CLAUSULAS DE SEGURIDAD PARA PLIEGOS: DESARROLLO DE SOFTWARE Y/O IMPLANTACIÓN DE APLICACIONES, INFRAESTRUCTURAS O SISTEMAS DE INFORMACIÓN, Y/O SERVICIOS DE SOPORTE

Fecha de actualización: Febrero de 2024

CLÁUSULAS DE SEGURIDAD GENERALES A INCLUIR EN ANEXOS DEL PCAP CUANDO APLIQUEN ENS (apartado 22) Y TRATAMIENTO DE DATOS PERSONALES (apartado 23).

NOTA: Los párrafos en rojo deben ser revisados por el responsable de preparar el expediente en la Universidad de Sevilla.

22.- CUMPLIMIENTO DEL ESQUEMA NACIONAL DE SEGURIDAD

1. Obligaciones del prestador del servicio y su personal

1.1. El prestador del servicio se compromete a cumplir con la Política de Seguridad de la Información de la Universidad de Sevilla y la Normativa General de Utilización de los Recursos y Sistemas de Información, y aceptará todas las normativas y procedimientos de seguridad aplicables en el contexto del servicio prestado publicadas en la web de la Oficina de Seguridad de la Información.

1.2. El personal de terceros prestando servicios para la Universidad de Sevilla será informado sobre buenas prácticas, uso responsable de los sistemas de intercambio de información y mecanismos existentes en la Universidad de Sevilla para la apertura de incidentes de seguridad relacionadas con dichos servicios.

1.3. El prestador del servicio hará extensibles todas las condiciones y obligaciones aquí contempladas a todo el personal que intervenga en la prestación del servicio.

2. Confidencialidad

2.1. La información facilitada para la prestación del servicio no se utilizará con una finalidad diferente a la que es objeto del servicio.

2.2. El prestador del servicio no la comunicará, ni siquiera a efectos de su conservación, a terceros.

2.3. El prestador del servicio y el personal a su cargo están obligados a guardar secreto y absoluta confidencialidad respecto de la información que les ha sido confiada en virtud del servicio. Las obligaciones de confidencialidad y deber de secreto subsisten durante 20 años, incluso tras la finalización del contrato con la Universidad de Sevilla.

2.4. El prestador del servicio deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de la información y eviten su alteración, pérdida, sustracción, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.

2.5. Se prohíbe el empleo de soportes de información extraíbles (CD's, DVD's, memorias USB, etc.), por parte del personal de terceros prestando servicios en la Universidad de Sevilla para el almacenamiento de información del organismo sin autorización previa.

2.6. Tras la finalización del proyecto la información será destruida en su totalidad o devuelta a la Universidad de Sevilla, teniendo en cuenta los distintos soportes o documentos donde estos puedan constar: bases de datos en discos, ficheros temporales, copias de seguridad, soportes en papel, etc.

2.7. Una vez se haya realizado la operación mencionada en el punto anterior, el prestador del servicio se compromete a entregar una declaración por escrito a la Universidad de Sevilla donde conste que así se ha hecho.

3. Gestión de incidentes de seguridad

3.1. El prestador del servicio deberá reportar, de manera completa y con la máxima celeridad posible, cualquier incidente de seguridad que tenga relación con el servicio prestado y que afecte o pueda afectar a la Universidad de Sevilla.

3.2. El prestador del servicio deberá colaborar activamente en el análisis, tratamiento y resolución de cualquier incidente de seguridad que pueda afectar al servicio prestado.

3.3. El prestador del servicio deberá proporcionar un plan de contingencias para el servicio, que garantice que, aún en caso de que ocurra un incidente grave que afecte al servicio, éste se podrá seguir prestando dentro de unos niveles aceptables.

3.4. Toda la información referente a la Política y Normativas de Seguridad pueden ser consultadas en: http://osi.us.es

4. Aplicación del Esquema Nacional de Seguridad

4.1. Cuando el servicio prestado esté dentro del alcance del Real Decreto 311/2022, de 3 de mayo, que regula el Esquema Nacional de Seguridad, serán de aplicación las medidas contempladas por él y sus futuras actualizaciones.

