CANDIDATURA AL PREMIO SOCINFO AL PREMIO SEGURIDD Y PROTECCIÓN DEL DATO

CANDIDATURA

Guía de Orientaciones para la validación de sistemas criptográficos en la protección de datos.

Agencia Española de Protección de Datos

RESUMEN DE LA PROPUESTA DE CANDIDATURA DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Para la candidatura al premio SOCINFO en materia de seguridad y protección de datos se plantea la candidatura del trabajo realizado por el equipo de expertos coordinado por la AEPD desde la División de Innovación y Tecnología que viene a poner en el mercado un conjunto de criterios que permiten evaluar las garantías de privacidad de los sistemas de cifrado, este trabajo es el documento sobre Orientaciones para la validación de sistemas criptográficos en la protección de datos cuya aplicación práctica supera los límites de la protección de datos y abarca la confidencialidad de la información en un sentido amplio.

Con frecuencia se aplican esquemas de cifrado que no proporcionan una garantía adecuada para los fines específicos de confidencialidad que se pretenden. En otras ocasiones de dota de una relativa máscara de apariencia segura mediante la implementación de sistemas de cifrado que no constituyen una garantía eficaz para dichos fines. En definitiva, no existía hasta la fecha un mecanismo que permitiera elegir adecuadamente un esquema de cifrado atendiendo a los objetivos para el que se diseñaba, sin embargo, una de las obligaciones del RGPD es dotar de seguridad a los tratamientos de protección de datos desde el diseño lo que, en la práctica, supone la implementación de modelos de seguridad que incluyan sistemas criptográficos adecuados para garantizar el cumplimiento de las previsiones del artículo 32 del RGPD.

Es preciso tener en cuenta que el propio RGPD plantea el cifrado como una de las obligaciones en materia de seguridad para los responsables y encargados de los tratamientos de datos personales considerando que el cifrado es una garantía limitada en términos de tiempo y medios necesarios para su quiebra. Por otra parte, el RGPD no proporciona criterios para validar un sistema criptográfico dejando esta valoración en el conjunto de decisiones que el RGPD pone en manos de responsables y encargados esta tarea. Este documento viene a dotar de criterios para asumir la implantación de un determinado sistema criptográfico en función de los riesgos que un tratamiento puede entrañar para los ciudadanos, sin embargo, estos criterios son también válidos a la hora de implantar sistemas de cifrado para garantizar la confidencialidad de las operaciones de negocio de cualquier organización.

DESCRIPCIÓN DEL PROYECTO

La presente candidatura supone la implementación de mecanismos para validar sistemas criptográficos que puedan ser incluidos para garantizar la privacidad y la confidencialidad en sistemas de información teniendo en cuenta la generalización de los servicios y las tecnologías de la información y la comunicación alcanzada en nuestra sociedad, puede suponer que dichos criterios criptográficos se conviertan en un estándar español para su validación e inclusión en cualquier sistema de información y comunicaciones con el objetivo de proteger la seguridad de los datos y las informaciones que puedan soportar.

El RGPD menciona explícitamente el cifrado como una medida para la mitigación de riesgos de seguridad en la protección de datos personales para:

- asegurar un nivel de seguridad apropiado para el riesgo a los derechos y libertades de los titulares de datos personales,
- garantía que forma parte de las condiciones para la conformidad con el RGPD,
- como salvaguarda que disminuye la probabilidad de un impacto sobre los interesados en el marco de una brecha de datos personales.

Por lo tanto, como medida de protección, el cifrado no tendrá el mismo impacto en todos los tratamientos, y necesariamente estará complementado por otras garantías de privacidad y medidas de seguridad.

Además, en otro orden de ideas, los sistemas criptográficos son parte esencial de cualquier SGSI, es decir, no puede diseñarse un sistema para la protección de la información sin tener en cuenta la fortaleza de los sistemas criptográficos que harán que dicho SGSI se eficiente de manera adecuada a las necesidades que puedan plantearse.

REPERCUSIÓN PARA EL CIUDADANO Y LAS ADMINISTRACIONES

En la práctica la adecuada implementación exige a responsables y encargados de un tratamiento la necesidad de verificar, evaluar y valorar todos los elementos que intervienen en el proceso de cifrado, más allá de limitarse a la selección de un algoritmo o una implementación concreta de éste.

