Requisitos de Seguridad Adicionales para Soluciones en la Nube (SaaS) implementadas en Modo Local

Abstract: *se hace necesario establecer unos requisitos de seguridad adicionales en los sistemas de información, que originalmente hubieran sido desplegados como soluciones en la nube, instalados en modo local por entidades proveedoras y así garantizar la seguridad de los sistemas implicados y velar por el cumplimiento de los requisitos establecidos en el Esquema Nacional de Seguridad (ENS) dadas las especiales características de seguridad que deben contemplarse.*

Contenido:

1. OBJETO 1
2. CRITERIOS GENERALES 1
2.1 REQUISITOS DE SEGURIDAD ENS DEL PROVEEDOR 2
2.2 REQUISITOS DE SEGURIDAD ENS DE LA ENTIDAD CONTRATANTE 2
2.3 REQUISITOS DE SEGURIDAD ADICIONALES 2
2.4 AUDITORÍAS DE CUMPLIMIENTO DEL ENS 4

1. OBJETO

El objeto del presente documento es establecer unos criterios generales para la certificación de aquellos sistemas de información instalados en modo local que originalmente hubieran sido desplegados como soluciones en la nube en su modalidad Software as a Service (SaaS).

2. CRITERIOS GENERALES

Los condicionantes de este tipo de sistemas, desarrollados por proveedores para prestar un servicio en la nube pero instalados en una entidad contratante (cliente) o en un tercero[1], pueden hacer que dentro del marco de cumplimiento del Esquema Nacional de Seguridad no se garantice plenamente la correcta implementación de las medidas de seguridad exigidas en el sistema en el que se ha alojado (de la entidad contratante o del tercero).

La casuística concreta de estos sistemas hace que no se puedan considerar certificaciones de conformidad del ENS al uso, ni tampoco que les sea de aplicación el Catálogo de Productos STIC (CPSTIC), ya que no son productos cuyas funciones principales estén asociadas a la seguridad.

Por esta razón, es necesario establecer unos requisitos adicionales para garantizar la seguridad en la implementación, en modo local, para este tipo de sistemas persiguiendo la adecuada conformidad con el ENS de los sistemas de información de las entidades donde se instalan.

[1] Relacionado con el cliente pero que no tiene que ver con el proveedor que ha proporcionado el servicio.

2.1 REQUISITOS DE SEGURIDAD ENS DEL PROVEEDOR

Las entidades del sector público que requieran la contratación en modo local de un proveedor de servicios, que afecte a los propios sistemas de información de la entidad contratante, deberán exigir al proveedor la adecuación al ENS del sistema instalado en modo local y su consiguiente Declaración o Certificación de Conformidad en la categoría de seguridad que la entidad contratante haya determinado para la correcta operación de los sistemas concernidos.

En aquellos casos que no existiese proveedor alguno cuyos sistemas que prestan el servicio dispongan de la Declaración o Certificación de Conformidad, se dará un plazo de dos (2) meses para iniciar el Procedimiento de Adecuación con el ENS y se definirán las medidas técnicas que es obligatorio que cumplan los sistemas implicados para poder comenzar a prestar el servicio.

Tanto los requisitos relativos a la adecuación del ENS del sistema del proveedor como las medidas que es necesario cumplir, en el caso de no disponer de una Declaración o Certificación de Conformidad, deberán aparecer reflejadas en el Pliego de Prescripciones Técnicas publicado por la entidad contratante.

2.2 REQUISITOS DE SEGURIDAD ENS DE LA ENTIDAD CONTRATANTE

El sistema a instalar en modo local, que presumiblemente interactuará con un sistema previamente configurado de manera segura y conforme con el ENS, deberá formar parte del Análisis de Riesgos del sistema global y tener en cuenta el resto de acciones contempladas en los Procedimientos de Gestión y Autorización de Cambios de la entidad contratante.

En el caso de que la entidad contratante no haya determinado la Declaración o Certificación de Conformidad con el ENS para sus sistemas, deberá realizar un Análisis de Riesgos contemplando todos los aspectos de los sistemas con los que interactuará el sistema instalado en modo local y valorar las salvaguardas a aplicar para minimizar el riesgo, siendo este riesgo aceptado por la autoridad responsable de la entidad contratante.

Si la entidad contratante quiere que el citado Análisis de Riesgos lo realice el proveedor, deberá reflejarlo en el Pliego de Prescripciones Técnicas publicado por la misma.

2.3 REQUISITOS DE SEGURIDAD ADICIONALES

Una vez garantizada la seguridad en los sistemas implicados (sistema propio de la entidad contratante y sistema contratado en modo local) se deberán establecer ciertos requisitos de seguridad adicionales que cubran las necesidades propias de los sistemas en modo local y satisfagan los controles requeridos en el ENS.