4.2. La Universidad de Sevilla podrá solicitar al prestador del servicio la correspondiente Certificación de Conformidad con el ENS (obligatoria, en sistemas de categorías MEDIA, y de aplicación voluntaria en categoría BÁSICA), utilizando los mismos procedimientos que los exigidos para las entidades públicas.

4.3. En su defecto, si la empresa no está certificada, se solicitará la aplicación de las medidas de seguridad establecidas en el Anexo II del ENS, a una o varias dimensiones de seguridad y según el nivel determinado en cada caso. Dichos niveles de seguridad vienen determinados conforme a lo establecido en el Anexo I del ENS por el órgano competente sobre la valoración e importancia de la información que se maneja y los servicios prestados. La Universidad de Sevilla se reserva el derecho de llevar a cabo una auditoría periódica en la que se verifique el cumplimiento las medidas de seguridad establecidas en el Anexo II del ENS. (La US tiene un sistema de información de Categoría MEDIA pero algunos servicios podrían tener sus dimensiones de seguridad CITAD valoradas de nivel BAJO – consultar con el Área de Gestión de la Seguridad).

4.4. Respecto a la instalación y configuración de los sistemas y aplicativos (NOTA: si los hubiera como parte de la prestación del servicio), el adjudicatario asumirá las reglas de "Mínimos privilegios" y "Seguridad por defecto" que establece el ENS. En concreto, en los casos en los que existan guías CCN-STIC serie 800 de aplicación, se podrán utilizar dichas guías para la instalación y configuración.

4.5. Para la prestación de servicios externos, en particular, de acuerdo a la medida de seguridad op.ext.1 del apartado 4.4.1 "Contratación y acuerdos de nivel de servicio" del ENS, podrá ser necesario, en función del nivel de seguridad requerido, el establecimiento de contratos con indicación de las características del servicio prestado y las responsabilidades de las partes. En estos Acuerdos de Nivel de Servicios (SLA) se detallará lo que se considera calidad mínima del servicio prestado y las consecuencias de su incumplimiento.

4.6. En relación al artículo 16 "Profesionalidad", la Universidad de Sevilla podrá exigir, de manera objetiva y no discriminatoria que la empresa adjudicataria preste los servicios con profesionales cualificados y con unos niveles idóneos de gestión y madurez. La seguridad debe ser atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento. (Si se considera oportuno, en "Requisitos de solvencia Técnica" se podrá especificar el número de personas que deberá contar con cada una de las certificaciones de seguridad necesarias, tipo CISA, CISM, CEH, CHFI, ISO 27001 Lead Auditor, etc. En otro caso, se podrán valorar las certificaciones mediante "Criterios de adjudicación mediante juicio de valor", dependiendo la puntuación asignada del tipo de contrato)

4.7. El adjudicatario deberá considerar en todo momento la necesidad de facilitar datos para el informe del estado de la seguridad (Artículo 32 del ENS). Se tendrá en cuenta la guía CCN-STIC-824, Informe nacional del estado de seguridad para facilitar los datos requeridos por la Universidad de Sevilla.

CLÁUSULAS DE SEGURIDAD ESPECÍFICAS PARA DESARROLLO DE SOFTWARE

Además de las cláusulas generales a continuación se recoge el catálogo de cláusulas específicas para desarrollo y/o implantación de aplicaciones en el que la seguridad sea un elemento significativo:

1. Durante el diseño y desarrollo de software el prestador del servicio deberá determinar formal y explícitamente al menos los siguientes aspectos de seguridad:
2. Mecanismos de identificación y autenticación utilizados, así como las capacidades de control de acceso, gestión de roles y permisos y trazabilidad, conforme a las medidas de seguridad del marco operacional del Anexo II del ENS aplicables (op.acc).
3. La utilización de soluciones criptográficas de protección de la información (cifrado, hash, firma electrónica y/o sellado de tiempo) así como el tratamiento de la documentación y sus metadatos, de conformidad con las medidas de protección de la información del Anexo II del ENS (mp.info), según aplique.
4. El prestador del servicio deberá garantizar que para las pruebas no se utilizan datos reales salvo que en dichas pruebas se garantice el cumplimiento de todas las medidas de seguridad exigibles tanto por el Esquema Nacional de Seguridad (mp.sw) como por el Reglamento General de

Protección de Datos para el nivel correspondiente de los datos personales tratados, siempre que sea de aplicación.

5. Durante la fase de pruebas el prestador del servicio llevará a cabo un análisis de vulnerabilidades y una prueba de penetración sobre el sistema de información desarrollado, de modo que todas las deficiencias identificadas sean corregidas antes de su puesta en producción, tal como exige el ENS en las medidas de protección de los servicios del Anexo II (mp.s).

CLÁUSULA DE SEGURIDAD ESPECÍFICA PARA ADQUISICIÓN DE PRODUCTOS DE SEGURIDAD

Respecto al suministro de productos de seguridad, en particular, el adjudicatario asumirá el cumplimiento del Artículo 19 del ENS, Adquisición de productos de seguridad y contratación de servicios de seguridad y lo indicado en la medida op.pl.5.1 sobre componentes certificados, recogida en el apartado 4.1.5 del Anexo II. Se utilizará el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) del CCN, para seleccionar los productos o servicios suministrados por un tercero que formen parte de la arquitectura de seguridad del sistema y aquellos que se referencien expresamente en las medidas de este real decreto. En caso de que no existan productos o servicios en el CPSTIC que implementen las funcionalidades requeridas, se utilizarán productos certificados de acuerdo a lo descrito en el artículo 19.

23.-TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

Si el contrato adjudicado implica el tratamiento de datos de carácter personal el contratista y subcontratistas, en su caso, se someterán en su integridad el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD), y la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de datos Personales y Garantía de Derechos Digitales (LOPDyGDD).

1. **Finalidad del tratamiento de datos personales.**

   Si el contrato adjudicado implica el tratamiento de datos de carácter personal, se ha de hacer constar en el pliego la finalidad del tratamiento de datos personales, que será la del objeto del contrato, y se incluirá también en el contrato de tratamiento de datos personales.

2. **Ubicación de Servidores**

   Si el contrato adjudicado implica el tratamiento de datos de carácter personal la empresa adjudicataria está obligada a presentar antes de la formalización del contrato una declaración en la que ponga de manifiesto dónde van a estar ubicados los servidores y desde dónde se van a prestar los servicios asociados a los mismos. La obligación de comunicar cualquier cambio que se produzca, a lo largo de la vida del contrato, de la información facilitada sobre ubicación de los servidores.

   Los licitadores tienen la obligación de indicar en su oferta, si tienen previsto subcontratar los servidores o los servicios asociados a los mismos, el nombre o el perfil empresarial, definido por

referencia a las condiciones de solvencia profesional o técnica, de los subcontratistas a los que se vaya a encomendar su realización.

3. Contrato de Responsable/Encargado

Si el contrato adjudicado implica el tratamiento de datos de carácter personal que realice el contratista por cuenta de la US, se deberá formalizar "Contrato de Tratamiento de datos Personales Responsable/Encargado", de conformidad con lo establecido en el art. 28 del RGPD.

Por tanto, cuando se adjudique el contrato definitivamente, el responsable del mismo deberá proceder a la tramitación con la empresa del Contrato de tratamiento de datos personales entre el responsable y el Encargado.

El procedimiento de tramitación del contrato responsable/encargado y el modelo se podrán encontrar en los siguientes enlaces:

- https://osi.us.es/sites/osi/files/doc/pd/procedimientos/procedimientocto.encargado.pdf
- https://osi.us.es/sites/osi/files/doc/pd/procedimientos/contratotratamientodedatos.docx