Sophos SPX** viaja cifrada desde el origen. Suponiendo que se utilizara TLS para cifrar las comunicaciones y éste sufriera de alguna vulnerabilidad, nadie podría leer nuestros ficheros adjuntos porque se cifraron antes de salir.

Las nuevas tecnologías de cloud, permiten alojar nuestra información en lugares ajenos a nuestra empresa

desde los cuales cualquiera pueda acceder, lo cual supone una gran ventaja pero también conlleva un riesgo, no importa donde alojemos nuestra información, si está cifrada desde el origen con **Sophos Cloud Encryption,** podemos subirlo a la nube sin problemas, si alguien accediera a nuestra cuenta o lo interceptara por el camino, no podría verse nada.

Las nuevas tecnologías de cloud, permiten alojar nuestra información en lugares ajenos a nuestra empresa desde los cuales cualquiera pueda acceder, lo que supone una gran ventaja pero también conlleva un riesgo, no importa donde alojemos nuestra información, si está cifrada desde el origen con **Sophos Cloud Encryption,** podemos subirlo a la nube sin problemas, si alguien accediera a nuestra cuenta o lo interceptara por el camino, no podría verse nada.

El cloud no solo se queda en la oficina o en nuestro ordenador, cada vez se utilizan mas los dispositivos móviles, tablets, teléfonos móviles… para ello Sophos dispone de Sophos Secure Workspace, que nos permitirá utilizar los datos cifrados en la nube desde nuestro dispositivo móvil.

Colaboración segura mediante **Sophos File Share**, no importa que compartamos carpetas, podemos cifrarlas y especificar quien puede leerlas independientemente de los permisos que Windows nos haya dado, podríamos evitar que el administrador de sistemas, que tiene permisos para acceder a cualquier parte de la red, leyera información confidencial del departamento de recursos humanos.

Gracias a Sophos Safeguard Encryption se podrán cifrar tanto entornos Windows como Mac y gracias a nuestra gestión de claves podemos compartir información entre ellos de forma segura y transparente para el usuario.

Un descuido en un taxi no debería ser un problema, si perdemos nuestro portátil con toda nuestra información corporativa cifrada con safeguard estaremos tranquilos ya que nuestros datos estarán cifrados con BitLocker (en Windows) o FileVault 2 (en MAC) o incluso las unidades autocifrables Opal.

En caso de auditoria, gracias a **Sophos Safeguard**, podríamos demostrar que cumplimos con las normativas de protección de datos.

Resolver casos complejos de Derecho Tecnológico es la principal función de Abanlex, despacho de abogados especializado en la protección de la información, la privacidad y la innovación jurídica. Los abogados de Abanlex permanecen en la vanguardia de los movimientos legislativos, colaborando en la elaboración de aquellos que tocan sus áreas de ejercicio.

Las soluciones que ha ejecutado para resolver casos de extraordinaria complejidad sitúan a Abanlex como un despacho de referencia internacional en diferentes materias como los nuevos sistemas electrónicos de pago, los sistemas de cifrado o los dispositivos de seguimiento. Sus últimos casos de relevancia internacional son: el Derecho al Olvido contra Google, que ha llevado ante el TJUE y ahora dirige ante la Audiencia Nacional, y los avances en criptomonedas, que le ha valido citas en varios documentos del Gobierno de España y del de Estados Unidos.

Abanlex tiene su sede en Madrid, España. Más información disponible en www.abanlex.com
Abanlex. c/ Velázquez, 109, 7ª Planta. 28006 Madrid. Correo electrónico: info@abanlex.com (@abanlex)

Securízame es una empresa española, integrada por profesionales que cuentan con 15 años de trayectoria dedicada íntegramente a la seguridad de sistemas y comunicaciones, en grandes y medianos proyectos, tanto a nivel nacional como internacional.

Securízame cuenta en su plantilla con profesionales especializados en seguridad informática y sistemas, conferencistas habituales en Congresos Nacionales e Internacionales, con amplia experiencia en consultoría, auditoría, peritaje informático forense y formación reglada en seguridad informática en empresas privadas, administración pública, entornos bancarios, así como Cuerpos y Fuerzas de Seguridad del Estado.

Más de 100 millones de usuarios en 150 países confían en las soluciones de seguridad completa de Sophos como la mejor protección contra amenazas complejas y fuga de datos. De fácil despliegue, administración y uso, las premiadas soluciones para la protección de estaciones de trabajo, web, email, móvil, cifrado y seguridad de red ofrecidas por Sophos, están respaldadas por SophosLabs, una red global de centros de investigación de amenazas.

Sophos ofrece seguridad completa protegiendo todos los puntos, desde la red a los servidores, pasando por las estaciones de trabajo y los dispositivos móviles. Gracias estas soluciones, las empresas podrán concentrarse en las necesidades de su negocio.

Sophos Iberia. c/Orense, 81 1ª Planta. 28020 Madrid. ComercialES@sophos.com (@sophosiberia)
Telf.: 913 756 756 - www.sophos.com/es-es .