Anexo de medidas de ciberseguridad para terceros.

Índice

1. Requisitos de Ciberseguridad.

El PROVEEDOR deberá garantizar que los servicios, trabajos, equipos o materiales contratados por ENCE cumplen con los estándares de ciberseguridad definidos en este documento.

Es imprescindible que el PROVEEDOR cumpla con todas las medidas de seguridad indicadas en los capítulos que apliquen al servicio desarrollado. En caso de no poder cumplir con alguno de ellos, deberá proponer medidas compensatorias o alternativas que serán evaluadas por ENCE. La falta de cumplimiento o de alternativas aceptables podrá dar lugar a la suspensión o cancelación del servicio contratado.

Todas las notificaciones con Ence en materia de ciberseguridad deberán realizarse a través de los canales y procedimientos establecidos por ENCE.

2. Definiciones

- **Activo o infraestructura de sistemas:** Incluye todos los sistemas y servicios electrónicos de información y comunicación, junto con los datos que contienen. Estos abarcan sistemas alojados localmente o en la nube, gestionados por ENCE o terceros. Comprenden hardware, software y dispositivos electrónicos como ordenadores, móviles, medios de almacenamiento, cámaras, sistemas GPS, infraestructura de red, entre otros.
- **Contrato:** Se refiere al acuerdo principal de servicios, suministro de materiales u otro contrato entre ENCE y el PROVEEDOR al cual este anexo está vinculado y forma parte.
- **Dispositivo de Propiedad Personal:** Dispositivo, incluyendo portátiles y móviles, que es propiedad privada de los usuarios, no siendo gestionado ni por ENCE ni por el PROVEEDOR.
- **Dispositivos Electrónicos:** Equipos con capacidad de procesamiento que permiten almacenar, transportar o acceder a información, redes y sistemas de ENCE. Incluyen laptops, teléfonos móviles, tabletas, cámaras, y dispositivos inteligentes, entre otros.
- **Dispositivos Portátiles:** Aparatos capaces de procesar datos y que pueden almacenar o acceder a información de ENCE. Comprenden laptops, teléfonos móviles, tabletas, cámaras, y otros dispositivos de uso portátil.
- **Incidente de Ciberseguridad**: Evento que genera un impacto negativo en la seguridad de las redes y sistemas de información de ENCE.
- **Información Confidencial:** Datos cuya divulgación no autorizada puede ocasionar perjuicios económicos, de reputación, regulatorios o legales. Ejemplos incluyen información financiera, planes estratégicos y datos relacionados con infraestructura.

- **IT (Tecnología de la Información)**: conjunto de tecnologías, herramientas y sistemas utilizados para gestionar, procesar y almacenar información, incluyendo software, hardware, redes y servicios relacionados.
- **OWASP (Open Web Application Security Project):** Proyecto de código abierto enfocado en identificar y mitigar vulnerabilidades en el software.
- **OT (Tecnología Operacional)**: Conjunto de tecnologías, sistemas y herramientas utilizados para monitorizar, controlar y automatizar procesos físicos en entornos industriales, infraestructuras críticas y operaciones físicas
- **Responsable del Servicio:** Empleado de ENCE encargado de definir, gestionar y facilitar la ejecución del contrato. Actúa como punto de contacto para necesidades, cambios o incidencias relacionadas con el proyecto.
- **SaaS (Software como Servicio)**: Modelo de distribución de software donde aplicaciones y datos se alojan en servidores del proveedor y se accede a ellos a través de Internet. El proveedor gestiona la infraestructura, el mantenimiento y el soporte, mientras el cliente utiliza las funciones del software según lo contratado.
- **Software:** Cualquier tipo de programación empleada por el PROVEEDOR, incluyendo sitios web, bases de datos, entornos en la nube, sistemas operativos, APIs, y más, como parte de la prestación de servicios
- **Terceros**: cualquier persona física o jurídica que, no siendo empleado ni miembro de los órganos de administración de ENCE, gestione activos de información de ENCE tanto en su propia infraestructura, como en la infraestructura de ENCE, o tenga acceso a esta última y, en particular, aquellos que cumplan alguna de las siguientes condiciones:
    - proporcionan servicios en la nube en cualquiera de sus modalidades
    - tienen acceso a información sensible, crítica o confidencial de clientes o empleados, de negocio, estratégica o financiera o información relativa a la infraestructura o mecanismos de defensa de ENCE
    - están involucrados en los procesos de desarrollo, integración, mantenimiento y/o funcionamiento de los sistemas y componentes de ENCE
    - tienen acceso físico a las instalaciones de ENCE.
- **Usuario:** Persona bajo la responsabilidad del PROVEEDOR que accede a los sistemas o información de ENCE, sin importar su relación laboral o la organización a la que pertenezca.
- **Violación de Seguridad de los Datos:** Incidente que compromete la seguridad, confidencialidad o integridad de la información protegida. Esto incluye pérdida, mal uso, acceso no autorizado o alteración indebida de los datos.

