Obligaciones de los prestadores de servicios a las entidades públicas

Abstract: el presente documento recoge las obligaciones de los prestadores de servicios a las entidades públicas, cuando tales servicios estén sujetos al cumplimiento del Esquema Nacional de Seguridad.

Contenido:

1. OBJETO

El objeto del presente documento es establecer las obligaciones a tener en cuenta por las organizaciones (públicas o privadas) que prestan servicios a las entidades del sector público, cuando estén sujetos al cumplimiento del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS).

Estas obligaciones, que incluyen necesariamente la conformidad con el ENS, van más allá. Puesto que la entidad del sector público a la que se proveen los servicios es la responsable última de los riesgos que afecten a la información tratada y los servicios prestados, debe exigir al proveedor la información y la ejecución de las acciones necesarias para que la entidad pueda cumplir sus objetivos.

2. MARCO NORMATIVO

Hay que comenzar señalando que el artículo 15.3 del ENS, “profesionalidad”, establece que las Administraciones públicas exigirán, de manera objetiva y no discriminatoria, que

las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

Por su parte, el control [op.ext], "Servicios externos", establece que cuando se utilicen recursos externos a la organización, sean servicios, equipos, instalaciones o personal, deberá tenerse en cuenta que la delegación se limita a las funciones, añadiendo que la entidad que delega las funciones dispondrá las medidas necesarias para poder ejercer su responsabilidad y mantener el control en todo momento.

Además, las organizaciones, públicas o privadas, cuando provean servicios o soluciones a las entidades públicas, que estén sujetos al cumplimiento del ENS, deberán estar en condiciones de exhibir, respecto a estos, la correspondiente Declaración de Conformidad con el ENS, cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el ENS, cuando se trate de sistemas de categorías MEDIA o ALTA, de acuerdo a lo establecido en la "*Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad"*, aprobada, el 13 de octubre de 2016, por Resolución de la Secretaría de Estado de Administraciones Públicas, y siempre que la categoría del sistema de información de que se trate haya sido determinada por la entidad pública contratante.

Para soluciones *on-premise*, independientemente de que originariamente hubieran sido desplegadas como soluciones en la nube o no, será de aplicación también lo indicado en la "*Guía CCN-STIC 858 Implantación de sistemas SaaS en modo local (on-premise)"* y el "*Abstract- Requisitos de Seguridad Adicionales para Servicios en la Nube prestados desde instalaciones en modo local*", en particular, en lo relativo a los requisitos de seguridad adicionales (*Guía de Instalación y Configuración Segura del Sistema* destinada a administradores y la *Guía de Uso Seguro del Sistema destinada a usuarios finales*).

Por otro lado, es responsabilidad de las entidades públicas contratantes notificar a los prestadores de servicios -muy especialmente, a los operadores del sector privado que participen en la provisión de soluciones tecnológicas o en la prestación de servicios-, la obligación de que tales soluciones o servicios sean conformes con lo dispuesto en el ENS, en la categoría y con el nivel de seguridad correspondiente a cada dimensión, que determine la entidad pública contratante, y posean las correspondientes Declaraciones o Certificaciones de Conformidad, según lo señalado en la mencionada Instrucción Técnica de Seguridad.

3. CRITERIOS GENERALES

Al inicio y durante la prestación del servicio, el prestador, en función de la modalidad prestacional que se haya contratado, deberá proveer al cliente de toda la información necesaria que permita evidenciar una adecuada diligencia en la relación con la entidad pública destinataria de los servicios.

Este requisito se considera indispensable para una correcta gestión del servicio o servicios objeto de contratación y la seguridad del sistema de información concernido en el servicio.

3.1 DESCRIPCIÓN DE SERVICIOS Y MODALIDAD

Los prestadores de servicios aportarán a la entidad del sector público contratante una descripción precisa de los servicios y su modalidad, indicando: el alcance de la prestación del servicio, si cubre funciones operativas del servicio o de control (aportando información clara sobre el objeto del servicio), expectativas y limitaciones del mismo.

Por ejemplo, si se prestan servicios en Cloud, será necesario indicar la modalidad de los servicios prestados: IaaS (*Infrastructure as a Service*), SaaS (*Software as a Service*) o PaaS (*Platform as a Service*). Si se prestan servicios de desarrollo de aplicaciones, asimismo, se deberá indicar si las soluciones se desplegarán en modo local *on-premise* o externalizado, etc.

3.2 INFORMACIÓN SOBRE LA ARQUITECTURA DE SEGURIDAD

Será requisito obligatorio que el prestador de servicios, cuando sea relevante para el servicio prestado, especialmente a efectos de definición de requisitos de interconexión, aporte la información necesaria sobre el sistema que soporta los servicios, respecto a la arquitectura de seguridad, con el objeto de facilitar a la entidad pública contratante el cumplimiento de sus obligaciones, tales como la realización del Análisis de Riesgos o el subsiguiente Plan de Tratamiento de Riesgos.