Por un lado, hay que determinar los requisitos que ha de cumplir el sistema de cifrado en el contexto del tratamiento, y por el otro ha de realizarse una validación de que dichos requisitos se satisfacen, así como supervisar que se mantienen en el tiempo. En todo caso hay que tener en cuenta que la protección de datos personales implica considerar el tiempo de vida de dichos datos, que puede ser tan extenso como la vida del titular de los datos y ello en el contexto de los cambios tecnológicos que ocurren en largos lapsos de tiempo. Es importante resaltar que el cifrado no comporta anonimización, aunque podría utilizarse como herramienta de seudonimización.

En todo caso, el nivel de detalle en el diseño, la validación y la supervisión de cualquier sistema criptográfico ha de adecuarse a la importancia y relevancia que tiene el cifrado en el tratamiento de los datos, así como el impacto que tiene dicho tratamiento para los

derechos y libertades de los interesados o, en su caso, a la confidencialidad de la información que se pretende proteger.

En definitiva, los sistemas de cifrado, cuando son seleccionados adecuadamente, permiten una garantía de confidencialidad eficiente para evitar fugas de información cuando el resto de las medidas de seguridad quiebran y, en particular, cuando se produce una brecha de datos personales.

Su repercusión en las administraciones y en el sector privado puede suponer la adecuada selección de medidas de confidencialidad no exclusivamente para garantizar los derechos y libertades de las personas físicas sino también para garantizar la eficacia de lo que podríamos denominar medida de seguridad de segundo nivel diseñada para evitar la pérdida de control de la información cuando se produce una fuga de información tras la quiebra de otras medidas de seguridad que podríamos denominar de primer nivel.

EQUIPO DE DESARROLLO Y PROVEEDORES

La elaboración del documento que ahora se presenta a la candidatura de este premio SOCINFO ha sido liderada desde la AEPD con la supervisión de la División de Innovación y Tecnología y la colaboración con la Asociación Profesional Española de Privacidad (APEP) y la Asociación Española para el Fomento de la Seguridad de la Información (ISMS Forum) y las revisiones realizadas por Carlos Bachmaier, DPD de Sociedad Estatal, María Isabel González Vasco, Catedrática del Departamento de Matemática Aplicada, Ciencia e Ingeniería de los Materiales y Tecnología Electrónica (MACIMTE) de la Universidad Rey Juan Carlos e Isabel Barberá, Ingeniera de Privacidad de Rhite.

VALORACIÓN ECONÓMICA

Este nuevo recurso de ayuda no ha supuesto ningún gasto presupuestario para ninguna de las entidades que han participado, todos los participantes han puesto a disposición de la sociedad en general sus conocimientos, su experiencia profesional y esfuerzo.

La obtención de este galardón sería un reconocimiento al esfuerzo y altruismo de todas aquellas personas que han intervenido en su elaboración y un aliciente para hacer que estos criterios de evaluación puedan servir como un estándar a la hora de poner en marcha un sistema criptográfico.

De nuevo, puede decirse que este proyecto es un ejemplo más de los objetivos que pueden ser alcanzables desde la colaboración público-privada y personal

PLAZOS DE CUMPLIMIENTO

Gracias al compromiso de las organizaciones y las personas implicadas en el proyecto de desarrollo del recurso de ayuda que ahora se presenta a la candidatura de este premio SOCINFO ha sido posible poner en el mercado un recurso de ayuda en un tiempo récord inferior a los seis meses de esfuerzo de coordinación desde que el proyecto fue comunicado a sus participantes.

CONCLUSIÓN

El propósito de esta candidatura es poner en relieve la actitud desinteresada del equipo de profesionales de la privacidad que han formado parte de este proyecto, en especial, la ilusión con la que asumieron las tareas que ello implicaba cuando desde la AEPD se les propuso la idea de colaborar con la elaboración de un recurso de ayuda que garantizara los derechos y libertades de los ciudadanos.

En definitiva, la consecución de este galardón supondría poner en relieve la colaboración público-privada y su beneficio para nuestra sociedad. Es preciso señalar que hasta la fecha se trata de un documento novedoso sobre el que ninguna otra autoridad de control ha dictado, hasta la fecha, recomendaciones.