CERTIFICADOS DIGITALES

RIESGOS ASOCIADOS A SU USO

La posibilidad de utilizar certificados digitales que permiten agilizar los trámites con las administraciones públicas, conlleva una serie de riesgos que pueden mitigarse mediante la aplicación de unas medidas de control que deben incorporarse al mapa de riesgos de las empresas.

J. Rafel Roig
IT Senior Manager, CIA, CISA, CISM, CRISC & BSI Lead Auditor ISO 27001:2005

Según el artículo 27.6 de la ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos, las administraciones públicas pueden obligar a las empresas a una relación telemática. Ya han hecho uso de esta potestad, por ejemplo, la Agencia Tributaria o la Seguridad Social. Para dotar de garantía suficiente a la relación telemática, en lo que se refiere a la autenticidad de la relación y a la validez jurídica de los actos realizados electrónicamente, en la misma ley se establece el requisito de uso de un certificado digital el cual, según la ley 59/2003 de firma electrónica, permite:

- Identificar de forma fehaciente a una persona física o representante de una persona jurídica en el mundo digital.
- Emitir firmas electrónicas equiparables a la firma manuscrita.

Como resultado, en las empresas empiezan a proliferar certificados digitales que dado su uso aislado y puntual, y en ocasiones adquiridos a raíz de necesidades sobrevenidas, pueden no contar con las actividades de control oportunas. A continuación se introducen algunos de los riesgos relacionados más destacables y que pueden afectar negativamente a los intereses de una empresa:

- Existen distintos tipos de certificados digitales: de persona física, de persona jurídica, de representante de persona jurídica, de empleado de empresa, etc. En el caso de discontinuidad en la empresa de un empleado que disponga de un certificado digital, de vinculación con o representación de la empresa, si su certificado digital no es revocado, seguirá teniendo la misma capacidad de vincular a la empresa en el mundo electrónico.
- Lo mismo pasará en el caso de que se haya comunicado formalmente a una Administración Pública los datos de la persona que pueda actuar en representación de la empresa ante la misma, identificándose con certificado digital de persona física. En el caso de discontinuidad en la empresa de esta persona, si no se informa convenientemente a la Administración Pública, seguirá teniendo la misma capacidad de actuar en el mundo electrónico en representación de la empresa.
- El uso de certificados digitales requiere de ciertos conocimientos específicos y, en caso de certificados basados en tarjeta cripto-

El uso de certificados digitales requiere de ciertos conocimientos específicos y, en caso de certificados basados en tarjeta criptográfica, de elementos hardware específicos. Estos certificados acaban concentrándose en un único ordenador y la persona que lo maneja concentra mucho poder de actuación.

gráfica, de elementos hardware específicos. Como resultado, los certificados digitales a menudo acaban concentrándose en un único ordenador, el de aquella persona de la empresa avanzada en estos temas y en la que se tiene confianza. Esta persona, en el entorno electrónico, acaba teniendo todo el poder de actuación en nombre de las personas a las que pertenecen los certificados digitales que custodia y, en su caso, de representación de la empresa, pudiéndose producir una suplantación de identidad con efectos jurídicos plenos.

- Añadido al anterior, el riesgo no es solo de confianza en la persona que concentra los certificados, sino también de que un ataque a su ordenador pueda ser mucho más perjudicial para los intereses de la empresa ya que, además del acceso no autorizado a información, los certificados digitales que contenga podrían utilizarse de forma malintencionada.
- Un mismo certificado digital, en caso de emisión en soporte software, puede estar replicado en distintos ordenadores y, susceptiblemente, será utilizado por personas distintas al propietario del certificado digital, con el consiguiente riesgo de suplantación de identidad. Este riesgo puede deberse a un mal uso del certificado por parte de su propietario; pero también a problemas organizativos, por ejemplo, en el proceso de cambio del ordenador con el que trabaja habitualmente el usuario sin que se borren los certificados de la máquina anterior o de la que se usa de manera provisional.
- Por el momento, el uso de los certificados digitales no puede limitarse en función de su finalidad, existiendo el riesgo de que un certificado entregado a un empleado sea utilizado para fines distintos a los cuales se había previsto. En estos casos, la empresa ni tan siquiera dispone de mecanismos para identificar este comportamiento, ya que el uso indebido se produce sobre sistemas informáticos no controlados por la empresa, sino en los de las administraciones públicas. Cabe decir que este problema es comparable, en la relación en papel, al bastanteo de poderes (la comprobación de las atribuciones o facultades de un representante), que se suele hacer de manera menos rigurosa en el entorno electrónico para facilitar el acceso a los servicios. Por lo tanto, en estos casos quien asume el riesgo es la Administración.
- Sin una gestión adecuada de los certificados digitales disponibles en una empresa, puede darse el

Hay formas de mitigar los riesgos, como establecer políticas, procedimientos y actividades de control para que el uso de certificados digitales en la empresa se ciña a razones estrictas de negocio y en su beneficio

De interés...