Asimismo, aportará los diagramas de red, esquemas de elementos físicos, esquemas de interconexión y esquemas lógicos de sistemas que muestren a la entidad cliente la infraestructura física y lógica de la que forma parte el servicio objeto de contratación. De esta forma, la entidad contratante podrá delimitar las dependencias entre sus activos esenciales y los activos subcontratados, y analizar las potenciales amenazas que se podrían materializar sobre los sistemas de información.

Todo ello será exigible siempre que los antedichos requisitos no estén adecuadamente cubiertos por la Declaración o Certificación de Conformidad con el ENS que pudiera poseer el proveedor, con relación a los sistemas de información utilizados para la prestación de los servicios contratados.

3.3 UBICACIÓN DE LA INFORMACIÓN

Con el fin de que la entidad destinataria de los servicios conozca con precisión la ubicación de los sistemas de información concernidos en la prestación y su información, el prestador de servicios aportará la documentación que detalle si los tratamientos de información van a ejecutarse en sistemas e instalaciones propias o de la entidad pública contratante.

Asimismo, en caso de que los tratamientos se realicen en sistemas del prestador del servicio, se indicarán las medidas de seguridad física asociadas. Este aspecto es importante ya que permite a la entidad contratante evaluar el cumplimiento de la normativa de protección de datos, en lo relativo a transferencias internacionales de datos y de la legislación en materia de administración digital, contratación del sector público y telecomunicaciones.

Las exigencias anteriores podrán ser evidenciadas a través de las correspondientes Declaraciones o Certificaciones de Conformidad con el ENS de las que el proveedor fuera titular.

3.4 MEDIDAS DE SEGURIDAD IMPLEMENTADAS

La entidad pública destinataria de los servicios podrá requerir del prestador, además de la correspondiente Declaración o Certificación de Conformidad con el ENS, el detalle de la Declaración de Aplicabilidad y, en su caso, de las medidas compensatorias y complementarias de vigilancia utilizadas si así se determinan.
De esta forma, la entidad destinataria de los servicios podrá dar conformidad a sus propios requisitos del ENS y conocer si existen medidas de seguridad adicionales o complementarias a las exigidas por la categoría de su/s sistema/s.

3.5 CUMPLIMIENTO DE LA NORMATIVA VIGENTE DE PROTECCIÓN DE DATOS

En aquellos casos en los que los servicios prestados impliquen el tratamiento de datos personales, será necesario la implementación de funcionalidades que garanticen el cumplimiento de la normativa vigente por parte de la entidad pública cliente. Por ejemplo, medidas destinadas a cumplir con los principios básicos del tratamiento y que permitan garantizar los derechos de los interesados (acceso, rectificación, supresión, bloqueo de datos, etc.).

Además de lo anterior, cuando resulte procedente, el proveedor de servicios estará obligado a cumplir las obligaciones que establece la normativa de protección de datos para los Encargados de Tratamiento.

3.6 INCIDENTES DE SEGURIDAD

Las entidades públicas tienen la obligación de notificar al CCN-CERT los incidentes de seguridad que puedan tener un impacto significativo, tal y como prescribe el art. 36 del ENS y desarrolla la Resolución de, 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

Por otro lado, la Resolución de, 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, prescribe que el ENS resulta también de aplicación a las entidades privadas cuando presten servicios o provean soluciones a las entidades públicas a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad.

La aplicabilidad del ENS a tales empresas privadas supone también la obligación de notificar a la entidad pública contratante a la que presten servicio los incidentes de seguridad, que puedan afectar la seguridad de los sistemas objeto del servicio.

El sector público, deberá notificar sus incidentes a través de la Plataforma LUCÍA, por lo que hay que exigir que aquellas entidades de dicho sector que no tengan instalada una instancia o estén federadas, lo hagan sin dilación indebida. Si todavía no disponen de la solución LUCÍA, deberán trasladar al CCN-CERT el procedimiento de notificación de incidentes.

De la misma forma, el proveedor del sector privado podrá notificar el incidente al CCN-CERT a través de la Plataforma LUCÍA del organismo al que presta servicio y, en el caso de que dicho organismo no disponga de la misma, podrá emplear otro mecanismo de notificación, como el correo electrónico a la dirección incidentes@ccn-cert.cni.es, prestándose el Servicio de Respuesta a Incidentes desde el CCN-CERT.

Por tanto, para facilitar el intercambio de información podrá resultar conveniente que los prestadores privados de servicios tecnológicos al sector público estén federados en LUCÍA, con lo que podrán beneficiarse del Servicio de Respuesta a Incidentes del CCN-CERT.

La resolución de un incidente de seguridad que haya tenido como víctima a una entidad pública, especialmente cuando tal incidente sea de peligrosidad alta o superior, exigirá la participación de la entidad proveedora de los servicios afectados por el incidente de seguridad, al objeto de calibrar el impacto del ataque y la adopción de las medidas necesarias de contención, mitigación, respuesta y recuperación.