3. Medidas de seguridad generales

El servicio objeto del presente contrato deberá cumplir con las siguientes medidas generales de seguridad en materia de ciberseguridad, las cuales son de carácter obligatorio:

- **Capacitación y Concienciación en Ciberseguridad.**

  El PROVEEDOR deberá garantizar que su equipo de trabajo se encuentra debidamente capacitado y concienciado en materia de ciberseguridad. Esta capacitación incluirá el conocimiento de las mejores prácticas, normativas vigentes y procedimientos de seguridad necesarios para proteger la información gestionada en el marco del servicio.

- **Notificación de Incidentes de Ciberseguridad.**

  El PROVEEDOR estará obligado a notificar de manera inmediata a ENCE sobre cualquier incidente de ciberseguridad, como pérdidas de información o brechas que puedan comprometer el servicio o los datos gestionados.

- **Derecho de Auditoría.**

  ENCE se reserva el derecho de llevar a cabo auditorías en cualquier momento para evaluar las medidas de seguridad implementadas por el PROVEEDOR. Estas auditorías podrán ser realizadas directamente por ENCE o a través de terceros designados, y el PROVEEDOR deberá facilitar el acceso y la colaboración necesaria para su ejecución.

- **Notificación al Finalizar la Actividad.**

  El PROVEEDOR se compromete a informar a ENCE al término de las actividades relacionadas con el servicio, detallando cualquier aspecto relevante o pendiente en el marco de la relación contractual.

4. Medidas de seguridad en caso de acceso a sistemas de ENCE.

En el caso de que el servicio requiera acceso a los sistemas IT/OT de ENCE, serán de aplicación las siguientes medidas de seguridad:

- **Notificación de Usuarios Asociados al Servicio:**

  El PROVEEDOR deberá notificar a ENCE, al inicio del servicio, los usuarios asociados que necesiten acceso a los sistemas. Asimismo, deberá informar de cualquier modificación que ocurra en relación con estos usuarios durante la vigencia del servicio, incluyendo la notificación de baja al finalizar las actividades relacionadas.

- **Prohibición de Compartir Credenciales:**

  Queda estrictamente prohibido compartir credenciales de acceso, salvo autorización expresa de ENCE. En caso de que, por la naturaleza del servicio, se requiera compartir credenciales, el PROVEEDOR deberá asegurar que estén debidamente identificadas y protegidas según las políticas de seguridad definidas por ENCE.

4.1. Uso de dispositivos de ENCE

En caso de que el servicio implique el uso de dispositivos proporcionados por ENCE, serán de aplicación las siguientes medidas:

- **Aceptación de la Política de Uso Aceptable:**

El PROVEEDOR deberá aceptar y cumplir la política de uso aceptable de dispositivos de ENCE, garantizando que estos se empleen exclusivamente para los fines establecidos y conforme a las normativas aplicables.

- **Notificación de Incidentes:**

  El PROVEEDOR deberá notificar de manera inmediata a ENCE cualquier incidente relacionado con la pérdida, extravío o robo de los dispositivos proporcionados.

4.2. Uso de dispositivos del Proveedor

En caso de que el servicio implique el uso de dispositivos propios del PROVEEDOR, se deberán cumplir las siguientes medidas:

- **Medidas Fundamentales de Seguridad:**

  Los equipos utilizados por el PROVEEDOR deberán contar con medidas fundamentales de seguridad que incluyan, como mínimo:

  - Antivirus activo y actualizado.
  - Actualización de los últimos parches de seguridad.
  - Control de acceso al equipo.
  - Cifrado del dispositivo.
  - Uso de contraseñas seguras.
  - Ausencia de software escaneadores o analizadores de red.
  - Garantía de que el software utilizado sea original y con licencias.

- **Prohibición del Uso de Dispositivos Personales:**

  Queda estrictamente prohibido el uso de dispositivos electrónicos personales para acceder a los sistemas de ENCE.