PWC ANALIZA EL IMPACTO DEL REPORTE INTEGRADO

El 63% de los inversores asegura que la integración en un único documento de toda la información corporativa de una compañía -que incluya y vincule aspectos como la estrategia, el modelo de negocio, los riesgos y oportunidades o la información

financiera- puede tener un impacto directo sobre su coste de capital. Es el resultado de los datos del estudio 'Información Corporativa: ¿qué quieren saber los inversores?', de PwC. Solo un 11% opina que dicho impacto no existe. Otro aspecto sobre el que reflexiona el informe es la inclusión, dentro del modelo del reporting integrado, de los asuntos relacionados con la estrategia. El informe señala que la principal petición de los inversores es una mayor claridad en determinar cómo se relaciona la estrategia con el modelo de negocio global de la compañía.

caso que caduquen cuando sea necesario utilizarlos, con lo que pueden generarse situaciones de incumplimiento de los plazos exigidos por una Administración Pública, que puedan derivar en incrementos de costes.

- La pérdida de certificados en soporte hardware o de olvido de las claves que no permitan su uso con el consiguiente impacto en su operatividad para los fines empresariales que motivaron su adquisición.

MITIGAR RIESGOS

Para mitigar estos riesgos, las empresas pueden establecer un entorno de control que minimice el impacto negativo que un uso fraudulento o inseguro de certificados digitales podría tener para sus intereses. Algunas directrices para ello son:

1/Establecer políticas, procedimientos y actividades de control para que el uso de certificados digitales en la empresa se ciña a razones estrictas de negocio y en su beneficio. A grandes rasgos se considerarán:

1.1 Procedimientos de solicitud, renovación y revocación de certificados digitales que garanticen que se adquieran por motivos justificados de negocio y estén disponibles mientras sea necesario.

1.2 Establecimiento de contratos de uso del certificado digital al que queda autorizado el empleado cuando lo obtiene, incluyendo las responsabilidades que comporta su uso y las consecuencias de un uso inapropiado.

1.3 Formación y difusión a los custodios de certificados para que sean conscientes de los riesgos asociados y se genere responsabilidad en su uso.

2/ Mantener un inventario actualizado de certificados digitales disponibles en la empresa, sus responsables, usos autorizados y fecha de caducidad. Este inventario conferirá información de base para la gestión efectiva de certificados.

3/ Utilizar herramientas automatizadas que identifiquen en tiempo real los certificados digitales existentes en la red informática de la compañía y su ubicación, y monitorizar la información en busca de usos inapropiados. Por ejemplo, un mismo certificado replicado en distintos ordenadores, un ordenador con certificados digitales pertenecientes a personas físicas o jurídicas distintas o certificados digitales no relacionados con las actividades de la empresa.

4/ Ampliar el proceso de bajas o modificación de puestos de trabajo de los recursos humanos para considerar la necesidad de revocar certificados digitales o modificar las personas autorizadas a actuar en representación de la empresa ante las administraciones públicas.

5/ En caso de volúmenes elevados de certificados digitales, utilizar servidores centralizados, denominados Hardware Secure Module (HSM), para albergar en un único punto los certificados digitales de toda la empresa. Un HSM, instalado en la sala de servidores de la empresa o en la nube de un tercero de confianza, permite la centralización del control de la seguridad de los certificados, evitando problemas de extravío de las tarjetas o instalación indebida de certificados en soporte software. Además, permite limitar las direcciones web en que no puede utilizarse un certificado digital concreto y registrar las direcciones web en que es utilizado cada certificado digital.

De todo lo antedicho se deduce que, aunque los certificados digitales posibilitan actuaciones telemáticas con efectos jurídicos plenos, agilizando muchas de las actuaciones de la empresa ante la Administración Pública, conlleva riesgos intrínsecos que deben incorporarse al mapa de riesgos de la empresa para su gestión efectiva en aras de evitar perjuicios a nivel económico y reputacional.

EL GOBIERNO APARCA LA LEY DE MECENAZGO

▶ La Ley de Mecenazgo no será finalmente una realidad antes de que acabe esta legislatura. A pesar de que el Gobierno ya ha anunciado que no existirá una norma como tal, el equivalente a lo que se perseguía con la ley se conseguirá a través de la futura Ley de Reforma Fiscal. Esta norma prevé la introducción de muchas ventajas con el objetivo de incentivar la donaciones de empresas y de particulares a la cultura.

OIT: EL DESAFÍO ES CRECER CON EMPLEO DE CALIDAD

▶ El informe 'España: Crecimiento con Empleo', de la Organización Internacional del Trabajo (OIT) insta al Gobierno y a los interlocutores sociales a formular conjuntamente un plan de acción sobre el empleo para evitar el 'crecimiento sin empleo', que tendría un impacto negativo y duradero sobre los españoles.

La OIT señala que mejorar las perspectivas de empleo exige, una estrategia que facilite la transición hacia un nuevo modelo económico.