Estas actividades, por su especialización, podrán requerir el concurso de su CSIRT de referencia, especialmente cuando el incidente hubiere afectado a sistemas que traten información de naturaleza administrativa o datos de los ciudadanos administrados. Dicha respuesta deberá gozar por tanto de las preceptivas medidas de seguridad y confidencialidad de la actuación administrativa que exige el art. 3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y que obliga a que tal conocimiento solo pueda extenderse a un organismo de las administraciones públicas, como el Centro Criptológico Nacional.

Esta realidad podrá ser expresada en los correspondientes Pliegos de Prescripciones Técnicas cuando una entidad pública pretenda la contratación de servicios externos con entidades privadas.

El Centro Criptológico Nacional recuerda que es obligación de las Entidades de Certificación acreditadas comprobar que los organismos públicos auditados disponen de LUCIA, instándoles a su implantación, debiendo figurar este comentario en el informe de auditoría si ese no fuera el caso. En este sentido, deberán ponerse en contacto con las cuentas info@ccn-cert.cni.es o lucia@ccn-cert.cni.es para poder disponer de LUCIA.

3.7 PORTABILIDAD DE LA INFORMACIÓN

Será necesario implementar mecanismos que garanticen la portabilidad de la información con el objetivo de facilitar a la entidad cliente el proceso de gestión del cambio ante el cese o baja de los servicios suministrados por parte del prestador de servicio.

Igualmente, el prestador de servicios deberá certificar que, al causar baja el servicio suministrado, los datos almacenados han sido eliminados de manera segura una vez finalizado el proceso de portabilidad.

3.8 CADENA DE SUBCONTRATACIÓN Y SUS CAMBIOS

La entidad proveedora del servicio deberá disponer de una documentación que detalle claramente los elementos que forman parte de la cadena de subcontratación, así como las implicaciones derivadas de cualquier cambio o modificación que pueda sufrir algún eslabón de dicha cadena.

El proveedor deberá asegurar que los sistemas de información de las empresas subcontratadas son conformes con el ENS en lo que respecta a los servicios que afecten a la entidad pública contratante, por lo que el contenido del presente documento resultará asimismo de aplicación a la cadena de suministro del proveedor.

En este sentido, la entidad pública destinataria de los servicios podrá requerir del prestador, además de la correspondiente Declaración o Certificación de Conformidad con el ENS, el detalle de la Declaración de Aplicabilidad y, en su caso, de las medidas compensatorias y complementarias de vigilancia utilizadas.

3.9 CAPACIDAD Y DIMENSIONAMIENTO DEL SISTEMA

Se deberá disponer de un sistema de gestión de la capacidad con mejora continua, que proporcione, de forma periódica, información relacionada con el sistema que soporta los servicios, como por ejemplo capacidad, dimensionamiento y rendimiento del sistema.

Análogamente, la entidad pública destinataria de los servicios podrá requerir del prestador, además de la correspondiente Declaración o Certificación de Conformidad con el ENS, el detalle de la Declaración de Aplicabilidad y, en su caso, de las medidas compensatorias y complementarias de vigilancia utilizadas.

3.10 SEGUIMIENTO DE LOS ACUERDOS DE NIEVEL DE SERVICIO

El proveedor del servicio (de conformidad con lo exigido por la medida [op.ext.2]), facilitará herramientas de monitorización o informes periódicos de modo que la entidad pública cliente pueda realizar un seguimiento y gestión del cumplimiento de los Acuerdos de Nivel de Servicio (SLA) contratados.

El prestador de servicio será proactivo en este ámbito, aportando estos datos con total transparencia y gestionando los incumplimientos diligentemente.

4. RECOMENDACIONES ADICIONALES

4.1 CONTINUIDAD

Con el fin de que la entidad pública contratante pueda garantizar la continuidad de los servicios prestados por el prestador, será necesario que este le facilite la información necesaria para establecer el plan de continuidad tal y como se exige en el ENS.

4.2 ANÁLISIS Y EXPLOTACIÓN DE REGISTROS

Para que los registros (*logs*) generados por los servicios contratados y que el proveedor deberá poner a disposición del cliente, de conformidad con la medida [op.exp.8], tanto en su utilización como en su gestión, puedan ser debidamente analizados y explotados, se recomienda establecer funcionalidades que permitan definir alertas y reglas, de forma que se facilite el análisis de la información registrada.

Estas funcionalidades permitirán a la entidad pública contratante detectar situaciones de alerta ante una posible utilización indebida de los servicios, de forma que sea posible depurar y analizar incidencias o acciones realizadas.

4.3 CONTROLES PERIÓDICOS

Con el fin de facilitar la realización de los controles periódicos exigidos para el cumplimiento de las exigencias establecidas en el ENS, el proveedor de servicios debe proporcionar los mecanismos y funcionalidades que permitan a la entidad pública conocer y analizar los controles llevados a cabo por parte del proveedor de servicios.

Algunos de esos controles serán, por ejemplo: auditorías de seguridad, informes de *hacking* ético, renovación de certificaciones de seguridad, etc.