4.3. Desarrollo de Software

En caso de que el servicio licitado implique el desarrollo de software, el PROVEEDOR deberá garantizar el cumplimiento de las siguientes medidas de seguridad:

- **Estándares de Desarrollo Seguro:**

  El PROVEEDOR deberá aplicar estándares de desarrollo seguro, siguiendo las mejores prácticas reconocidas como OWASP y SecDevOps, para garantizar la protección contra vulnerabilidades en el software desarrollado.

- **Documentación Adecuada:**

  Todo desarrollo o proyecto deberá contar con una documentación adecuada y completa que incluya detalles sobre la arquitectura, el código implementado y las pruebas de seguridad realizadas.

- **Segregación de Entornos (si el desarrollo se realiza en la infraestructura del PROVEEDOR):**
  - Mantener los entornos de desarrollo y/o pruebas completamente segregadas del entorno de producción, incluyendo la separación de credenciales asociadas a cada entorno.
  - Garantizar que no se almacene información sensible de ENCE en los entornos de desarrollo y pruebas para preservar la confidencialidad e integridad de los datos.

- **Auditorías y Pruebas de Seguridad del Software:**
  - Realizar auditorías y pruebas de seguridad del software con el fin de identificar y mitigar posibles vulnerabilidades antes de su implementación.

- **Gestión de Vulnerabilidades:**

  En caso de detectar debilidades en el software, el PROVEEDOR deberá informar de inmediato a ENCE y adoptar las medidas necesarias para corregirlas en el menor tiempo posible.

4.4. Uso de SaaS

Cuando el servicio licitado implique el uso de soluciones SaaS (Software as a Service), el PROVEEDOR deberá garantizar el cumplimiento de las siguientes medidas de seguridad:

- **Certificaciones:**

  El PROVEEDOR deberá contar con certificaciones de ciberseguridad reconocidas, tales como ISO 27001, IEC 62443 u otras equivalentes, que garanticen el cumplimiento de estándares de seguridad internacionales.

- **Gestión de Vulnerabilidades:**

  Se deberán realizar pruebas de seguridad de manera regular, incluyendo pruebas de penetración, informando a ENCE sobre cualquier vulnerabilidad detectada y aplicando las medidas correctivas necesarias en tiempo y forma.

- **Gestión de Accesos:**
  - Implementar un modelo centralizado para gestionar roles y permisos, asegurando flujos de aprobación previamente establecidos.
  - Utilizar contraseñas robustas: un mínimo de 10 caracteres para usuarios estándar y 16 caracteres para usuarios con privilegios administrativos.

- **Segregación de Entornos:**

  Los entornos de producción, pruebas y desarrollo deberán mantenerse completamente segregados.

- **Cifrado de Conexiones:**

  Garantizar que todas las conexiones sean cifradas, utilizando protocolos seguros como HTTPS u otros equivalentes.

- **Aislamiento de la Información:**

  Asegurar el aislamiento lógico de la información de ENCE respecto a la de otros clientes y la propia del PROVEEDOR, protegiendo la confidencialidad y la integridad de los datos.

- **Respuesta a Incidentes:**

  El PROVEEDOR deberá disponer de procedimientos establecidos para la gestión de incidentes, asegurando tiempos de respuesta adecuados que minimicen el impacto de los mismos.

- **Garantía de Disponibilidad del Servicio:**
  - Implementar planes de contingencia que garanticen la continuidad del servicio en caso de incidentes o interrupciones.
  - Realizar copias de seguridad regulares, asegurándose de que estén disponibles para su restauración en caso de pérdida de datos.

- **Registros de Auditoría:**

  Bajo petición, el PROVEEDOR deberá tener la capacidad de proporcionar registros de auditoría que permitan monitorear el acceso al servicio y a los datos que contiene.

5. Acceso a datos reales de ENCE

Cuando el servicio licitado implique el acceso a datos reales de ENCE, el PROVEEDOR deberá garantizar el cumplimiento de las siguientes medidas de seguridad:

- **Protocolos y Procedimientos de Seguridad Física:**

  El PROVEEDOR deberá garantizar que existen protocolos, procedimientos y medidas de seguridad física adecuados para restringir el acceso a cualquier información confidencial de ENCE, ya sea en formato digital o en papel.

- **Acceso Restringido a Personal Autorizado:**

  El acceso a dichas áreas deberá ser exclusivamente permitido a las personas que estén debidamente autorizadas en cada momento, asegurando que solo el personal autorizado pueda interactuar con los datos de ENCE.