Este tipo de necesidades adicionales de seguridad se dan principalmente en dos (2) niveles:

- en la configuración y administración del sistema,
- y en el uso del sistema por parte de los usuarios finales.

En ambos casos, la falta de conocimiento sobre las configuraciones y acciones a ejecutar sobre el sistema instalado puede desembocar en deficiencias graves de seguridad y vulnerabilidades explotables por potenciales amenazas.

De cara a suplir posibles carencias y falta de conocimiento, la empresa proveedora del sistema deberá proporcionar a la entidad contratante los documentos de seguridad necesarios para evitar un mal uso y deficiente configuración del sistema.

En este sentido, es importante determinar las responsabilidades que son propias del usuario al utilizar el servicio/aplicación y las que son del proveedor. Todo ello permitirá concretar y determinar cómo deben operarse este tipo de sistemas instalados en modo local salvaguardando los requisitos de seguridad y no poniendo en riesgo la adecuación al ENS.

Por tanto y para minimizar el riesgo, se elaborarán los documentos de seguridad que se determinen y que comprenderán como mínimo:

- **La Guía de Instalación y Configuración Segura del Sistema destinada a administradores**, donde se explicarán todas las acciones que deben realizar los administradores a la hora de instalar la aplicación, establecer una configuración inicial, actualizar el sistema y realizar pruebas de integridad del mismo, así como los requisitos de seguridad, los controles del ENS que se implementen y cualquier otro aspecto que se estime relevante para la seguridad del sistema.

  Una guía CCN-STIC especificará y concretará todos los aspectos que deben incluirse en la Guía de Instalación y Configuración destinada a los administradores.

- **La Guía de Uso Seguro del Sistema destinada a usuarios finales**, donde se detallará la Normativa de Uso del sistema, el Manual de Usuario (resaltando las implicaciones de seguridad en las acciones que puedan realizar los usuarios) y todas aquellas configuraciones, procedimientos de seguridad que deban ser realizados por los usuarios finales para el uso seguro del sistema y los requisitos de seguridad y controles del ENS implementados, todo ello alineado con los requisitos del ENS exigidos.

  Una guía CCN-STIC facilitará la elaboración de la Guía de Uso Seguro destinada a los usuarios finales.

Igualmente, será responsabilidad de la entidad contratante adoptar estos documentos como propios del organismo, formando parte de las medidas de seguridad de la propia entidad (configuraciones de seguridad, normativas de seguridad y procedimientos de seguridad) en el grado y circunstancias que se estimen apropiadas.

Estos requisitos de seguridad adicionales y su documentación asociada, junto con la necesidad de obtener la conformidad con el ENS, deben ser igualmente exigidos en los Pliegos de Prescripciones Técnicas publicados por la entidad contratante.

Además, el proveedor deberá facilitar un documento que analice en todo su conjunto las obligaciones directas de cumplimiento del ENS. Es decir, una guía que persiga aclarar la relación entre un proveedor de software y un cliente contratante, en modo compatible con el ENS:

- **Una Guía de Recomendaciones para la gestión de la relación entre proveedor y cliente contratante**, donde se identificará la relación entre el cliente contratante y un proveedor de software, y establecerá la carga de responsabilidad de cada parte respecto a los controles de seguridad del ENS que aplican y al Análisis de Riesgos descrito en el Apartado 2.2.

  Una guía CCN-STIC facilitará la elaboración de la Guía de Recomendaciones para la gestión de la relación entre el proveedor y el cliente contratante.

2.4 AUDITORÍAS DE CUMPLIMIENTO DEL ENS

Durante el proceso de auditoría, será responsabilidad de la Entidad de Certificación inspeccionar la correcta implementación de los requisitos descritos en el presente documento.

En consecuencia, se deberá verificar que se cumplen tanto las exigencias de seguridad del proveedor, como las condiciones previamente mencionadas que fueran responsabilidad de la entidad contratante. Para facilitar esta tarea, se dispondrá de una guía CCN-STIC que sirva de base para la verificación de los requisitos de seguridad exigidos en este Abstract.

Al final de la auditoría y tras haber obtenido el sistema de la entidad contratante la Certificación de Conformidad con el ENS, la Entidad de Certificación será responsable de remitir al CCN, junto con dicha Certificación de Conformidad, la Guía de Instalación y Configuración Segura del Sistema destinada a administradores, la Guía de Uso Seguro del Sistema destinada a usuarios finales, la Guía de Recomendaciones para la gestión de la relación entre proveedor y cliente contratante, y cualquier otro documento que pudiera haber sido contemplado como requisito de seguridad adicional para sistemas de información instalados en modo local que originalmente hubieran sido desplegados como soluciones en la nube en su modalidad Software as a Service (SaaS).

CCN centro criptológico nacional
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.01.05 12:25:52 +01'00'