5.1. Acceso a datos personales de ENCE

Cuando el servicio licitado implique el acceso a datos personales sobre los que ENCE es responsable de tratamiento , el PROVEEDOR deberá garantizar el cumplimiento de las siguientes medidas de seguridad:

- **Firmar un Acuerdo de Encargo de Tratamiento:**

  Deberá garantizar que el tratamiento de dichos datos se realice conforme a la legislación aplicable y a las instrucciones de ENCE.

- **Mantener Separada y Cifrada la Información Confidencial:**

  La información confidencial de ENCE deberá mantenerse separada y cifrada respecto a la información de otros clientes y la propia del PROVEEDOR, protegiendo su integridad y confidencialidad en todo momento.

- **Transferencias Seguras de Información Confidencial:**

  Las transferencias electrónicas de información confidencial de ENCE a través de redes públicas o no seguras deberán realizarse de manera segura, utilizando métodos de cifrado apropiados y estándares internacionales, tales como FIPS o NIST.

- **Obligaciones de Confidencialidad para el Personal:**

  Todos los empleados y contratistas que tengan acceso a información confidencial de ENCE estarán sujetos a obligaciones de confidencialidad que serán, al menos, tan estrictas como las establecidas en el contrato con ENCE.

5.1.1. Transferencia de datos personales fuera de la Unión Europea.

En caso de que se prevea la transferencia de datos personales fuera de la Unión Europea, se deberán cumplir las siguientes medidas:

- **Información y Autorización Previa:**

  Será imprescindible solicitar y obtener la autorización expresa a ENCE para transferir datos personales fuera del territorio de la Unión Europea.

5.2. Acceso a información confidencial de ENCE

Cuando el servicio implique el acceso a información confidencial de ENCE, se deberán cumplir las siguientes medidas de seguridad:

- **Cláusulas de Confidencialidad (NDA):**

  Se deberán firmar cláusulas especiales en los contratos que garanticen la confidencialidad de la información de ENCE, incluyendo acuerdos de no divulgación (NDA) cuando sea necesario.

- **Separación y Cifrado de la Información Confidencial:**

  Se deberá mantener la información confidencial de ENCE completamente separada y cifrada respecto a la información de otros clientes y la propia del PROVEEDOR, garantizando la integridad y la confidencialidad de los datos.

- **Transferencias Seguras de Información Confidencial:**

  Las transferencias electrónicas de información confidencial de ENCE a través de redes públicas o no seguras deberán realizarse de forma segura, utilizando métodos de cifrado apropiados de acuerdo con estándares internacionales, como FIPS o NIST.

- **Obligaciones de Confidencialidad para Empleados y Contratistas:**

  Se deberá garantizar que todo aquel que tenga acceso a la información confidencial de ENCE esté sujetos a obligaciones de confidencialidad no menos estrictas que las impuestas en el contrato.

6. Acceso físico a instalaciones con sistemas IT/OT de ENCE

Cuando el servicio licitado requiera acceso físico a las instalaciones donde se encuentren sistemas IT/OT de ENCE, se deberán cumplir las siguientes medidas de seguridad:

- **Lista de Personal Autorizado:**

  Se deberá proveer una lista detallada del personal del PROVEEDOR que requerirá acceso a las instalaciones donde se encuentren sistemas IT/OT de ENCE, incluyendo los detalles de identificación de cada persona.

- **Identificación Visible:**

  Todo el personal del PROVEEDOR que se encuentre en las instalaciones donde haya sistemas IT/OT de ENCE deberá llevar una identificación visible en todo momento, conforme a los protocolos de seguridad establecidos por ENCE.

7. Impacto en negocio

En caso de que el servicio implique situaciones de impacto crítico en el negocio, se deberán cumplir las siguientes medidas de seguridad:

- **Colaboración en Gestión de Incidentes:**

  En caso de incidentes, se deberá colaborar con ENCE en las notificaciones a las autoridades o terceros y en la implementación de las medidas necesarias para gestionar la situación, según lo requiera el CLIENTE o lo exijan las normativas vigentes.

- **Confidencialidad en Comunicaciones:**

El PROVEEDOR no podrá compartir con terceros, ni publicar ninguna comunicación o nota de prensa sobre un incidente de ciberseguridad que mencione a ENCE, salvo que cuente con la autorización previa y por escrito de ENCE.